Network Manager IP Edition
Version 3 Release 9

Installation and Configuration Guide

R2E2

Network Manager IP Edition
Version 3 Release 9

Installation and Configuration Guide

R2E2

Note
Before using this information and the product it supports, read the information in "Notices" on page 353.

This edition applies to version 3, release 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 Installation and Configuration Guide* describes how to install Network Manager IP Edition. The guide also describes post-installation configuration tasks. This publication is for administrators who need to install and set up Network Manager IP Edition.

Intended audience

This publication is intended for administrators who need to install Network Manager and perform post-installation configuration.

Readers need to be familiar with the following topics:

- Network management
- Operating System configuration

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 vi.

What this publication contains

This publication contains the following sections:

- Chapter 1, "Planning for installation," on page 1

  Provides information on what to consider before installing Network Manager, such as deployment configurations including failover and network domains, hardware, operating system, software, and communication requirements.
- Chapter 2, "Installing," on page 51

  Describes how to install Network Manager.
- Chapter 3, "Upgrading and migrating," on page 127

  Describes how to upgrade to the latest version of Network Manager, including the migration of existing data from your previous production environment.
- Chapter 4, "Configuring Network Manager," on page 155

  Describes tasks to perform after installing Network Manager, and settings you can change later on during the use of the product.

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 IBM Knowledge Center Web site at:

http://www-01.ibm.com/support/knowledgecenter/

Network Manager documentation is located under the **Cloud & Smarter Infrastructure** node on that Web site.

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 accessibility of the Network Manager Knowledge Center is described in the Knowledge Center itself.

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. Planning for installation

Read about deployment considerations and system requirements for Network Manager.

IPv6 dual stack support is required if workstations or network devices have IPv6.

Deployment of Network Manager

Use this information for guidance on how to configure the physical deployment of your Network Manager installation.

Deployment scenarios

How you deploy Network Manager depends on your environment, including factors such as the size and complexity of your network and the number of operations staff who require system access.

The following are typical Network Manager deployment scenarios:

- Small demonstration or educational system deployment
- Small customer network
- Medium customer network
- Telecommunications company or service provider network
- Large customer network
- Very large customer network

Note: Failover can be applied to each of these Network Manager deployments.

This section provides general guidance to assist you in deciding how to deploy Network Manager. For more detailed information, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide* and the *IBM Tivoli Network Manager IP Edition Release Notes*.

Network and deployment comparisons

Use this information to compare the example customer networks and to compare the Network Manager deployments for each of the example customer networks.

Customer networks compared:

Use this information to compare the example customer networks and to identify which example most closely matches your network.

The following table lists typical features for each of the example customer networks. These values are example values only. Your specific network values might vary. In particular, you should note the following:

- With regard to the values for *Average number of interfaces per device* specified in this table, the actual interface counts can vary considerably from the average interface count. An example of this is found in MPLS networks, where the number of interfaces per device is very high in the core network, but might be as low as 2 to 3 interfaces per device for the edge devices.

- With regards to the number of devices for a telecommunications company, the value specified (15,000) is an average value. A national telecommunications company will have a far larger number of devices, a small local telecommunications company will have far fewer.

Table 1. Example customer networks compared

Feature	Demo	Enterprise				Telco
		Small	**Medium**	**Large**	**Very large**	
Number of devices	25	150 to 300	250 to 5,000	5,000 to 15,000	15,000 to 30,000	15,000
Average number of interfaces per device	1-2	3-5	20-30	30 or more	30 or more	1,200
Network locations	Single location	Single location	Distributed	Global network	Global network, distributed management	One or more locations
Network architecture	Flat	Flat	Flat	Complex	Complex	Complex
Number of active GUI clients	1 to 3	3	5 to 20	5 to 20	5 to 20	5 to 20
Chassis ping polling examples	Values set for demonstration purposes	2-minute intervals	2 - 5 minutes	2 - 5 minutes	2 - 5 minutes	2 - 5 minutes
SNMP polling examples	Values set for demonstration purposes	3 to 6 values at 30 minute intervals	5 to 15 minute intervals	10 to 15 minute intervals.	Intervals of 15 minutes or longer	5 values at 5 minute intervals
	SNMP v1, 2c, or 3 polling in any of the environments listed Device and interface polls in any of the environments listed.					
Tivoli® product integrations	None	None	ITM with TDW	ITM with TDW TBSM TADDM	ITM with TDW TBSM TADDM	ITM with TDW TBSM TADDM
Performance data collection period	1 to 5 days	31 days	31 days	31 days	31 days	7 days

Network Manager deployments compared:

Use this information to compare the Network Manager deployments for each of the example customer networks.

The following table lists the settings required for the Network Manager deployments for each of the example customer networks. These values are example values only. The values that are appropriate for your specific deployment might vary.

Note: With regard to the values for *Deployment* specified in this table, these values do not take failover servers into account.

Table 2. Example Network Manager deployments compared

Settings	**Demo**	**Enterprise**				**Telco**
		Small	**Medium**	**Large**	**Very large**	
Platform	Windows or Linux x86	Any supported platform	Any supported platform	Linux and UNIX	Linux and UNIX	Any supported platform
Deployment	Single server	Single server	1- 2 servers	3-4 servers	4 or more servers	3 servers
Client system	Single processor 2 GB DRAM minimum, or 4 GB DRAM for large networks Supported JRE and Internet browser					
Topology database	Default database	Default database	Any supported RDBMS	Any supported RDBMS	Any supported RDBMS	Any supported RDBMS
Number of network domains	1	1	1 - 2	2 or more	2 or more	1 - 2
Number of polling engines based on network size	1	1	Consider more than one poller	Consider more than one poller	Consider more than one poller	Consider more than one poller

Reasons for multiple domains:

There are a number of reasons why you might need to partition your network into multiple domains.

You might need to partition your network into multiple domains for one of the following reasons:

- Your network exceeds a certain size. See the section *Guidelines for number of network domains* to determine whether your network requires multiple domains.
- Discovery takes a very long time. You can shorten your discovery times by partitioning your network into multiple domains.
- Operational boundaries dictate the need for multiple domains. Examples of operational boundaries include geographical boundaries and security boundaries.
- Your network contains overlapping IP addresses.

Guidelines for number of network domains:

If your network exceeds a certain size, you might need to break up the network into multiple domains. Guidelines are provided here to help work out the number of network domains needed for your deployment. The number of domains is influenced by the number of entities that are discovered, which depends on the technical features of the network, and the business requirements that control your environment.

Depending on the operating system, a single Network Manager domain can support approximately 250,000 or 400,000 network entities that are created during a discovery operation. Network entities include ports, interfaces (including logical interface elements), cards, slots, and chassis. The following table identifies, for each

supported operating system, the maximum memory supported for a discovery process and the number of network entities supported for each Network Manager domain:

Operating system	Maximum memory for a discovery process	Number of network entities supported for each domain
Solaris	4 GB	400,000
Linux	4 GB	400,000
zLinux	2 GB	250,000
AIX	3.25 GB (The operating system reserves some of the pointer memory range.)	400,000
Windows 2008	2 GB	250,000

The number of network entities that a discovery operation creates is dependent on a number of factors that might require you to create and configure extra network domains. These factors include the following:

- Device types — For example, a Cisco NEXUS or Juniper router with virtual router instances can contribute hundreds or thousands of network entities (ports, interfaces, cards, slots, and so on) per chassis.
- Network type — For example, a discovery operation performed on a local area network (LAN) typically contributes more network entities than a comparable size wide area network (WAN).
- Type of discovery agents enabled — For example, the Entity and JuniperBoxAnatomy discovery agents are inventory based discovery agents that typically create extra network entities that other agents do not create.
- Routed or switched network — For example, switched networks tend to generate more network entities than routed networks because they contain VLANs, which contain multiple entities.

The size of a Network Manager domain might be driven by business requirements. For example, a customer might require a network discovery to complete within defined daily maintenance periods. In this scenario, although a single Network Manager domain running on Solaris, Linux, or AIX can support approximately 400,000 network entities, the length of time to complete a discovery of this size might not fit within the daily maintenance period. Consequently, two scoped domains, each supporting approximately 200,000 network entities, are required to support this business requirement.

Use the following procedure to determine the number of required domains. For information on how to create and configure extra network domains, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

Note: The calculations presented here provide approximate figures only. The actual number of domains required varies, depending on various factors, including the factors described previously.

1. Gather the following data:
   - Number of devices in the network
   - Average number of interfaces per device

     Note: The actual interface counts on a given device can vary considerably from the average interface count. An example of this is found in MPLS

networks, where the number of interfaces per device is very high in the core network, but might be as low as 2 to 3 interfaces per device for the edge devices.

2. Apply the following equation to determine an approximate number of network entities:

   Number of network entities = Number of devices * Average interface count * *multiplier*

   Where:

   - *multiplier* = 2 for a routed network
   - *multiplier* = 3.5 for a switched network

   Note: Switched networks tend to generate more network entities because they contain VLANs, which contain multiple entities.

3. Apply one of the following equations to determine the suggested number of network domains:

   Number of domains required = (Number of network entities) / 250,000

   Where 250,000 is the suggested maximum number of network entities in a domain for operating systems that support this number of network entities.

   Number of domains required = (Number of network entities) / 400,000

   Where 400,000 is the suggested maximum number of network entities in a domain for operating systems that support this number of network entities.

   Note: The suggested maximum number of network entities is only a rough guideline for domain sizing. The actual number of network entities per domain varies depending on various factors, including the factors described previously.

Router-centric customer

The data for this customer is as follows:

- Number of devices in the network: 15,000
- Average number of interfaces per device: 20

This customer is running on Linux (which supports 400,000 network entities).

This customer network will produce approximately 600,000 network entities:
Number of network entities = 15,000 * 20 * 2 = 600,000

Based on the following calculation, this network requires *two* network domains:
Number of domains required = 600,000 / 400,000 = 1.5

Switch-centric customer

The data for this customer is as follows:

- Number of devices in the network: 1,000
- Average number of interfaces per device: 24

This customer is running on Solaris (which supports 400,000 network entities).

This customer network will produce approximately 84,000 network entities:
Number of network entities = 1,000 * 24 * 3.5 = 84,000

Based on the following calculation, this network requires *one* network domain:
Number of domains required = 84,000 / 400,000 < 1

What to do next

- Create and configure the extra network domains. For more information about creating and configuring extra network domains, see the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.
- Fix Pack 4 To link the discovered domains in a single network topology, configure the cross-domain discovery function.

Demonstration or educational system deployment

This is a small installation for use as a demonstration system or for training and educational purposes.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

This environment consists of about 25 network devices and key servers combined. All devices are in one location, on the same network subnet as the devices to be managed. There is one local GUI client session supported by the same machine that hosts the Network Manager product components. There might be one or two GUI client sessions on other machines. The network devices come from multiple vendors. The network architecture is flat. All devices are attached to a LAN and have Fast Ethernet connections. For demonstration purposes only, a number of network devices have SNMPv3, and a number of workstations have IPv6.

Within this environment the following example conditions apply:

- 1 to 3 active GUI clients.
- Chassis ping polling and some SNMP polling activity is required.
- No major Tivoli products are integrated with the system, other than the required Tivoli Netcool/OMNIbus.
- Performance reports are required for short data collection periods (typically 1 to 5 days) to match the length of the training course.

Network Manager deployment

A single-server deployment is sufficient for this type of environment. In addition to the single-server deployment description provided elsewhere, the following deployment settings are appropriate for this type of environment.

- Windows or Linux x86 platform.
- System is an entry workstation class machine, with 4 to 6 GB of memory, dual-core processor preferred, single-core acceptable, reasonable current processor speed, and Fast Ethernet capability.
- Default database used for the NCIM database.
- Client system: single processor, 3 GB of memory, supported JRE and Internet browser
- IPv6 dual stack support is required if workstations or network devices have IPv6.

Small customer network

This customer is a company with a network consisting of about 150-300 network devices and key servers. The purpose of this installation is to manage this customer network by alerting the operations staff to major failures.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

The primary users of the product are the networking operations staff. All devices are in one location and managed by a small operations group of a few people. Network devices come from multiple vendors. A mixture of layer 2 and layer 3 network devices are present. Approximately 20 to 30 VLANs are defined. The network architecture is fairly flat and simple. All devices to be managed are located in the same network as the Network Manager system and have Fast Ethernet connections. Internet connections are passed through a firewall and access to the systems within the protected network is available through a company VPN. The network operations staff have clients attached by means of one of the following: a local LAN, WiFi connections, or by means of a VPN established by a telecommunications service provider. Network changes are made once a month and a new discovery is anticipated at this time.

Within this environment the following example conditions apply:

- 3 active GUI clients.
- Chassis ping polling at two-minute intervals. SNMP polling at 30 minute intervals. Typically three to 6 SNMP MIB values require polling.
- No major Tivoli products are integrated with the system, other than the required Tivoli Netcool/OMNIbus.
- Performance reports are required for data collection periods on the order of 31 days.

Network Manager deployment

A single-server deployment is sufficient for this type of environment. In addition to the single-server deployment description provided elsewhere, the following deployment settings are appropriate for this type of environment.

- A single network domain is sufficient for this size of network.
- System can be any of the supported platforms. System requires 6 to 8 GB of memory, dual-core processor, and multiple physical disks in RAID 5 configuration.
- Client system: single processor, 3 GB of memory, supported JRE and Internet browser
- Default database used for the NCIM database.
- A single ncp_poller polling engine is sufficient for this environment.
- IPv6 dual stack support is required if workstations or network devices have IPv6.

Medium customer network

This customer is a company with a central major data center and connections to several remote sites. The purpose of this installation is to manage this customer network by alerting the operations staff to major failures.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

This network has between 250 and 5000 network devices and key servers of interest. Workstations, while numbering in the thousands, are not managed. Network devices come from multiple vendors. All devices in the central location have Fast Ethernet or Gigabit Ethernet connections. Remote sites are connected by WAN connections. The devices and servers to be managed are distributed among the central and remote sites.

Within this environment the following example conditions apply:

- There are 5 to 20 active GUI clients.
- Chassis ping polling at two to five-minute intervals. SNMP polling at five to 15-minute intervals.
- Other major Tivoli products integrated with the system, other than the required Tivoli Netcool/OMNIbus: IBM Tivoli Monitoring with Tivoli Data Warehouse running DB2® to support performance reporting.
- Performance reports are required for data collection periods on the order of 31 days.

Network Manager deployment

Each customer environment with this kind of network is different. The key to success is adequate memory and a careful understanding of the polling targets, combined polling rates, and the event rates. The following deployment settings are appropriate for this type of environment.

- One or two network domains are required, depending on the size of network.
- Single server deployment

  Minimum of four processors, up to eight processors for two domains or 10 to 20 concurrent Tivoli Integrated Portal users

  Minimum of 12 GB memory, up to 32 GB memory for a large network in the medium customer network or 10 to 20 Tivoli Integrated Portal users

  Multiple physical disks in RAID 5 configuration
- System may be any of the supported platforms.
- Client system: single processor, 3 GB of memory, supported JRE and Internet browser
- Any supported RDBMS used for the NCIM database.
- Number of polling engines:

  Single-server deployment: 1

  Two-server deployment: One poller for chassis pings, two or more pollers for SNMP polls
- Number of polling engines: Minimum of one, with two or more needed depending on polling needs.

Large customer network

This customer is a large enterprise company with a globally deployed network. The purpose of this installation is to manage this customer network by alerting the operations staff to major failures and to support the latest network devices and network architecture.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

The architecture of the network is complex. and contains the most up to date technology. For example, the network contains MPLS core networks. The network device count ranges from 5,000 to 15,000 devices, and the complexity of the network is reflected in the fact that there are 30 or more ports per device on average. Network operations are done from a central location with operations staff constantly monitoring the core network. Network devices come from multiple vendors.

Within this environment the following example conditions apply:

- There are typically 5 to 20 concurrently active GUI clients.
- Polling:

  Chassis ping polling at two to 5 minute intervals.

  SNMP polling at 10-15 minutes.

  SNMPv3 polling of key network devices

  SNMPv1 polling for real time graphing as well as storage for performance reports.
- Other major Tivoli products integrated with the system, other than the required Tivoli Netcool/OMNIbus:

  IBM Tivoli Monitoring (ITM) with Tivoli Data Warehouse (TDW) running DB2 to support performance reporting.

  IBM Tivoli Business Service Manager (TBSM)

  IBM Tivoli Application Dependency Discovery Manager (TADDM)
- Performance reports are required for data collection periods on the order of 31 days.

Network Manager deployment

Deployment choices vary depending on the size of the network. For the 1000 device network in this customer range, the choice ranges from a single-server to a two-server deployment. Key factors for success include the network response time for the targets (given that this is a county or global distribution of target devices), memory availability on the supporting servers, the polling selected and the rates of polling.

For the top end of the network (approximately 15,000 devices), a distributed, multiple domain deployment is required. In addition to the multiple-server deployment description provided elsewhere, the following deployment settings are appropriate for this type of environment.

- Deploy a minimum of two domains with one server for every two domains.
- Deployment of a dedicated database server is recommended.

- Deployment of a dedicated server to host Tivoli Integrated Portal and Tivoli Netcool/OMNIbus is recommended.
- Each of the servers requires the following:
  - Four processors.
  - 32 GB of memory.
  - 3 disk, RAID 5 multiple disk array
- For the systems used for each domain, deploy as follows:
  - Server 1: Network Manager
  - Server 2: Tivoli Netcool/OMNIbus and Tivoli Integrated Portal
  - System 3 (optional): a customer-selected RDBMS supporting both domains
- Systems to be deployed on Linux or UNIX platform.
- Any supported RDBMS used for the NCIM database.
- A minimum of two polling engines is recommended:
  - Use the default ncp_poller process for chassis ping.
  - Create a separate ncp_poller for the SNMP polls.
- Client system: single processor, 3 GB of memory, supported JRE and Internet browser
- IPv6 dual stack support is required if workstations or network devices have IPv6.

Very large customer network

This customer is a very large global enterprise company with a simple network architecture but very large numbers of devices. The purpose of this installation is to manage this customer network by alerting the operations staff to major failures and to support short-term capacity planning.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

Network management is done from a central location and from regional locations. The network is very large and contains over 15,000 network devices and critical servers. Network devices come from multiple vendors. The devices fall into two categories:

- Network device infrastructure with interface counts in the range of 30 or more per device.
- Managed devices with 1-2 interfaces per device.

The majority of the devices are in the second category, managed devices. To manage a network of this size, the network is partitioned for management on a geographical basis.

Within this environment the following example conditions apply:

- There are 5 to 20 active GUI clients.
- Polling:
  - Chassis ping polling at two to 5 minute intervals.
  - SNMP polling at 15 minutes or longer.
  - SNMPv1 data collection

- Other major Tivoli products integrated with the system, other than the required Tivoli Netcool/OMNIbus:

  IBM Tivoli Monitoring (ITM) with Tivoli Data Warehouse (TDW) running DB2 to support performance reporting.

  IBM Tivoli Business Service Manager (TBSM)

  IBM Tivoli Application Dependency Discovery Manager (TADDM)
- Performance reports are required for data collection periods on the order of 31 days.

Network Manager deployment

Assistance from an experienced IBM services group or qualified IBM business partner is highly advisable for a successful deployment. Multiple domains are needed, supported by a collection of individual servers, or running together on a very large system. After completing a survey of the network to be managed, break the network up into sections that yield about 300,000 to 400,000 network entities, and then assign each of these sections be to a domain. In addition to the multiple-server deployment description provided elsewhere, the following deployment settings are appropriate for this type of environment.

- Multiple network domains.
- Platform selections: Linux and UNIX.
- Large systems (many processors and very large amounts of memory) can host multiple domains as long as the memory allocations and processor counts are acceptable.

  Memory: 16-32 GB per domain

  Processors: 4-8 per domain depending on workloads
- Any supported RDBMS used for the NCIM database.
- Minimum of two polling engines for each domain:

  Use the default ncp_poller process for chassis ping.

  Create a separate ncp_poller for the SNMP polls.
- Individual process memory limitations are a factor in this environment. If using AIX®, enable large memory access.
- Client system: single processor, 3 GB of memory, supported JRE and Internet browser
- IPv6 dual stack support is required if workstations or network devices have IPv6.

Telecommunications company network

This customer is a telecommunications company and internet services provider. The purpose of this installation is to manage this customer network by alerting 24x7 network operations center staff to major failures.

The following sections describe this network in greater detail and provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

The network to be managed has about 300 network devices; with an average interface count per device of 500. This is an MPLS network, and consequently the network devices are “large” in terms of their interface counts and complexity. Network devices come from multiple vendors. All devices are in one or more

locations and are managed by a small network operations group. All devices to be managed are connected via Fast Ethernet or Gigabit Ethernet.

Within this environment the following example conditions apply:

- Number of simultaneous active clients: 5-20.
- Polling requirements: chassis pings at two to 5-minute intervals; SNMP polling of 5 values at 5 minute intervals.
- Some SNMPv3 polling is in place.
- Other major Tivoli products integrated with the system, other than the required Tivoli Netcool/OMNIbus:

  IBM Tivoli Monitoring (ITM) with Tivoli Data Warehouse (TDW) running DB2 to support performance reporting.

  IBM Tivoli Business Service Manager (TBSM)

  IBM Tivoli Application Dependency Discovery Manager (TADDM)
- Performance reports done once a day for key devices, used to assemble weekly capacity reports.

Network Manager deployment

A three-server deployment is needed for this type of environment. In addition to the multiple-server deployment description provided elsewhere, the following deployment settings are appropriate for this type of environment.

- One to two domains.
- A three-server deployment is advised.
- System specifications:

  System 1: two to four processors, 6-8 GB of memory, two or more disks

  System 1: To host Network Manager components: four processors, 16-32 GB of memory, two or more disks. Note that beyond 4 processors or processor cores, the core clock speed and on-chip cache can be more important than additional cores. The general rule is as follows: select the fastest 4 cores before additional cores.

  System 2: To host the NCIM database: two to four processors, 16-32 GB of memory, two or more disks in a suitable RAID configuration to provide the necessary fault tolerance and performance.

  System 3: To host the Tivoli Integrated Portal and Tivoli Netcool/OMNIbus: Four processors, 16 GB of memory.
- Any supported RDBMS used for the NCIM database.
- A minimum of two polling engines:

  Use the default ncp_poller process for chassis ping.

  Create a separate ncp_poller for the SNMP polls.
- Client system: single processor, 3 GB of memory, supported JRE and Internet browser
- IPv6 dual stack support is required if workstations or network devices have IPv6.

Deployment considerations

You can deploy your entire Network Manager installation on a single server or as a distributed installation.

During a Network Manager installation, you install the following four Network Manager components.

Network Manager core
This component consists of the core Network Manager processes: network discovery, polling, root cause analysis and event enrichment.

NCIM database
This database stores topology data. You can opt to install the default Informix database, or use an existing MySQL, DB2, Informix, or Oracle database.

Tivoli Netcool/OMNIbus
This component consists of the Tivoli Netcool/OMNIbus event management software. Many customers choose to have a trouble-ticketing system integrated with Tivoli Netcool/OMNIbus.

Tivoli Integrated Portal
This component consists of the Tivoli Integrated Portal user interface framework, together with the web applications.

The objective of the installation is to place these components on one or more servers.

The following are typical Network Manager deployment configurations:

- Single-server deployment
- Distributed deployment: two servers or more

The factors that require an increased number of servers in a distributed deployment include the following:

- Active event rates
- Amount and rate of stored polling data
- Device status polling rates and number of polling targets
- Network response times for polled targets
- Discovery frequency and
- Size of the network to be discovered (for each domain, where there are multiple domains)

Note: These deployment configurations do not take into consideration requirements for other product integrations.

In addition, you must consider deployment of appropriate systems to support GUI client sessions.

Also, IPv6 dual stack support is required if workstations or network devices have IPv6.

Single-server deployment

Single-server deployments are appropriate for small demonstration or educational systems, and for systems to support small to medium customer networks.

A single-server deployment must meet the following minimum specification:

- A minimum of two processors of current speeds, preferably four processors. Examples of current speeds include 3 GHz or better for processors from the Intel product line, and 1.6 GHz or better for processors from the Sun product line.
- A minimum of 6 GB of memory, preferably 8 GB.

Distributed deployment: two servers or more

In distributed deployments, Network Manager components are distributed across multiple servers, that is, two servers or more. Here are some guidelines for distributed deployments:

- Two-server deployments are appropriate for the top end of the range of medium customer networks.
- Deployments might require three servers or more in situations where there are multiple network domains.
- Three-server deployments might also be deployed where it is determined that a separate server is required to support a relational database product that provides topology data storage. In addition, a separate database server enables the relational database to support multiple applications, in addition to Network Manager.

Two-server deployment

An example of a two-server deployment consists of the following allocation of host workstations:

- *Server 1*: Network Manager core components and the NCIM database. The core components are the network discovery, polling, root cause analysis and event enrichment components.
- *Server 2*: Tivoli Integrated Portal with associated Network Manager web applications.

In this two-server deployment, each server must meet the following minimum specification:

- A minimum of two processors of current speeds, preferably four processors.
- A minimum of 8 GB of memory.
- For improved performance report response time, an enhanced disk I/O system, consisting of three to 6 physical disks in RAID supporting a logical volume.

Three-server deployment

An example of a three-server deployment consists of the following allocation of host workstations:

- *Server 1*: Network Manager core components.
- *Server 2*: Tivoli Netcool/OMNIbus
- *Server 3*: Tivoli Integrated Portal with associated Network Manager web applications, together with the NCIM database.

Client systems

You must consider deployment of appropriate systems to support GUI client sessions.

The following system specification provides support for a wide range of end-user activities on GUI client sessions:

Note: The web application clients, notably the Tivoli Netcool/OMNIbus Web GUI Active Event List and the Network Manager Network Views, Hop View, and Structure Browser, are Java-based and therefore are dependent on the performance of the client system. Consequently, the more memory and CPU performance on the client system, the better.

- Windows 2008 or Windows 7
- Larger display supporting comfortable viewing at higher resolution, such as 1280x1024
- Current® speed single or dual core processor
- 3 GB of memory
- Supported JRE and Internet browser
- Fast Ethernet.
- Processor specification:

  For normal topology displays or event displays
  Single processor with the following speeds: 1 GHz or better, as found on many laptops, 2.4 GHz, as found in many workstations

  Enhanced time to display larger or complex topology maps and enhanced display of MIB graphs
  A very current processor (3.0 GHz or better) typically available in the latest workstation class systems.

Deployment examples

Use these examples of Network Manager to help you plan your deployment architecture.

Constraints for installing and starting components

Some components must be installed and started before others. Use this information as well as the installation examples to understand the order in which you must install and start components.

Topology database constraints

You must install a topology database before you install the Network Manager core components, or as part of the same installation process.

You must install a topology database before you install the Network Manager Web applications (including the Tivoli Integrated Portal), or as part of the same installation process.

You must create database tables only during the first installation of the Network Manager core components or the Network Manager Web applications (including the Tivoli Integrated Portal), and not during subsequent installations.

Tivoli Netcool/OMNIbus constraints

You must install Tivoli Netcool/OMNIbus before you install the Network Manager Web applications (including the Tivoli Integrated Portal), or as part of the same installation process.

Web application constraints

You must install the Network Manager core components before you install the Network Manager Web applications, or as part of the same installation process.

If you are using ObjectServer authentication for the Network Manager Web applications, Tivoli Netcool/OMNIbus must be running during the installation of the Network Manager Web applications.

Starting components in the right order

Do not start the Network Manager core components until the installation of the Network Manager Web applications is complete.

Ensure that both Tivoli Netcool/OMNIbus and the topology database are running before starting the Network Manager core components.

Ensure that Tivoli Netcool/OMNIbus, the topology database, and the Network Manager core components are running before using the Network Manager Web applications.

Related reference:

"Server allocation for failover" on page 284
Any primary system must be installed on a separate host to a backup system, so that if the primary host fails, the backup host is unaffected.

Example simple deployment architecture

Use this example to familiarize yourself with the architecture of a simple Network Manager deployment.

Components

This example simple deployment consists of the following components:

- One ObjectServer virtual pair.
- One Tivoli Integrated Portal server.
- One Network Manager installation running one domain with failover.
- One instance of the NCIM topology database.

The following figure shows the architecture for this deployment.

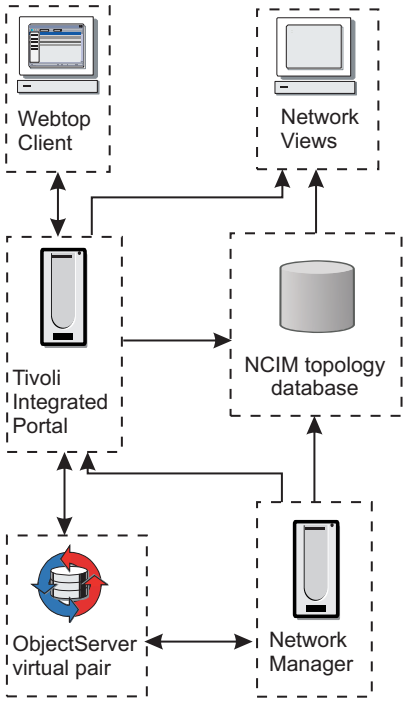

Figure 1. Simple deployment architecture

Allocation of host workstations

The following figure shows an example allocation of host workstations for this deployment.

Note: If you have a particularly large topology, you might want to install the topology database on its own server. This decision depends on the specification of your machines and how you want to spread the load between them.

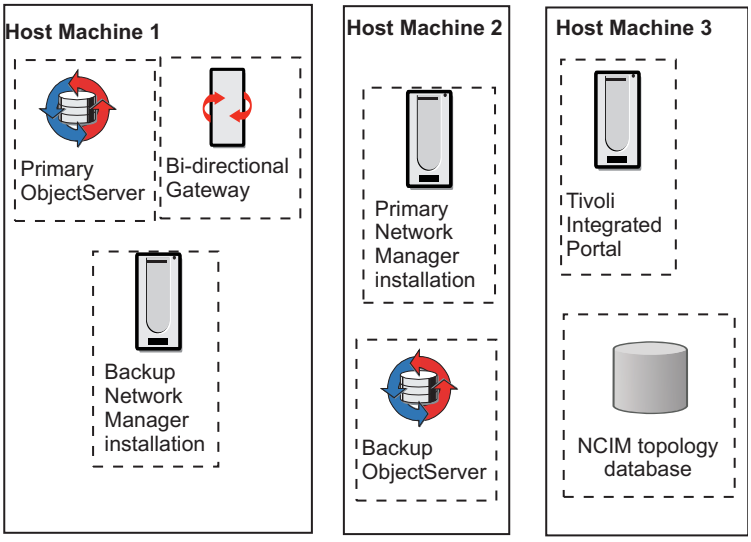

Figure 2. Simple deployment host machine allocation

Steps to install a simple deployment

The following steps provide an overview of the tasks required for this deployment, and help plan for a similar deployment. .

To install the deployment described above, perform the following steps:

1. Install the topology database on host machine 3, create the necessary tables, and start the database.

   Note: The topology database must be installed and started before you start the Network Manager core components so that discovery data can be saved.
2. Install the following ObjectServers and related components:
   a. Install the primary ObjectServer and the Bi-directional Gateway on host machine 1.
   b. Install the backup ObjectServer on host machine 2.
3. Configure and run the ObjectServers.

   Note: The ObjectServers must be running before the Network Manager core components are started.
4. Install the primary Network Manager core components on host machine 2.
5. Install the backup Network Manager core components on host machine 1.
6. Install the Network Manager Web applications on host machine 3 (part of the **GUI components** category in the installation wizard).

   The Tivoli Integrated Portal server is automatically installed with the installation of the Network Manager Web applications.

   Tip: If you install the Tivoli Integrated Portal on a machine with no other products, performance is likely to be better than if you install it on a machine with other products.

   When you install the Network Manager web applications, the Tivoli Netcool/OMNIbus Web GUI is installed and automatically configured on host machine 3 if it is not already installed there. The Tivoli Netcool/OMNIbus Web GUI was known as Netcool/Webtop in versions 2.2 and below.

   Note: The Network Manager core components must be installed before the Web applications.
7. Configure the primary Network Manager for failover and start it.
8. Configure the backup Network Manager for failover and start it.

Example large deployment architecture

Use this example to familiarize yourself with the architecture of a large Network Manager deployment.

Components

This example deployment consists of:

- One ObjectServer and one Network Manager installation in London. The London domain sends events and topology to San Francisco.
- One ObjectServer and one Network Manager installation in New York. The New York domain also sends events and topology to San Francisco.
- One ObjectServer and one Tivoli Integrated Portal installation in San Francisco. The ObjectServer in San Francisco consolidates the events from London and

New York. The Tivoli Integrated Portal server in San Francisco can access topology from both London and New York, but does not consolidate the topologies. Clients anywhere in the world can connect to the Tivoli Integrated Portal server, and view topology from London and New York.

The following figure shows the architecture for this deployment.

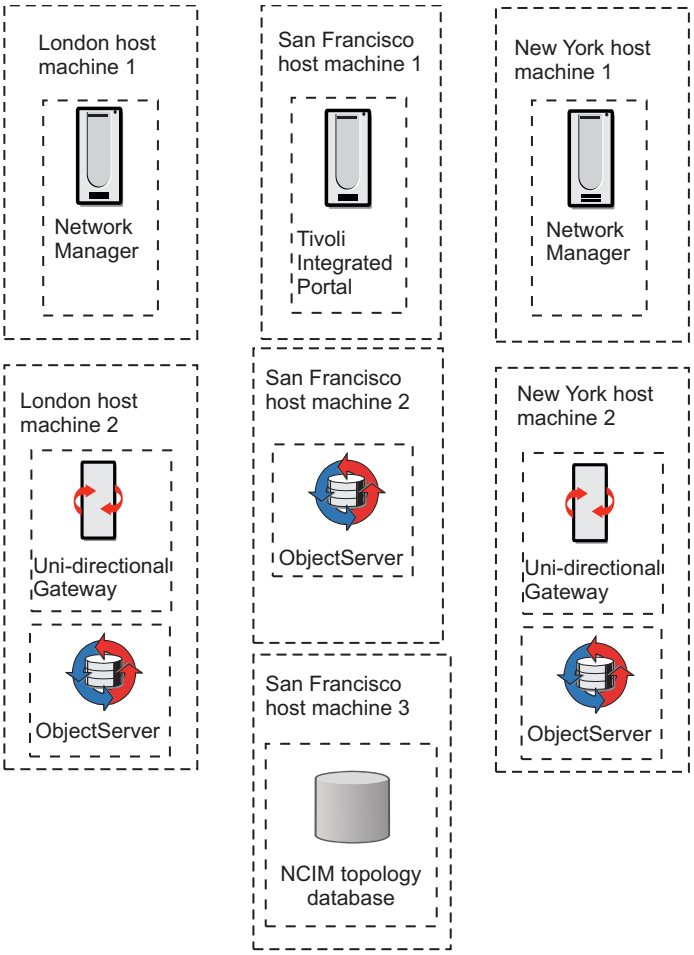

Figure 3. Large deployment architecture

Allocation of host workstations

The following figure shows an example allocation of servers for this deployment.

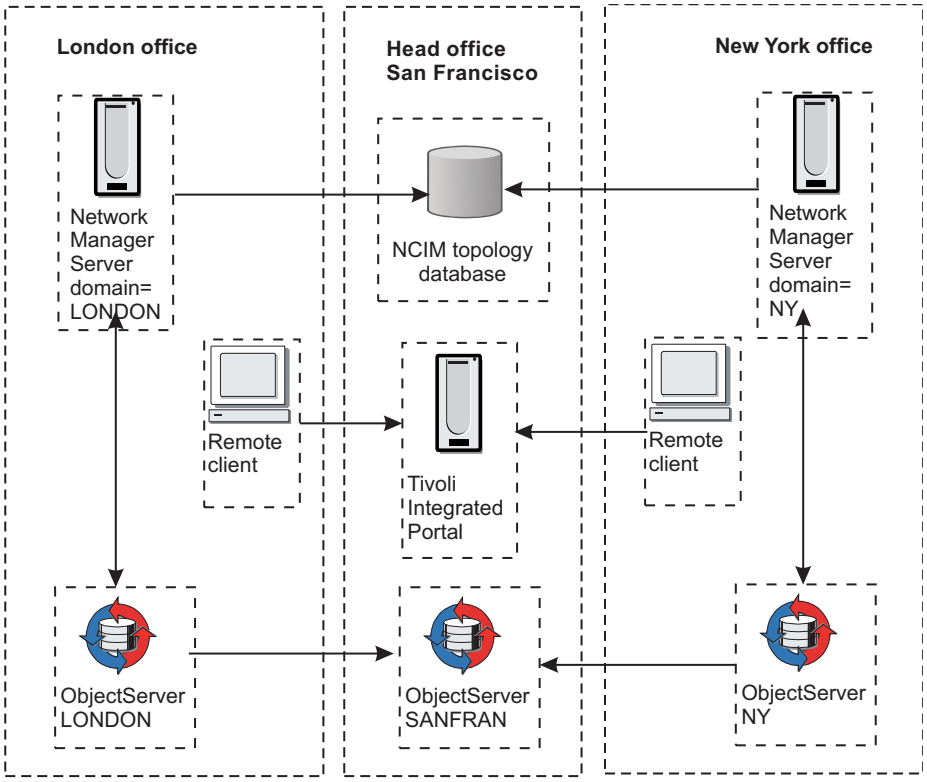

Figure 4. Large deployment host machine allocation

Steps to install a large deployment

The following steps provide an overview of the tasks required for this deployment, and help plan for a similar deployment. .

To install this deployment, perform the following steps:

1. Install the topology database on San Francisco host machine 3, and create the necessary database tables.

   Note: The topology database must be installed and started before you start the Network Manager core components so that discovery data can be saved.
2. Install the following ObjectServers and related components:
   - Install the ObjectServer on San Francisco host machine 2.
   - Install the ObjectServer and the uni-directional gateway on London host machine 2.
   - Install the ObjectServer and the uni-directional gateway on New York host machine 2.
3. Configure and run the ObjectServers.

   Note: The ObjectServers must be running before the Network Manager core components are started.
4. Install the Network Manager core components on London host machine 1.

   Note: The Network Manager core components must be installed before the Web applications.
5. Install the Network Manager core components on New York host machine 1.

6. If a version of Netcool/Webtop earlier than version 2.1 is already present on host machine 3, then upgrade this to the Tivoli Netcool/OMNIbus Web GUI version 7.3.1. Network Manager is not compatible with versions of the Tivoli Netcool/OMNIbus Web GUI prior to 2.2.
7. Install the Network Manager Web applications on host machine 3 (part of the **GUI components** category in the installation wizard).

   The Tivoli Integrated Portal server is automatically installed with the installation of the Network Manager Web applications.

   Tip: If you install the Tivoli Integrated Portal on a machine with no other products, performance is likely to be better than if you install it on a machine with other products.

   When you install the Network Manager web applications, Tivoli Netcool/OMNIbus Web GUI version 7.3.1 is installed and automatically configured on host machine 3 if it is not already installed there.

Network domains

Before installing, you need to consider whether to partition your network into domains, or have a single domain for the entire network. A network domain is a collection of network entities to be discovered and managed.

Restriction: Use only alphanumeric characters and underscores (_) in domain names. All other characters, for example hyphens (-), are not permitted.

Reasons for partitioning your network into multiple domains

Partitioning your network into domains allows you to discover your network in sections. Reasons for partitioning your network include:

- Scalability: Your network might be too big to be discovered in one piece.
- Geography: You might want to break the network into geographical regions, and make each region correspond to a domain.
- Logical network boundaries: You might want to discover and manage the network based on particular network boundaries.

Discovered domains can be monitored separately.

You can run multiple domains in order to perform multiple network discoveries, and multiple Network Manager processes can run independently of each other on the same server if they belong to different domains.

Identifying the domain of an event

Identifying the domain of an event enables the Network Views and Hop view to generate the correct topology map for that event.

The domain in which an event originates can be identified in the following ways:

- By using one domain per ObjectServer and using the name of the ObjectServer to identify the domain from which the event originates.
- By using multiple domains per ObjectServer requires configuration of probes in each domain to enable the event itself to hold information that identifies the domain. This approach enables multiple Network Manager domains to be connected to a single ObjectServer.

Event collection using one domain per ObjectServer

You can configure independent Network Manager domains by using a *collection ObjectServer* and an *aggregation ObjectServer*.

Restriction: The architecture described in this topic is only applicable to Tivoli Netcool/OMNIbus versions 7.2.1 or earlier, and is based on the standard architecture from the Event Services Framework (ESF) that was previously released by the IBM Tivoli Netcool Advanced Architecture Group.

The collection ObjectServer collects events from the probes that are connected to each domain, whereas the aggregation ObjectServer gathers events from each of the collection ObjectServers.

As a result the Network Manager domains are independent. One domain can be up while the other is down for maintenance. Furthermore, the scopes of the discovery can overlap.

This structure is flexible as additional ObjectServers can be added when new domains are required, providing scalability when working with large networks. However, this approach requires multiple ObjectServers and therefore may only be of interest to customers with larger networks.

The following figure shows an example architecture using one domain per ObjectServer.

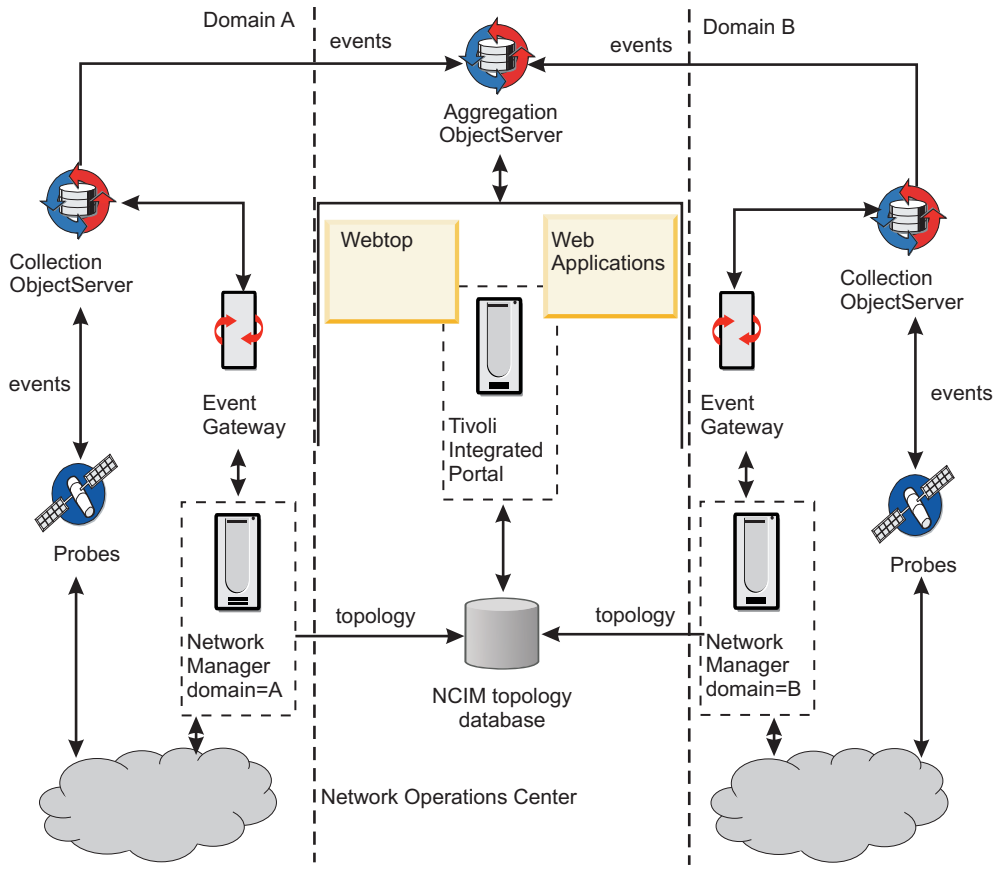

Figure 5. Managing event ownership: architecture for single-domain ObjectServers

Event collection using multiple domains per ObjectServer

You can connect multiple Network Manager domains to a single ObjectServer.

In this configuration, the Tivoli Netcool/OMNIbus probes collect information on the name of the domain when an event is generated and populate the NmosDomainName field to hold this domain name.

To implement this configuration you must first modify all Tivoli Netcool/OMNIbus probe rules files to ensure that each event contains an `NmosDomainName` field. This field is used to store the domain name associated with the event. This also ensures that the event is processed by the Event Gateway.

Note: The incoming event filter in the Event Gateway handles both single-domain and multi-domain systems by default. For more information see the *IBM Tivoli Network Manager IP Edition Event Management Guide*.

Note: This is a less expensive approach as it requires a single ObjectServer only. Scalability might be an issue as each new domain requires extra probe configuration.

The following figure shows an example architecture using multiple domains per ObjectServer.

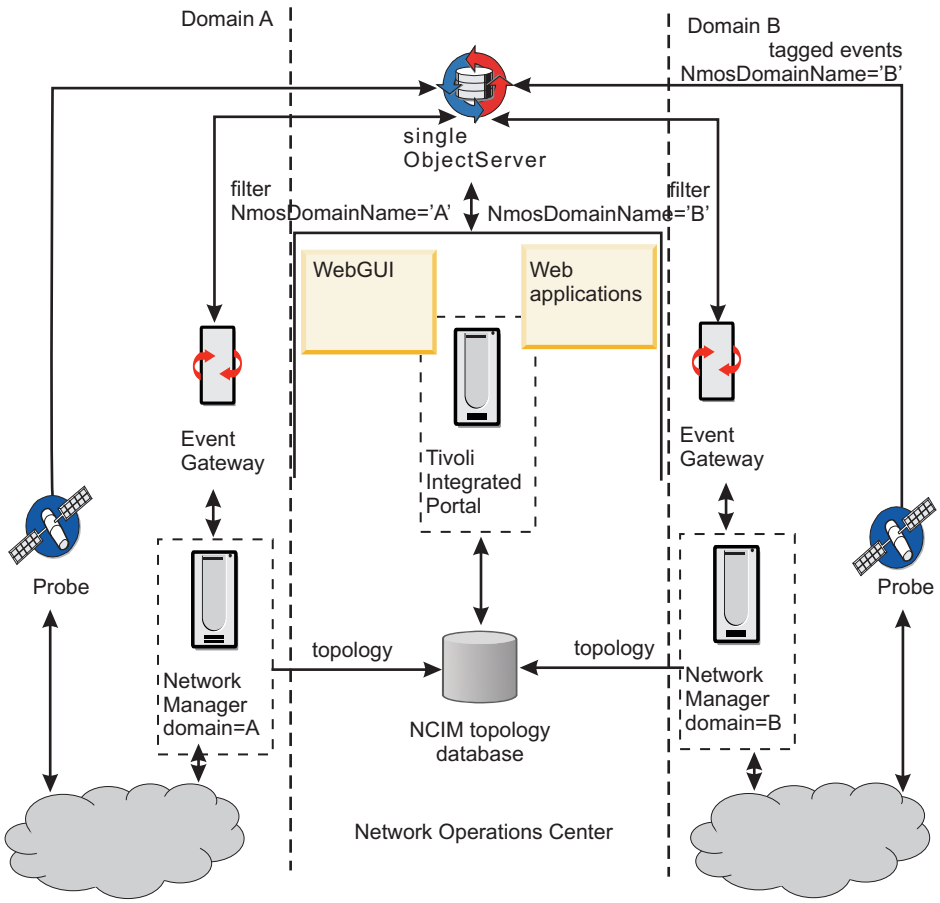

Figure 6. Managing event ownership: architecture for multiple-domain ObjectServer

Example visualization of topology from multiple domains

Web clients using a single Tivoli Integrated Portal can view topology from more than one Network Manager domain.

For more information about viewing topology, see the *IBM Tivoli Network Manager IP Edition Network Visualization Setup Guide*.

To enable topology visualization from multiple domains, each Network Manager domain forwards topology information to the Network Connectivity and Inventory (NCIM) topology database. When you have multiple domains, the topology from each domain is held in NCIM.

Fix Pack 4

Linking discovered domains

You can find links between devices in different domains by configuring and running a cross-domain discovery. The following figure shows an example of three discovery domains feeding data into a single NCIM topology database. In Tivoli Integrated Portal, you can view topology maps in any of the domains by choosing a single domain from the domain menu.

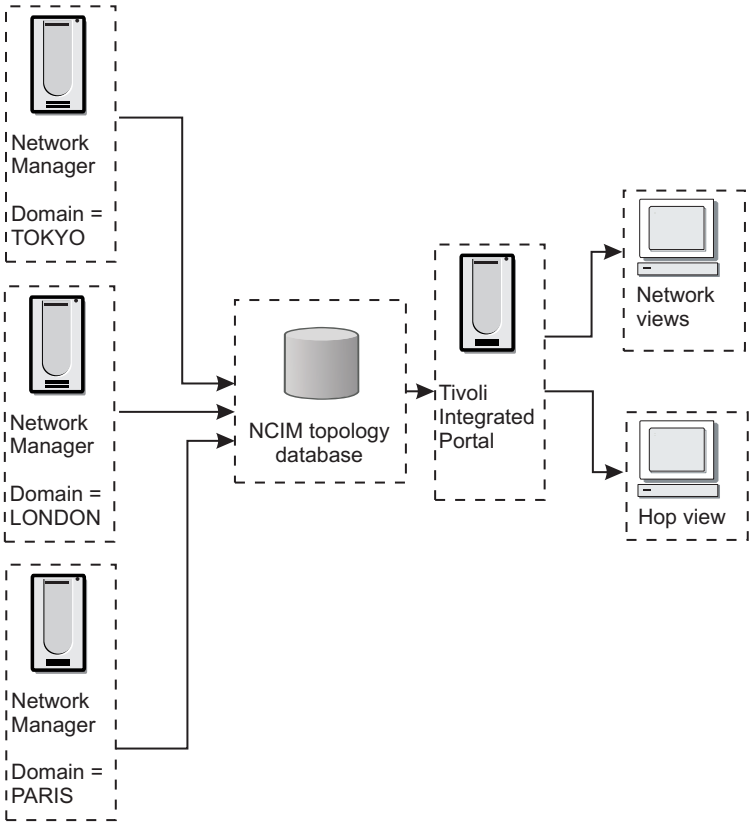

Figure 7. Viewing topology from multiple domains

After cross-domain discoveries are run, an aggregated domain is created in the topology database. The aggregated domain includes device collections from all discovered domains. In Tivoli Integrated Portal, you can view topology maps in all domains by choosing the **AGGREGATION** domain from the domain menu.

Hardware requirements

Hardware requirements vary according to the size and composition of your network and the features of Network Manager you want to use.

Ensure that your servers meet the hardware requirements before you install Network Manager.

Important: Do not run any other resource-intensive applications during the installation of Network Manager.

Processor selection guidelines

Read about guidelines for processor requirements before selecting the right server to install Network Manager on.

The guidelines discussed here are for servers expected to support only Network Manager components. The guidelines assume the deployment of other Tivoli products, such as IBM Tivoli Monitoring, Tivoli Data Warehouse, and IBM Tivoli Business Service Manager on other servers. To combine the deployment of multiple major products on a single server, add the minimal requirements for each product together (see the individual product documentation for more information).

For small customer networks and demonstration or educational system deployments, use two processors at least on all platforms. Deployments of medium or large customer networks require four processors.

Note: For multiple core processors, individual core speed can be more important than the number of cores. While processors of any speed can be used, selecting the fastest core speed and largest on-chip cache makes a significant difference depending on the size of the network being discovered and polled.

For virtualized settings (supported by AIX LPARS, VMWare ESX, and so on) use both processor and memory resources fixed to a virtual system supporting Network Manager.

For zLinux settings, use the CPU allocation equivalent to that of two modern processors, from any of the native UNIX or Windows platforms supported by Network Manager.

For more details on processor selection and other deployment considerations, see "Deployment of Network Manager" on page 1.

Requirements to run the installer

To install any components of Network Manager, your server must meet the hardware requirements.

Disk space requirements for the installer

You need a certain amount of space free in certain directories to be able to run the installer, regardless of which components you are installing.

On UNIX operating systems, you need at least 170 MB space in the `/tmp` directory and at least 350 MB space in the `/usr` directory, and 500 KB in the `/var` directory. If you install Network Manager into any location other than `/opt`, you must have at least 50 MB of space in the `/opt` directory.

Disk space requirements for installing as a non-root user

On UNIX operating systems, if you are installing as a non-root user, you must have at least 350 MB space free in your home directory to store files related to the installation.

Requirements for the core components

To install the Network Manager core components, your servers must meet the minimum hardware requirements.

Memory requirements

Ensure that the server where you want to run Network Manager meets the following memory requirements.

- For a single-server deployment, where the Network Manager core components, Web applications, topology database, and Tivoli Netcool/OMNIbus are all on the same server, you need a minimum of 6 GB DRAM, preferably 8 GB DRAM in a production environment, and 9 to 12 GB DRAM for large networks.

  Note: The installer checks to ensure a minimum of 4 GB DRAM is available to accommodate demonstration and educational system deployments. However, a minimum of 6 GB DRAM is required in production environments.
- For a distributed deployment, where only the Network Manager core components are installed on the server, you need a minimum of 4 GB DRAM.

  Note: The installer checks to ensure a minimum of 3 GB DRAM is available to accommodate demonstration and educational system deployments. However, a minimum of 4 GB DRAM is required in production environments.

The amount of memory required depends on how you deploy Network Manager. For more detailed memory requirements, see "Deployment of Network Manager" on page 1.

Disk space requirements

Ensure that the server where you want to run Network Manager meets the following disk space requirements.

- 2 GB hard disk space to store the software
- 2 GB hard disk space for cache storage
- As a guidance estimate for log files, assuming that each log file is 1 GB in size and six processes are 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).

Bandwidth requirements

The Network Manager server requires a 100 Mbps full duplex fast Ethernet connection (or equivalent) with the DNS server.

It is required that the systems supporting Network Manager components are placed in the data center with LAN speed connections of 100 Mbps fast Ethernet or Gigabit Ethernet to the DNS system and the core network devices to be discovered and managed. Slower connection speeds can be used, but might impact client

session response times and must be factored into key workloads such as polling (including response times, retry count, and total network traffic introduced).

Note: During the discovery of a network device, many SNMP queries are made of that device. After discovery, routine polling (ICMP and SNMP) can introduce significant traffic on the network. With the supporting network hosted by modern LAN speeds, these workloads can be accommodated.

For more details on discovery bandwidth requirements, see "Bandwidth requirements for discovery" on page 29.

Other requirements

You also need a DVD drive, if you are not installing the software from a download.

Requirements for the GUI components

The server on which you install the GUI components of Network Manager (also referred to as Web Applications, which includes Tivoli Integrated Portal, Tivoli Common Reporting, and Tivoli Netcool/OMNIbus Web GUI) must meet the following hardware requirements.

- 5.5 GB hard disk space.
- A minimum of 4 GB DRAM.

  Note: The installer checks to ensure a minimum of 3 GB DRAM is available to accommodate demonstration and educational system deployments. However, a minimum of 4 GB DRAM is required in production environments.
- 500 MB in the `/tmp` directory.
- DVD drive if not installing from download.

Hardware requirements for Tivoli Common Reporting

Review the hardware requirements for Tivoli Common Reporting to make sure you meet your performance requirements.

For detailed information on hardware requirements for Tivoli Common Reporting, see the Tivoli Common Reporting information center at the following URL: http://www-01.ibm.com/support/knowledgecenter/SSH2DF_2.1.1/ctcr_prodoverview.html

Installation directory requirements

When installing on the same machine, the GUI components of Tivoli products using Tivoli Integrated Portal 1.1.x cannot be installed in the same directory as the GUI components of products using Tivoli Integrated Portal 2.1.

For example, Network Manager 3.9 GUI components must be installed in a different directory than IBM Tivoli Business Service Manager 4.2.1 GUI components (the former uses Tivoli Integrated Portal 2.1, while the latter uses 1.1.x). When installing Network Manager, the installation process might recognize existing Tivoli Integrated Portal directories. Make sure you use a different directory if you have products running a previous Tivoli Integrated Portal version.

Requirements for the topology database server

Read about Network Manager topology database requirements.

Memory requirements

If you are installing the default Informix® database with Network Manager installer locally, ensure that the server where you want to run Informix has a minimum of 4 GB DRAM memory available (you might need more for large networks). For information on memory requirements of other databases, see the documentation for the database.

For more information about setting up a remote Informix database or other databases, see the tasks in "Setting up a topology database" on page 56.

Disk space requirements

To store Network Manager data, ensure you have at least the following minimum disk space available for your topology database:

- 5 GB for Informix and on Linux for Z series, you need at least 500 MB free space in the `/tmp` directory, and at least 500 MB free space in the `/` directory.
- 3 to 5 GB for DB2, MySQL, and Oracle.

Note: These figures are minimum values. The actual disk space required depends on the size of your network and the amount of data stored. The storage of performance data can require a large amount of disk space. If you are planning to store such large amounts of data, consider 50 GB for Network Manager-related disk space.

Ensure that the server where you want to run the topology database meets the following disk requirements:

- Three disks in RAID 1 configuration (more disks for RAID 5)
- High speed SATA or SCSI disks

Disk space for events and interfaces

You must calculate and allow additional disk space for the number of events and interfaces on your installation.

The additional hardware requirements for Network Manager are as follows:

- 4 KB of disk space for each expected event, per day of storage required
- 4 KB of disk space for each interface or port on a managed device

For example, if you have 5000 ports on devices in your network, expect 3000 events each day and require events to be stored for 30 days, you require:

```
3000 * 30 * 4 KB = 360 MB
```

The total disk space required is therefore:

```
512 MB + 512 MB cache + 360 MB + (4 KB * 5000) = 1.4GB
```

Swap space requirements (UNIX)

On UNIX platforms, you must ensure that you have adequate free disk space that is configured to be used as swap space.

The exact amount of swap space needed depends on the size and composition of your network and the type of discovery. For smaller amounts of physical RAM, you need proportionally greater amounts of swap space. The following figures show the approximate amount of swap space depending on the amount of physical RAM.

4GB RAM
Configure 10GB swap space.

8GB RAM
Configure 16GB swap space.

12GB RAM
Configure 18GB swap space.

For amounts of RAM greater than 12 GB, configure the same amount of swap space. For example, for 24GB RAM, configure 24GB swap space.

Bandwidth requirements for discovery

Network discovery operations require a minimum of broadband connection speed.

Do not attempt discoveries over dial-up connection speeds. If the connection speed is not sufficient, packets might be lost due to the amount of SNMP traffic that is generated by the default discovery and monitoring operations. Even over a broadband connection, the number of SNMP helper threads must be kept low. This might cause the discovery to take a long time.

Discoveries should be run using an Ethernet (or similar speed) connection. The required speed of the Ethernet connection depends on the size of your network:

- 10 Mbps full duplex speed is required to support up to 100 SNMP helper threads and a relatively low number of devices. If you are using Telnet with SSH to access many devices in the discovery, the number of SNMP helper threads should be reduced due to the bandwidth used by the Telnet Helper.
- 100 Mbps full duplex fast ethernet connection (or equivalent) is required for discovering a large network. Bandwidth should not be a problem over a 100 Mbps connection regardless of the number of SNMP helper threads used, unless there are other bandwidth-hungry applications sharing the link.

The above figures assume an average round trip time for an SNMP packet is 10 milliseconds, and the average SNMP packet size is around 125 bytes. This means each SNMP helper thread could transmit 12,500 bytes per second, and retrieve 12,500 bytes per second, which equals 100,000 bits per second. If there are 20 threads, then 20 multiplied by 100,000 equals 2,000,000 bits per second, which is 2 Mbps. For 100 threads, the figure is 10 Mbps. By default, the SNMP helper runs 120 threads.

These estimates assume that every thread in the SNMP helper is in full operation at the same time, which is generally not the case. However, if there is insufficient bandwidth, the UDP packets used to transport SNMP could either be lost, or the packets might queue up in the network and arrive with a delay.

For more information on configuring the SNMP helper, see *IBM Tivoli Network Manager IP Edition Discovery Guide*.

Discovery memory requirements

When discovering very large networks, the discovery process (ncp_disco) and the topology model process (ncp_model) use the most memory. If the network is very large, consider dividing it into multiple domains.

Software requirements

Software requirements vary according to the operating system, products, and features of Network Manager that you want to use.

Requirements for other products

Make sure that you meet the requirements for the products that are integrated with Network Manager.

Extra product requirements

Important: These requirements are in addition to any other hardware, software, installation directory, user or other requirements discussed in the individual product documentation. Ensure that you are familiar with all of the requirements and prerequisites before installing any product.

Tivoli Netcool/OMNIbus

Make sure that Tivoli Netcool/OMNIbus V7.2.1, V7.3, V7.3.1, V7.4, Fix Pack 5 or V8.1 is installed on a server to which Network Manager can connect. If you do not have an installation of Tivoli Netcool/OMNIbus, you must install it. You must download Tivoli Netcool/OMNIbus separately.

The Network Manager installer looks for Tivoli Netcool/OMNIbus version 7.3.1 only. If it does not find the Tivoli Netcool/OMNIbus image (based on image name or part number), it asks for the file location. If you want the installer to install a supported Tivoli Netcool/OMNIbus version other than 7.3.1, then create a subdirectory called `OMNIbus` in the extracted Network Manager installation package, and extract the downloaded Tivoli Netcool/OMNIbus package into this directory.

Restriction: Due to a known issue, the Network Manager 3.9 installer cannot install or configure Tivoli Netcool/OMNIbus 7.4 on Linux and Solaris systems. Due to this issue, the **`ConfigOMNI`** script provided with Network Manager 3.9 cannot configure Tivoli Netcool/OMNIbus 7.4 on Linux and Solaris systems. For more information about this issue and the how to resolve it, see the following troubleshooting technote http://www-01.ibm.com/support/docview.wss?uid=swg21615671.

If you install Tivoli Netcool/OMNIbus not using the Network Manager installer, you must install from a different window to that used to install Network Manager, ensuring that any environment variables are set correctly according to the Tivoli Netcool/OMNIbus documentation.

Restriction: You must install Network Manager 3.9 in a different **directory** to an existing installation of Tivoli Netcool/OMNIbus 7.2.1 or earlier. On Windows, you must install Network Manager 3.9 on a different **server** to an existing installation of Tivoli Netcool/OMNIbus 7.2.1 or earlier.

Restriction: Fix Pack 5 The following restrictions apply to Tivoli Netcool/OMNIbus V8.1:

- You cannot install Tivoli Netcool/OMNIbus V8.1 on the same server as Network Manager.
- You cannot install Tivoli Netcool/OMNIbus V8.1 using the Network Manager installer. If you want to use Tivoli Netcool/OMNIbus V8.1, you must install it on a remote host and connect to it.

Tivoli Netcool/OMNIbus Web GUI

The Tivoli Netcool/OMNIbus Web GUI was known as Netcool/Webtop in versions 2.2 and below. If you install the Web GUI not using the Network Manager installer, you must install from a different window to that used to install Network Manager, ensuring that any environment variables are set correctly according to the Tivoli Netcool/OMNIbus documentation.

Tivoli Common Reporting

Network Manager installs the reports package required for network management reports on the server where the Network Manager GUI components are installed. If the chosen installation location for Network Manager already has existing Tivoli Integrated Portal and Tivoli Common Reporting instances, then Network Manager automatically configures the reports to be used with that Tivoli Common Reporting instance.

If you do not have Tivoli Common Reporting installed when installing Network Manager, you can install Tivoli Common Reporting at a later date and configure the reports then as described in "Configuring reports for existing installations" on page 247.

IBM Tivoli Business Service Manager

You must install IBM Tivoli Business Service Manager from a different window to that used to install Network Manager, ensuring that any environment variables are set correctly according to the IBM Tivoli Business Service Manager documentation.

Previous versions

Install Network Manager 3.9 in a different directory to Network Manager V3.8 or earlier, and Netcool/Webtop V2.1 or earlier.

Related tasks:

"Configuring integrations with other products" on page 155
You can set up Network Manager to work with a number of Tivoli® products. Read about necessary configuration tasks required to set up the available integrations.

Compatibility with other Tivoli products

Network Manager is compatible with other Tivoli products, providing options for integrating with other products to build a solution to address your requirements.

The following table describes the compatibility of Network Manager V3.9 with other Tivoli products.

Table 3. Compatibility of Network Manager V3.9 with other products

Product	Compatible versions
IBM Tivoli Netcool/OMNIbus	7.2.1 7.3 7.3.1 7.4 **Note:** Fix Pack 5 If you want to use Oracle 11 or 12 as the topology database, and you have IBM Tivoli Netcool/OMNIbus installed on the same Solaris server as Network Manager Fixpack 5, you must install or upgrade to IBM Tivoli Netcool/OMNIbus 7.4 before installing FixPack 5. Fix Pack 5 8.1 (remote IBM Tivoli Netcool/OMNIbus only)
Tivoli Netcool/OMNIbus Web GUI	7.3.1 7.4
IBM Tivoli Netcool Configuration Manager	6.3 6.4
Tivoli Integrated Portal	2.1 2.2 **Note:** Fix Pack 5 If FIPS 140-2 compliance is important to you, do not use versions prior to 2.2.0.17. Version 2.2.0.17 of the Tivoli Integrated Portal introduced SHA-2 compliance.

Table 3. Compatibility of Network Manager V3.9 with other products (continued)

Product	Compatible versions
Tivoli Common Reporting	2.1 2.1.1 Fix Pack 5 3.1 **Restriction:** Tivoli Common Reporting 3.1 is available for Netcool Operations Insight users only. **Restriction:** If you want to use the reporting feature and you are installing Network Manager on Red Hat Enterprise Linux 6.0, you must install Tivoli Common Reporting version 2.1 or 2.1.1 on a separate host, as these versions of Tivoli Common Reporting are not supported on Red Hat Enterprise Linux 6.0. You can specify not to install reporting when launching the Network Manager installation process by using the `-DinstallReports=0` option, as described in the installation tasks in "Installing Network Manager" on page 72. **Restriction:** Tivoli Common Reporting version 2.x does not support Internet Explorer 10 or Firefox 24 Extended Support Release (ESR). This means you cannot use the reporting feature if you are using these browser versions for the Network Manager GUI. **Restriction:** Fix Pack 5 Tivoli Common Reporting version 3.1 does not support MySQL.
Tivoli Data Warehouse	2.1
IBM Tivoli Change and Configuration Management Database	7.1.1
IBM Tivoli Application Dependency Discovery Manager	7.2 7.2.1
IBM Systems Director	6.2.1
IBM Tivoli Business Service Manager	4.2.1 6.1 **Note:** Compatibility between Network Manager 3.9 and IBM Tivoli Business Service Manager 4.2.1 is restricted to launch-in-context and DLA export capabilities. For more information, see "Exporting discovery data to CCMDB, TADDM, and TBSM" on page 181, and also refer to the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*.
IBM Tivoli Monitoring	Fix Pack 5 6.2.2 or later.

Supported topology databases

By default, an IBM Informix database is included in the product for storing the topology data. Other database types are supported. If you do not use the default database, use only a supported database.

Important: Apply all the recommended patches to your database.

If you use separate databases for the MIB data and topology data, each database must be of the same type. For example, you cannot use a DB2 database for topology data and an Informix database for MIB data.

The following table lists the supported database types, versions, and editions.

Table 4. Supported database types, versions, and editions

Database type	Version and edition	Notes
IBM DB2	• DB2 V9.1 • DB2 V9.5 • DB2 V9.7 • Fix Pack 4 DB2 V10.1 • Fix Pack 5 DB2 V10.5	When setting up failover, you can configure Network Manager to operate in the DB2 High Availability Disaster Recovery (HADR). **Restriction:** The DB2 database that ships with Network Manager is a limited license version. Depending on your environment, the size of your network, and the amount of data you plan to store, you might need to upgrade your license of DB2. For more information, contact your IBM Sales Representative.
MySQL	• 5.1 • Fix Pack 4 5.5 • Fix Pack 4 5.6	If you use MySQL for the topology database, you can not use Tivoli Common Reporting V3.1 You must use Tivoli Common Reporting V2.1. For upgrades to MySQL 5.5 or MySQL 5.6, apply the fix pack before you upgrade the database. If you do not, errors can occur on the Network Views GUI. (The MYSQL JDBC library that is used in earlier versions that fix pack 4 is not compatible with MySQL 5.5 or MySQL 5.6.) For more information, see the `INSTALL` file that is included in the fix pack.

Table 4. Supported database types, versions, and editions (continued)

Database type	Version and edition	Notes
Oracle	• V11*g* Standard Edition • V11*g* Enterprise Edition • Fix Pack 5 V12c	If you use Oracle V12c, you can not use Tivoli Common Reporting V2.1.1. You must use Tivoli Common Reporting V3.1. Fix Pack 5 When setting up failover, you can configure Network Manager to operate in the Oracle Real Application Clusters (RAC). **Restriction:** Fix Pack 5 The use of Oracle 11 as the topology database is not supported if Network Manager is running on Linux for zSeries and System z.

Table 4. Supported database types, versions, and editions (continued)

Database type	Version and edition	Notes
IBM Informix	• V11.5 Ultimate Edition • V11.5 Ultimate Edition • V11.7 Enterprise Edition • V11.5 Workgroup Edition	The version of Informix that is included in the product differs depending on the product image that you downloaded. The base GA product image includes Informix Workgroup Edition version 11.5 (11.50.xC6). The product image that was released on 14 September 2012 (build level 3.9.0.71) includes Informix Growth Edition 11.7 (11.70.xC5). If you are running the base GA product image, you can upgrade from Informix Workgroup Edition version 11.5 to Informix Growth Edition 11.7. The upgrade is a manual process and differs depending on your operating system. For more information, search for *Upgrading Informix from V11.5 to V11.7* in the *IBM Tivoli Network Manager IP Edition Release Notes* . For more information about installing Informix as a nonroot user, see "Installing Informix as a nonroot user." Linux Informix V11.7 is not supported on SUSE Linux Enterprise Server (SLES) 10. Use Informix V11.5 or another supported database For more information, search for *Installing Informix 11.5 on SuSE Enterprise Linux 10* in the *IBM Tivoli Network Manager IP Edition Release Notes*. AIX Informix V11.5 is not supported on AIX V7.1.

Installing Informix as a nonroot user

To install Informix as part of a nonroot installation, set the permissions of all directories in the Informix path to 775. For example, on a Linux host where the $NCHOME environment variable is set to `/home/IBM/tivoli/`, the Informix path is `/home/IBM/tivoli/platform/linux2x86/users/informix/`. In this example, set the permissions of the following directories to 775:

- `/home/`
- `/home/IBM/`
- `/home/IBM/tivoli/`
- `/home/IBM/tivoli/platform/`

- /home/IBM/tivoli/platform/linux2x86/
- /home/IBM/tivoli/platform/linux2x86/users/
- /home/IBM/tivoli/platform/linux2x86/users/informix/

Related tasks:

"Installing fix packs" on page 125
To obtain the latest fixes, apply fix packs. Fix packs are available for the Network Manager product and also for other products and components such asTivoli Integrated Portal and the Tivoli Netcool/OMNIbus Web GUI. You can download fix packs from IBM Fix Central. Ensure that you keep the fix pack level up to date.

"Setting up a topology database" on page 56
Apart from the default Informix database, you can use a DB2, MySQL, or Oracle database to store your topology. Unless you are installing the default Informix database bundled with Network Manager, you must configure an existing database or install and configure a new one before installing Network Manager.

"Configuring Network Manager to work with DB2 HADR or Oracle RAC" on page 313
You can configure Network Manager core processes to use the DB2 catalog and the Network Manager GUI to operate in the DB2 high availability disaster recovery (HADR) environment. Fix Pack 5 Similarly, you can also configure Network Manager core processes and the Network Manager GUI to operate in the Oracle Real Application Clusters (RAC) environment.

Supported operating systems

Network Manager is supported on various versions of UNIX, Linux, and Windows.

Network Manager V3.9 is supported on the following operating systems at the time of release.

For the most current information about supported operating systems, see the Software Product Compatibility Reports at:

http://www.ibm.com/software/reports/compatibility/clarity/index.html

Important: Ensure that your operating system has all the recommended patches installed, including the latest patch levels.

On Sun Microsystems processors, the following versions are supported:

- Solaris 10 SPARC
- Zones SPARC

On IBM PowerPC-based systems, the following versions are supported:

- AIX 6.1 iSeries and pSeries
- AIX 7.1 iSeries and pSeries

On Intel and Advanced Micro Devices (AMD) x86 processors, the following versions are supported:

- Red Hat Enterprise Linux 5.0 (x86-32, x86-64)
- Red Hat Enterprise Linux 6.0 (x86-32, x86-64)

Restriction: If you want to use the reporting feature and you are installing Network Manager on Red Hat Enterprise Linux 6.0, you must install Tivoli Common Reporting version 2.1 or 2.1.1 on a separate host, as these versions of Tivoli Common Reporting are not supported on Red Hat Enterprise Linux 6.0. You can specify not to install reporting when launching the Network Manager installation process by using the `-DinstallReports=0` option, as described in the installation tasks in "Installing Network Manager" on page 72.
Attention: Make sure you disable Security-Enhanced Linux (SELinux) or set it to permissive in the `selinux` configuration file before attempting to install or use Network Manager. Linux systems running Security-Enhanced Linux (SELinux) are not supported.

- SuSE Linux Enterprise Server (SLES) 10.0 (x86-32, x86-64)
- SuSE Linux Enterprise Server (SLES) 11.0 (x86-32, x86-64)

Note: Network Manager does not support SuSE Linux Enterprise Server (SLES) 11.0 SP2 (for details, see http://www-01.ibm.com/support/docview.wss?uid=swg21619336).

Note: Fix Pack 4 Network Manager supports SuSE Linux Enterprise (SLES) 11.0 SP2 and SP3.

- SuSE Linux Enterprise Desktop (SLED) 11 (x86-64)
- Windows Server 2008 (R1) Standard Edition (x86-32, x86-64)
- Windows Server 2008 (R2) Standard Edition (x86-64)
- Windows Server 2008 (R1) Enterprise Edition (x86-32, x86-64)
- Windows Server 2008 (R1) Enterprise Edition (x86-64)
- Windows Server 2008 (R2) Enterprise Edition (x86-64)
- Windows Server 2008 (R2) Datacenter Edition (x86-64)

On IBM System z mainframes, the following versions are supported:

- Red Hat Enterprise Linux 5.0 (zSeries and System z®)
- Red Hat Enterprise Linux 6.0 (zSeries and System z)

Restriction: If you want to use the reporting feature and you are installing Network Manager on Red Hat Enterprise Linux 6.0, you must install Tivoli Common Reporting version 2.1 or 2.1.1 on a separate host, as these versions of Tivoli Common Reporting are not supported on Red Hat Enterprise Linux 6.0. You can specify not to install reporting when launching the Network Manager installation process by using the `-DinstallReports=0` option, as described in the installation tasks in "Installing Network Manager" on page 72.
Attention: Make sure you disable Security-Enhanced Linux (SELinux) or set it to permissive in the `selinux` configuration file before attempting to install or use Network Manager. Linux systems running Security-Enhanced Linux (SELinux) are not supported.

- SuSE Linux Enterprise Server (SLES) 10.0 (zSeries and System z)
- SuSE Linux Enterprise Server (SLES) 11.0 (zSeries and System z)

The following hypervisor and operating system combinations are supported:

- Fix Pack 5 Kernel-Based Virtualization is supported on all supported versions of SUSE Linux
- IBM PowerVM® Hypervisor (LPAR, DPAR, Micro-Partition) any supported version: on AIX

- IBM PR/SM™ any version: SLES and RHEL environments
- IBM z/VM® 6.1: SLES and RHEL environments
- VMware ESX 3.5: SLES, RHEL, and Windows 2008 Enterprise Edition and Standard Edition
- VMware ESX and ESXi 3.5, 4.0, 4.1, and 5.0: SLES, RHEL, and Windows 2008 Enterprise Edition and Standard Edition
- Sun and Oracle Logical Domains (LDoms) any version: Solaris SPARC

Restriction:

- Linux systems running AppArmor are not supported. Disable AppArmor to allow the installation to continue.
- Linux systems running Security-Enhanced Linux (SELinux) are not supported. Disable SELinux when installing and using Network Manager.

Additional requirements for UNIX operating systems

If you are installing on a flavour of UNIX that gives you a choice of whether to install Korn shell (ksh), for example, SUSE Enterprise Linux, you must ensure that Korn shell is installed before running the Network Manager installer.

Uninstall any NFS (Network File System) mounts that are not accessible before you run the installer. To check for inaccessible NFS mounts, run the following command:

```
df -kP
```

If the command runs successfully, there are no inaccessible NFS mounts.

Additional requirements for AIX

If you are installing Network Manager on AIX operating systems, make sure you have the X11 filesets, including the `X11.apps.xterm` fileset, installed before starting the Network Manager installation.

Additional requirements for Red Hat Enterprise Linux 6.0 on zSeries and System z

If you are installing RHEL 6.0 on zSeries and System z systems, make sure you have the following prerequisites covered:

- Ensure that Korn shell (ksh) is installed before running the Network Manager installer. The ksh executable is required in the `/bin` directory for Network Manager scripts, and in the `/usr/bin` directory for the Informix database.
- Ensure you have the 32-bit libstdc++.so.6.0.8 library in the `/usr/lib` directory.
- If you use Tivoli Netcool/OMNIbus, ensure you have the 32-bit RPMs required, see section *Prerequisites for operating systems* in the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* .

Additional requirements for Solaris

If you are installing Network Manager on Solaris operating systems, you must install the SUNWsprot package first.

Additional requirements for Tivoli Common Reporting on Linux and Linux on System z

If you are installing Network Manager on Linux or zLinux operating systems with an Informix database on zLinux, or with an Informix or MySQL database on Linux, you must ensure you have a 32 bit unixODBC RPM available on your system where you are installing GUI components before the installation.

- On all versions of Linux, make sure you have the `libXm.so.3` or later (available from the openmotif RPM 22 or later) available on your system before the installation. For versions of `libXm.so.x` later than `libXm.so.3`, make a symbolic link from the later version to `libXm.so.3`, using a command similar to the following example: **`ln -s /usr/lib/libXm.so.4 libXm.so.3`**.
- On Red Hat Enterprise Linux systems, make sure you have the `unixODBC-2.2.x.x` or higher RPM available on your system before the installation.
- On SuSE Linux Enterprise Server (SLES) systems, make sure you have the `unixODBC-2.2.X.X` or higher RPM available on your system before the installation.

Important:

Some versions of unixODBC define the main library at `/usr/lib/` as `libodbcinst.so.1`. The main library must be defined as `/usr/lib/libodbcinst.so`. Create a symbolic link if necessary.

```
ln -s /usr/lib/libodbcinst.so.x /usr/lib/libodbcinst.so
```

Restriction: You cannot use Tivoli Common Reporting with MySQL on zLinux.

For detailed information on software requirements for Tivoli Common Reporting, see the Tivoli Common Reporting information center at the following URL: http://www-01.ibm.com/support/knowledgecenter/SSH2DF_2.1.1/ctcr_prodoverview.html

Restriction: If you want to use the reporting feature and you are installing Network Manager on Red Hat Enterprise Linux 6.0, you must install Tivoli Common Reporting version 2.1 or 2.1.1 on a separate host, as these versions of Tivoli Common Reporting are not supported on Red Hat Enterprise Linux 6.0. You can specify not to install reporting when launching the Network Manager installation process by using the `-DinstallReports=0` option, as described in the installation tasks in "Installing Network Manager" on page 72.

Additional requirements for Red Hat Enterprise Linux AS, ES, and WS 5

If installing Network Manager on Red Hat Enterprise Linux AS, ES, or WS 5, you must ensure that the following RPMs are available on your system before the installation:

- `compat-libstdc++-33-3.2.3-61`
- `libXp-1.0.0-8`
- `openmotif22-2.2.3-18`
- `libXmu-1.0.2-5`
- `libXpm-3.5.5-3`
- `compat-libstdc++-296-2.96-138`

These files should be available on the installation CDs for the operating system.

For more information about obtaining packages, go to the IBM WebSphere® Application Server Information Center at http://www-01.ibm.com/support/knowledgecenter/SSAW57_6.1.0/as_ditamaps/welcome_nd.html, and search for the package name.

Additional requirements for Linux on System z

If you are using Oracle 12c on zLinux, ensure you have the following library installed: `libaio.so.1`.

Additional requirements for SuSE Linux Enterprise Server (SLES)

If installing Network Manager on SLES, you must ensure that the following RPMs are available on your system before the installation:

- `libstdc++33.rpm (formerly called compat-libstdc++-5.0.7-22.2)`
- `openmotif-libs-2.2.4-21.17`
- `openmotif-devel-32bit-2.2.4-21.17`
- `openmotif-2.2.4-21.17`
- `openmotif-libs-32bit-2.2.4-21.17`
- `openmotif21-libs-32bit-2.1.30MLI4-143.9`
- `openmotif-devel-2.2.4-21.17`

For more information about obtaining packages, go to the IBM WebSphere Application Server Information Center at http://www-01.ibm.com/support/knowledgecenter/SSAW57_6.1.0/as_ditamaps/welcome_nd.html, and search for the package name.

Note: SLES 10 is not compatible with Informix 11.7. See the Release Notes for your version of Network Manager for more details of which topology database to install and how to obtain and install it.

Additional requirement for Linux systems

On both Intel -based Linux and on IBM System z installations, make sure you have both the 32 bit and 64 bit versions of the pam-1.1.1-10.el6.*system* packages installed. For example, for System z installations, ensure you have both of the following packages:

- `pam-1.1.1-10.el6.s390`
- `pam-1.1.1-10.el6.s390x`

Supported browsers

Ensure that clients use one of the supported web browsers. If your browser is not supported, a web application might hang or crash.

The following table describes the supported browsers and the Java Runtime Environment versions for each client operating system. Certain browsers work only with specific levels of Tivoli Integrated Portal V2.2. For more information, search for *Tivoli Integrated Portal compatibility* in the *IBM Tivoli Network Manager IP Edition Release Notes*.

Table 5. Supported browsers for client operating systems

Browser	Client operating system	JRE version
Internet Explorer 7.0 Internet Explorer 8.0 Internet Explorer 9.0. Supported in fix pack 2 and later versions, including the full product image refresh (build level 3.9.0.71). Requires Tivoli Integrated Portal V2.2.0.5 or later. Fix Pack 4 Internet Explorer 10. Requires Tivoli Integrated Portal V2.2.0.13 or later and the Tivoli Netcool/OMNIbus Web GUI V7.4.0.2 or later. **Restriction:** Tivoli Common Reporting version 2.x does not support Internet Explorer 10. Consequently, you cannot use the reporting feature if you are using Internet Explorer 10 for the Network Manager GUI.	Windows XP Service Pack 3 Windows 7 Enterprise Windows Vista Enterprise Windows Server 2008 (R1) Standard Edition Windows Server 2008 (R1) Enterprise Edition Windows Server 2008 (R2) Datacenter Edition Windows Server 2008 (R2) Enterprise Edition Windows Server 2008 (R2) Standard Edition	Oracle JRE 1.6 Fix Pack 4 Oracle JRE 1.7 Fix Pack 5 Oracle JRE 1.8 Fix Pack 4 Ensure that the JRE version is compliant with the Oracle JRE Security Baseline. For more information, see *Deploying Java Applets With Family JRE Versions in Java Plug-in for Internet Explorer* at http://www.oracle.com/technetwork/java/javase/family-clsid-140615.html.

Table 5. Supported browsers for client operating systems (continued)

Browser	Client operating system	JRE version
Mozilla Firefox 3.6.x Firefox 10 Extended Support Release (ESR). Supported in fix pack 2 and later versions, including the full product image refresh (build level 3.9.0.71). Requires Tivoli Integrated Portal V2.2.0.7 or later. Fix Pack 3 Firefox 17 ESR. Requires Tivoli Integrated Portal V2.2.0.11 or later. Fix Pack 4 Firefox 24 ESR, Requires Tivoli Integrated Portal V2.2.0.13 or later and the Tivoli Netcool/OMNIbus Web GUI V7.4.0.2 or later. **Restriction:** Tivoli Common Reporting version 2.x does not support Firefox 24 ESR. Consequently, you cannot use the reporting feature if you are using Firefox 24 ESR for the Network Manager GUI. Fix Pack 5 Internet Explorer 11	Red Hat Enterprise Linux Desktop 5.0 Red Hat Enterprise Linux (RHEL) 5.0 SuSE Linux Enterprise Desktop (SLED) 10 and 11 SuSE Linux Enterprise Server (SLES) 10 and 11 Solaris 9, 10, and Zones SPARC Windows XP Service Pack 3 Windows 7 Enterprise Windows Vista Enterprise Windows Server 2008 (R1) Standard Edition Windows Server 2008 (R1) Enterprise Edition Windows Server 2008 (R2) Datacenter Edition Windows Server 2008 (R2) Enterprise Edition Windows Server 2008 (R2) Standard Edition VMWare ESX Server 3.5	Oracle JRE 1.6 Fix Pack 4 Oracle JRE 1.7 Fix Pack 5 Oracle JRE 1.8 Ensure that the JRE version is compliant with the Oracle JRE Security Baseline. **Tip:** UNIX Linux Ensure that the Java™ plug-in is correctly installed, and that all required symbolic links are made. For more information, see the Firefox documentation.

Supported browsers for the installer launchpad

To run the installer launchpad, ensure that a supported browser is installed. The supported browsers for the installer launchpad are not necessarily the same as the supported browsers for the web applications.

The supported browsers for the installer launchpad are described in the following table.

Restriction: Linux On Red Hat Enterprise Linux and SUSE Enterprise Linux (S/390 and S/390x only), only Firefox 2.x is supported.

Table 6. Supported browsers for the installer launchpad

Browser	Version
Firefox	2.0 and above
Mozilla	1.7 and above
Internet Explorer	6.0
SeaMonkey	1.1.4 and above

Operating system tools

Because the stability of the installation process depends on the stability of the Operating System (OS) tools, ensure that the OS versions of standard tools are included in your path before non-OS versions of the same tools (for example, GNU utilities).

Domain Name Service (DNS) requirements

Ensure that your servers have DNS set up correctly before installing Network Manager.

Domain names

Ensure that all servers onto which you want to install any components of Network Manager have the host name defined as a fully qualified domain name (FQDN). Incomplete or incorrect DNS setup can cause problems installing or using Network Manager.

UNIX On UNIX platforms, the host name is defined in the `/etc/hosts` file.

Windows On Windows, the host name is defined in the `%WinDir%\system32\drivers\etc\hosts` file.

On the machine where you install Network Manager components, ensure you include the IP address, FQDN, and short name in the `/etc/hosts` file before installing Network Manager, and ensure that the FQDN and short name only resolve to the same IP address and reverse resolve to the FQDN or short name.

The format is *`IP address FQDN shortname`*. For example, add a line similar to the following to `/etc/hosts`:
`9.10.11.12 yourserver.domainname.com yourserver`

This ensures that the FQDN is set as the Hostname entry when Network Manager is installed.

Restriction: Do not use underscore when specifying host names. Use of underscores as part of a host name causes the installation of the Tivoli Integrated Portal to fail.

UNIX user restrictions

On UNIX operating systems, if you have installed other Tivoli network management products on a particular server, you must install Network Manager into the same directory as the same user.

If you install the Network Manager Web applications as the root user, Network Manager will not integrate with IBM Tivoli Business Service Manager. If you want to use Network Manager with TBSM, you must create a different user to install and manage all Tivoli products on this server.

If you install Network Manager as a non-root user, you must perform extra post-installation configuration steps in order to run the core components as the root user.

If you install Network Manager as a non-root user, you must install all future Tivoli products as the same user.

If you install and run Network Manager as a non-root user, then it is not possible to have two versions of Network Manager installed on the same server.

Related tasks:

"Configuring root/non-root permissions" on page 221
On UNIX, if you installed Network Manager as a non-root user, you must perform additional configuration.

Windows user restrictions

On Windows operating systems, all Tivoli network management products must be installed into the same installation directory by the same user.

You can install Network Manager as the administrator user.

Restriction: You must be the Administrator user to install on Windows Server 2008 systems.

You also need write permission to the installation directory and administrative privileges on the workstation.

Requirements for Solaris zones

If you are installing Network Manager on servers that are running Solaris 10 zones, you might need to perform extra configuration tasks.

Installing in global zones

There are no special requirements for installing Network Manager in global zones.

Installing in local zones

If you are planning to install in a local zone, you must first configure the local zone to enable Network Manager to build its own raw packets. A default local zone does not allow applications running on it to build its own raw packets.

To configure Network Manager to build its own raw packets, configure your zone to include the net-rawaccess privilege, as described in the following steps.

1. On the local zone enter the following commands:

   ```
   zonecfg -z zone_name
   zonecfg:zone_name> set limitpriv=default,net_rawaccess
   zonecfg:zone_name> verify
   zonecfg:zone_name> commit
   zonecfg:zone_name> exit
   ```

   Where *zone_name* is the name of your local zone.
2. Shut down and reboot your zone in order to pick up the new settings.

   ```
   zlogin zone_name shutdown
   zoneadm -z zone_name boot
   ```
3. Check that the privilege has been successfully added using the `ppriv` command. The following example shows sample output from this command with the net-rawaccess privilege added.

   ```
   # ppriv $$
   4547:   -sh
   flags =

   E: basic,contract_event,contract_observer,file_chown,
   file_chown_self,file_dac_execute,file_dac_read,
   ```

```
file_dac_search,file_dac_write,file_owner,file_setid,
ipc_dac_read,ipc_dac_write,ipc_owner,
net_bindmlp,net_icmpaccess,net_mac_aware,net_privaddr,
net_rawaccess,proc_audit,proc_chroot,proc_owner,
proc_setid,proc_taskid,sys_acct,sys_admin,sys_audit,
sys_mount,sys_nfs,sys_resource

I: basic
P: basic,contract_event,contract_observer,file_chown,
file_chown_self,file_dac_execute,file_dac_read,
file_dac_search,file_dac_write,file_owner,file_setid,
ipc_dac_read,ipc_dac_write,ipc_owner,net_bindmlp,
net_icmpaccess,net_mac_aware,net_privaddr,
net_rawaccess,proc_audit,proc_chroot,proc_owner,
proc_setid,proc_taskid,sys_acct,sys_admin,sys_audit,
sys_mount,sys_nfs,sys_resource

L: basic,contract_event,contract_observer,file_chown,
file_chown_self,file_dac_execute,file_dac_read,
file_dac_search,file_dac_write,file_owner,file_setid,
ipc_dac_read,ipc_dac_write,ipc_owner,net_bindmlp,
net_icmpaccess,net_mac_aware,net_privaddr,
net_rawaccess,proc_audit,proc_chroot,proc_owner,
proc_setid,proc_taskid,sys_acct,sys_admin,sys_audit,
sys_mount,sys_nfs,sys_resource
```

Full-root zones and sparse zones are variants of the local zone. The following sections detail requirements for these types of zone.

Installing in full-root zones

There are no special requirements for installing Network Manager in full-root zones.

Installing in sparse zones

In a default installation, the Tivoli Integrated Portal is automatically installed. In a custom installation, you can choose whether or not to install the Tivoli Integrated Portal. When the Tivoli Integrated Portal is installed, some files used by a component called the Deployment Engine are placed in the `/usr/ibm/common/acsi` directory. In sparse zones, the root user does not have write access to the `/usr` directory, which causes installation of the Tivoli Integrated Portal to fail.

If you want to install the Tivoli Integrated Portal as the root user in a sparse zone, you cannot use the installer launchpad. You must start the installation from the command line and override the default location of the Deployment Engine using the following parameter:

```
-DIAGLOBAL_DE_INSTALL_LOCATION=/opt/ibm/common/acsi
```

Where `/opt/ibm/common/acsi` is any directory to which the root user has write access.

Sample commands to install as root in a sparse zone

Use commands similar to the following commands to install as root in a sparse zone.

GUI mode

```
./install.sh -DIAGLOBAL_DE_INSTALL_LOCATION=/opt/ibm/common/acsi –i
gui
```

Console mode

```
./install.sh -DIAGLOBAL_DE_INSTALL_LOCATION=/opt/ibm/common/acsi –i
console
```

Silent mode

Edit the sample response file, and add the line `IAGLOBAL_DE_INSTALL_LOCATION=/opt/ibm/common/acsi` after the line: `IAGLOBAL_INSTALL_LOCATION_SELECTION=create`.

IBM Tivoli License Compliance Manager

Network Manager is compatible with IBM Tivoli License Compliance Manager. IBM Tivoli License Compliance Manager allows you to monitor and manage your IBM software usage and license compliance.

Network Manager does not require a license key in order to run. IBM Tivoli License Compliance Manager is available separately to Network Manager.

Windows Installer requirements

You must ensure that you have the correct version of Windows Installer for your version of Windows.

For 64 bit Windows

Before installing on 64 bit Windows 2008 Server, you must install Windows Installer version 4.5.

By default, Windows Installer version 4.0 is supplied with Windows 2008 Server. Network Manager does not install correctly with Windows Installer version 4.0 on 64 bit systems.

To check which version of Windows Installer is installed, run the **msiexec -help** command at the command prompt. You can download Windows Installer version 4.5 by searching for "Windows Installer 4.5" from the following URL:

http://www.microsoft.com/downloads

For other versions of Windows

For all versions of Windows except 64 bit Windows 2008 Server, you must ensure that Windows Installer version 3.1 or later is installed before installing Network Manager.

Installation directory requirements

The directory where you install Network Manager must fulfill certain requirements.

Requirements on all operating systems

By default, the installer places Tivoli Network Management products into the same directory.

The full path to the installation directory must contain only alphanumeric characters (A-Z, a-z, 0-9), dashes, underscores, periods, colons, slashes, or spaces.

Requirements on UNIX operating systems

The user installing Network Manager must have write permission to the installation directory, and if different, the `/opt` directory.

Requirements on Windows

On Windows, you cannot install to a mapped network drive. You can only install to a physical disk or low level partition of a physical disk that is visible to all Windows users.

If you want to use an Oracle database for the topology data, you must install Network Manager in a location that does not contain a "(" character. If you install Network Manager in a location that contains a "(" character, you must download a patch from Oracle as described in Oracle issue #3807408, and then configure and populate the NCIM topology database manually after installing the Oracle patch.

Requirements for the installer

The installer installs files in the main installation directory that you choose during the installation process. It also installs files in other directories, depending on the operating system being installed on and the user performing the installation. Review the default directory structure and ensure that the user performing installation has write access to the relevant directories.

Related reference:

"Default directory structure" on page 333
Use this information to understand the Network Manager directory structure.

File handle requirements

On UNIX and Linux operating systems, ensure that enough file handles are allowed.

If you are installing Network Manager on a UNIX or Linux operating system, ensure that the number of open files for processes is set to an appropriate value in all environments for the user who runs Network Manager. Set the number of open files to at least 512 on the server where the core components are installed, and 8192 for the GUI server. You can check this value by running the following command as the user who is running Network Manager: `ulimit -n`

If this value is too low, contact your system administrator to increase the value for your user.

The following are examples of using the command to increase the value:

AIX `chuser nofiles=8192 user_id`

Solaris, Linux, and Linux on System z

```
ulimit -n 8192
```

Set the number of processes per user set a minimum of 1024. You can check this value by using the following command: `ulimit -u`

Note: The 1024 value is a minimum one and this value might need to be adjusted for your environment based on your needs.

Requirements for charting

Charting is an optional component that enables you to display charts from supported Tivoli products and charts that were created with the Business Intelligence and Reporting Tools Designer.

The Charting option also installs the ITM Web Service with the Tivoli Integrated Portal Server. When Tivoli Management Services is part of your networked enterprise, the ITM Web Service is used to query attribute values collected by your IBM Tivoli Monitoring or OMEGAMON® XE products and retrieve them to chart portlets in the console.

Important: If your installation will use the ITM Web Service, be sure to read "Configuring SSO between Charting and Tivoli Monitoring" on page 344 before installing Tivoli Integrated Portal.

Your product may already come with predefined charts or perhaps the chart format is not appropriate for your product. In either case, you will not see the Charting option during an advanced installation if it is not offered with your product.

Secure Web service connection

Charting supports the HTTPS protocol for confidentiality. When data requests are made from the portal to the IBM Tivoli Monitoring application server (Tivoli Enterprise Portal Server) the credentials of the logged-in user are passed to the Web service for authentication and authorization. When requests are made to retrieve Tivoli Monitoring data into a chart portlet, the user name and password that were provided at installation time are passed to the Tivoli Enterprise Portal Server, and an LTPA token is passed to the backend Web service.

To participate in this secure connection, the ITM Web Service must be installed and run on the same Tivoli Integrated Portal Server instance.

Chapter 2. Installing

Use this information to plan and perform an installation of Network Manager.

After installation, you might need to perform configuration tasks.

Preparing to install

Before you begin installing Network Manager, you must obtain and extract the installation package, and depending on your installation, complete additional tasks.

If you want to integrate Network Manager with an existing installation of Tivoli Netcool/OMNIbus on a different server, you must configure the Tivoli Netcool/OMNIbus installation before installing Network Manager.

You must complete additional tasks before installing if you want to install Network Manager on an AIX operating system.

Informix is the default topology database provided with Network Manager, and you can use an existing Informix database also. If you want to use a DB2, MySQL, Oracle, or a remote Informix database for topology data, you must complete additional tasks after extracting the installation package and before installing Network Manager.

Click the following link to retrieve technotes about known installation issues in version 3.9 of Network Manager:
http://www-01.ibm.com/support/search.wss?word=ow
&wfield=install+installation+installing&rs=3118&tc=SSSHRK&atrn=SWVersion
&atrv=3.9&ibm-go.x=18&ibm-go.y=12

Restriction: Any passwords you choose for Network Manager must conform to the password policies of the server or system environment.

Configuring an existing Tivoli Netcool/OMNIbus installation

If you want to integrate Network Manager with an existing installation of Tivoli Netcool/OMNIbus on a different server, or with an existing installation of Tivoli Netcool/OMNIbus prior to version 7.3.1 on the same server, you must configure the Tivoli Netcool/OMNIbus installation before installing Network Manager.

If you are installing Tivoli Netcool/OMNIbus 7.3.1 as part of the Network Manager installation, you do not need to do this task.

If you want to integrate Network Manager with an existing installation of Tivoli Netcool/OMNIbus 7.3.1 on the same server, you do not need to do this task.

Attention: Using the Network Manager installer to configure an existing Tivoli Netcool/OMNIbus also installs the SNMP probe and the Netcool/OMNIbus Knowledge Library. If you do not want to overwrite your existing SNMP probe and Netcool/OMNIbus Knowledge Library customizations, you must select **Do not install or configure Tivoli Netcool/OMNIbus at this time** when prompted in panel **Select Components to Install**, under **Tivoli Netcool/OMNIbus**. After the installation of Network Manager, copy the installation package to the server where your existing Tivoli Netcool/OMNIbus installation is, and run the **ConfigOMNI** script to configure your Tivoli Netcool/OMNIbus, but ensure you do not select options to configure the SNMP probe or the Netcool/OMNIbus Knowledge Library.

Restriction: You must install Network Manager 3.9 in a different **directory** to an existing installation of Tivoli Netcool/OMNIbus 7.2.1 or earlier. On Windows, you must install Network Manager 3.9 on a different **server** to an existing installation of Tivoli Netcool/OMNIbus 7.2.1 or earlier.

Restriction: Due to a known issue, the Network Manager 3.9 installer cannot install or configure Tivoli Netcool/OMNIbus 7.4 on Linux and Solaris systems. Due to this issue, the **ConfigOMNI** script provided with Network Manager 3.9 cannot configure Tivoli Netcool/OMNIbus 7.4 on Linux and Solaris systems. For more information about this issue and the how to resolve it, see the following troubleshooting technote http://www-01.ibm.com/support/docview.wss?uid=swg21615671.

To configure an existing Tivoli Netcool/OMNIbus for use with Network Manager, complete the following tasks.

1. Make sure you have an existing Tivoli Netcool/OMNIbus ObjectServer installation to configure.
2. If your Tivoli Netcool/OMNIbus installation is version 7.2.1, ensure that you have installed the Tivoli Netcool/OMNIbus 7.2.1 libncrypt patch (available from the Network Manager 3.9 installation media).
3. Download and uncompress the Network Manager installation package on the server that contains the Tivoli Netcool/OMNIbus installation.
4. If you are configuring Tivoli Netcool/OMNIbus V7.2.1, V7.3, or V7.3.1, download the installation package for the appropriate version of the SNMP Probe (also known as the MTTRAPD Probe).
5. Start the configuration script either from the installer launchpad or the command line.

Option	Description
Run the script from the launchpad.	1. Depending on your operating system, start the launchpad using the **launchpad.sh** script on UNIX or the **launchpad.exe** executable on Windows. 2. Go to **Preinstallation and Migration** and expand the **Configure an existing Netcool/OMNIbus installation** section. 3. Click **Configure existing Netcool/OMNIbus installation**. 4. Enter the access credentials for the ObjectServer you want to configure.

Option	Description
Run the script from the scripts directory of the installation package.	• Depending on your operating system, run the `ConfigOMNI.sh` script on UNIX or the `ConfigOMNI.bat` script on Windows. • Enter the access credentials for the ObjectServer you want to configure.

If you install Tivoli Netcool/OMNIbus as part of the Network Manager installation, the installer adds the itnmadmin and itnmuser users to the ObjectServer, turns on AES encryption, turns on process control for the Objectserver, and installs the SNMP Probe and the Netcool/OMNIbus Knowledge Library.

If you use the **ConfigOMNI** utility (from launchpad or from command line), you can choose which options are configured using the appropriate command line arguments. If you are configuring Tivoli Netcool/OMNIbus V7.2.1, V7.3, or V7.3.1, supply the installation package for the appropriate version of the SNMP Probe using the -m command line argument.

6. Required: After you configure Tivoli Netcool/OMNIbus, install Network Manager.
   a. During the installation, select the option to use an existing installation of Tivoli Netcool/OMNIbus.
   b. Provide the details of the ObjectServer that you configured using the script.
7. Optional: If you have Tivoli Netcool/OMNIbus V7.2.1 or V7.3, the `nco_p_ncpmonitor` process might fail due to missing NmosEventMap and BSM_Identity fields in the ObjectServer. Make sure your ObjectServer is running and run the **ncp_configure_omnibus.sql** script as described in "Adding event fields" on page 160.

ConfigOMNI command-line options

Use the **ConfigOMNI** script, with optional advanced arguments, to configure Tivoli Netcool/OMNIbus for use with Network Manager before installing Network Manager.

The **ConfigOMNI** script is started by using the following command line; optional arguments are shown enclosed in square brackets.

```
ConfigOMNI -o name -p password [ -a ] [ -c ] [ -e ] [ -h directory ] [ -k package ]
 [ -m package ] [ -n portnumber ] [ -u password ]
```

The following example runs the script on ObjectServer DIAMOND with the administrative password p3w0d. If the ObjectServer DIAMOND does not already exist, it is created. Using the appropriate options, you can configure the script to add the itnmadmin and itnmuser users to the ObjectServer, turn on AES encryption, turn on process control for the Objectserver, and install the SNMP Probe and the Netcool/OMNIbus Knowledge Library.

Note: The **ConfigOMNI** script does not perform any configuration unless the appropriate command line options are provided, or you respond to the appropriate questions.

```
ConfigOMNI -o DIAMOND -p p3w0d
```

Note: The **ConfigOMNI** script is intended for use when first setting up an ObjectServer. If the **ConfigOMNI** script is run multiple times on the same host, it might be necessary to edit the following files:

1. `nco_p_mttrapd.props` file to remove duplicate `Server`, `ServerBackup`, `RulesFile`, `MIBFile` and `QuietOutput` properties at the end of the file.
2. `nco_pa.conf` file to change any duplicate `nco_process` names, as the script will always provide entries with the names `MasterObjectServer` and `Mttrapd`. For more information on how to edit this file, see the Tivoli Netcool/OMNIbus documentation at http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html, and search for the topic on "Defining processes in the process agent configuration file".

The following table describes the command-line options for the **ConfigOMNI** script.

Table 7. ConfigOMNI command-line options

Command-line options	Description
`-o` *name*	The name of the ObjectServer that you want to create or configure.
`-p` *password*	The administrative password of the ObjectServer that you want to create or configure.
`-a`	Optional. Runs the script in interactive mode, which prompts for all information.
`-c`	Optional. Configures the ObjectServer to run under Tivoli Netcool/OMNIbus process control. This is necessary for the **itnm_start**, **itnm_stop**, and **itnm_status** scripts to function correctly with the ObjectServer.
`-e`	Optional. Set AES encryption for the ObjectServer password.
`-h` *directory*	Optional. The directory containing the Tivoli Netcool/OMNIbus installation (OMNIHOME).
`-k` *package*	Optional. Install Netcool/OMNIbus Knowledge Library from this package. You must specify the path to the package if it is not in the current directory.
`-m` *package*	Optional. Install the SNMP Probe from this package. You must specify the path to the package if it is not in the current directory.
`-n` *portnumber*	Optional. The port number of the ObjectServer that you want to create or configure.
`-u` *password*	Optional. Create the itnmadmin and itnmuser users in the ObjectServer.

Uncompressing the installation file

If you have downloaded the installation file, you must uncompress the installation package before installing the product.

To uncompress the installation file, perform the following steps:

Uncompress the file.

- UNIX Type the following command: `gunzip -d < installation_file.tar.gz | tar xvf -`
- Windows Right-click on the archive file and uncompress it using any installed uncompression utility.

Checking system prerequisites

The product launchpad includes a prerequisite checker that you can use to verify that a computer is suitable for installing the Network Manager product or individual components of the product. Alternatively, you can download and use IBM Prerequisite Scanner, which is a separate utility for checking systems.

IBM Prerequisite Scanner V1.2.0.10 supports Network Manager V3.9. IBM Prerequisite Scanner is a stand-alone prerequisite checking tool that analyzes system environments before the installation or upgrade of a Tivoli product or IBM solution. IBM Prerequisite Scanner is not included in the Network Manager product. It can be downloaded from IBM Fix Central. You can use IBM Prerequisite Scanner as an alternative to the prerequisite checking functions in the Network Manager installer and launchpad. It is useful on computers that host more than one product or a solution because it can assess the suitability of the computer for multiple products. For more information about how to download and run the tool, and a list of supported products, see http://www-01.ibm.com/support/docview.wss?uid=swg24031503.

To use the launchpad, install a browser that supports the launchpad. Also, download and decompress the installation package.

To run the launchpad and check that suitability of a computer for installing Network Manager:

1. Start the launchpad by running the **launchpad** utility.
2. Click **Prerequisite Information** and type the installation path in the **Installation Location** field.
3. Select the components for which you want to check and click **Check System Prerequisites**.

The results of the check are displayed and indicate whether the computer is suitable for installing your choice of components.

Related reference:

"Supported browsers for the installer launchpad" on page 43
To run the installer launchpad, ensure that a supported browser is installed. The supported browsers for the installer launchpad are not necessarily the same as the supported browsers for the web applications.

Setting up a topology database

Apart from the default Informix database, you can use a DB2, MySQL, or Oracle database to store your topology. Unless you are installing the default Informix database bundled with Network Manager, you must configure an existing database or install and configure a new one before installing Network Manager.

You have the following options to set up a database for your topology:

- You can install and configure the default Informix database bundled with Network Manager and set it up using the Network Manager installer. In this case, you do not need to follow any of the database setup tasks before installing Network Manager. You can start the installer and select the options for setting up a new Informix database.
- If you want to use an existing Informix database on either a local or a remote host, you must configure it before installing Network Manager as described in the following tasks that discuss configuring existing Informix databases on your platform.
- If you want to use a DB2, MySQL, or Oracle database, you must follow the setup tasks for the appropriate database on your platform. The installation and configuration process is different for each type of database and each operating system.

Note: UNIX Linux To install Informix as part of a nonroot installation, set the permissions of all directories in the Informix path to 775. For example, on a Linux host where the $NCHOME environment variable is set to `/home/IBM/tivoli/`, the Informix path is `/home/IBM/tivoli/platform/linux2x86/users/informix/`. In this example, set the permissions of the following directories to 775:

- `/home/`
- `/home/IBM/`
- `/home/IBM/tivoli/`
- `/home/IBM/tivoli/platform/`
- `/home/IBM/tivoli/platform/linux2x86/`
- `/home/IBM/tivoli/platform/linux2x86/users/`
- `/home/IBM/tivoli/platform/linux2x86/users/informix/`

You must configure databases for Network Manager after you have uncompressed the Network Manager installation package, and before you start the product installation. For information about setting up your database for an existing Network Manager installation, see the tasks about creating topology database schemas in the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Important: Apply all the recommended patches to your database.

Related tasks:

"Configuring NCIM for Tivoli Common Reporting" on page 256
If you want to use Informix, MySQL, or Oracle as the NCIM database, you must configure the databases before you can use Tivoli Common Reporting reports.

Related reference:

"Supported topology databases" on page 34
By default, an IBM Informix database is included in the product for storing the topology data. Other database types are supported. If you do not use the default database, use only a supported database.

Configuring an existing Informix database on UNIX

To use an existing Informix database as the topology database on UNIX, you must configure an instance, prepare a dbspace, and create a database before Network Manager is installed.

Note: You only need to follow these steps if you want to use an existing local or remote Informix database for your Network Manager installation. If you want to install and set up a new Informix database on either a local or remote host for Network Manager, you can use the Informix bundled with Network Manager and set it up using the Network Manager installer.

The database is created by scripts that are contained in the `/PrecisionIP/scripts` directory of the extracted installation image. You must have uncompressed the installation package before you configure your existing Informix database.

The Informix environment must be set up as the Informix administrative user on the server hosting Informix. If the host is on a remote server, then copy the database creation scripts to the remote server.

During installation of Network Manager, the NCIM topology database is installed on the Informix database that you create.

1. Go to the host where you have your existing Informix installed.
2. Use the Informix `onspaces` command-line utility to create a dbspace to allocate the necessary disk space for the NCIM database tables. You can create the dbspace anywhere on your file system, provided there is sufficient disk space in that location for the dbspace to grow as the database grows in size.
   a. Create two empty files and name these files as follows: *ncimdbspace*, to hold the normal database tables, and *ncimsbspace*, to hold database tables containing BLOBs. Ensure that this file is readable and writable by the informix user and the informix group. To do this on UNIX, set a filemask of 660.
   b. Create the dbspace using the Informix `onspaces` command-line utility, as shown in the following example.

      ```
      onspaces -c -d ncimdbspace -p pathname/ncimdbspace -o 0 -s 1000000
      onspaces -c -S ncimsbspace -p pathname/ncimsbspace -o 0 -s 100000
      ```

      where:

      pathname
      Is the path to the directory containing the dbspace.

      This command creates a dbspace named *ncimdbspace* of roughly 1GB in a file of the same name and a second smaller dbspace for binary large objects named *ncimsbspace*. For more information on the `onspaces` command-line, see the Informix documentation.
3. Change to the `/PrecisionIP/scripts` directory of the extracted installation image.
4. Optional: If you are configuring Informix on a different server to Network Manager, copy the `create_informix_database.sh` script to the remote host where you have Informix installed.
5. To create the database, type the following command:
   `./create_informix_database.sh database_name user_name`, where:

   database_name
   Is the required name of the database to create and is also used as a prefix for the polling data database name.

user_name
Is the Informix Network Manager 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`. After you run the command, the Informix database is created. For information on how to install and configure Informix, see your Informix documentation.

6. When running the Network Manager installer later on, make sure you select **Start Custom Installation**. Then, in the Select Installation Options panel, you must select **Number of Servers** > **Multi-server Installation** (even if Network Manager is being installed on the same server as Informix), and also select **Default values** > **Customize settings**. You will then have the option to connect to an existing Informix database. This is required to ensure that the installer sets the Network Manager Informix environment variables and the `DbLogins` configuration file correctly (for example, the `INFORMIXDIR` and the `m_DbServer` values are set as required). The Network Manager installer can then create the tables in the database either on the local or a remote host, depending on where your database is installed.

Once you have created the database, you must perform the following steps on the server hosting the Informix database to enable Java processes to find the Informix database:

1. Edit the file pointed to by the `INFORMIXSQLHOSTS` environment variable.
2. Change the hostname field by prefixing the name with an asterisk; for example, change *`hostname`* to *`*hostname`*. The hostname field is usually the third field on the last line of the file.
3. Stop and restart Informix, using the `onmode -ky` and `oninit` commands.

Configuring an existing Informix databases on Windows

To use an existing Informix database as the topology database on Windows, you must configure an instance and create a database before Network Manager is installed.

Note: You only need to follow these steps if you want to use an existing local or remote Informix database for your Network Manager installation. If you want to install and set up a new Informix database on either a local or remote host for Network Manager, you can use the Informix bundled with Network Manager and set it up using the Network Manager installer.

The database is created by scripts that are contained in the `\PrecisionIP\scripts` directory of the extracted installation image. You must have uncompressed the installation package before you configure your existing Informix database.

The Informix environment must be set up as the Informix administrative user on the server hosting Informix. If the host is on a remote server, then copy the database creation scripts to the remote server.

During installation of Network Manager, the NCIM topology database is installed on the Informix database that you create.

1. Go to the host where you have your existing Informix installed.

2. Use the Informix `onspaces` command-line utility to create a dbspace to allocate the necessary disk space for the NCIM database tables. You can create the dbspace anywhere on your file system, provided there is sufficient disk space in that location for the dbspace to grow as the database grows in size.
   a. Create two empty files and name these files as follows: *ncimdbspace*, to hold the normal database tables, and *ncimsbspace*, to hold database tables containing BLOBs.
   b. Create the dbspace using the Informix `onspaces` command-line utility, as shown in the following example.

      ```
      onspaces -c -d ncimdbspace -p pathname\ncimdbspace -o 0 -s 1000000
      onspaces -c -S ncimsbspace -p pathname\ncimsbspace -o 0 -s 100000
      ```

      where:

      pathname
      Is the path to the directory containing the dbspace.

      This command creates a dbspace named *ncimdbspace* of roughly 1GB in a file of the same name and a second smaller dbspace for binary large objects named *ncimsbspace*.For more information on the `onspaces` command-line, see the Informix documentation.
3. Open a Command window and change to the `\PrecisionIP\scripts` directory of the extracted installation image.
4. Optional: If you are configuring Informix on a different server to Network Manager, copy the `create_informix_database.bat` script to the remote host where you have Informix installed.
5. To create the database, type the following command: `create_informix_database.bat` *database_name user_name*, where:

   database_name
   Is the required name of the database to create and is also used as a prefix for the polling data database name

   user_name
   Is the Informix Network Manager 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.bat NCIM ncim`. After you run the command, the Informix database is created. For information on how to install and configure Informix, see your Informix documentation.
6. When running the Network Manager installer later on, make sure you select **Start Custom Installation**. Then, in the Select Installation Options panel, you must select **Number of Servers** > **Multi-server Installation** (even if Network Manager is being installed on the same server as Informix), and also select **Default values** > **Customize settings**. You will then have the option to connect to an existing Informix database. This is required to ensure that the installer sets the Network Manager Informix environment variables and the `DbLogins` configuration file correctly (for example, the `INFORMIXDIR` and the `m_DbServer` values are set as required). The Network Manager installer can then create the tables in the database either on the local or a remote host, depending on where your database is installed.

Once you have created the database, you must perform the following steps on the server hosting the Informix database to enable Java processes to find the Informix database:

1. On the Windows **Start** menu, click **Start** > **Programs** > **IBM Informix Client-SDK**.
2. In the IBM Informix Setnet32 window, prefix the HostName field with an asterisk; for example, change *hostname* to **hostname*.
3. Stop and restart Informix.
   a. Go to the Windows Services window.
   b. Select the IBM Informix Dynamic Server service.
   c. Click **Restart Service**.

Installing and configuring DB2 databases on UNIX

To use a DB2 database as the topology database on UNIX, you must install DB2, configure an instance, and create a database before Network Manager is installed.

The database is created by scripts that are contained in the `/PrecisionIP/scripts` directory of the extracted installation image. You must have uncompressed the installation package before you install DB2 and attempt to create the database.

The DB2 environment must be set up as the DB2 administrative user on the server hosting DB2. If the host is on a remote server then copy the database creation scripts to the remote server.

During installation of Network Manager, the NCIM topology database is installed on the DB2 database that you create.

Restriction: AIX If you install the Network Manager core components as a non-root user on AIX, and you are using DB2 as the NCIM topology database, you must ensure that only one DB2 client library is active on the DB2 server. Having multiple DB2 clients active on the server might cause issues and is not supported.

For more information about how to install and configure DB2, see the information center for your DB2 version.

Fix Pack 4 If you plan to use the DB2 high availability disaster recovery (HADR) feature in Network Manager 3.9 Fix Pack 4, you must install DB2 9.7 or DB2 10.1. The DB2 HADR feature in Network Manager 3.9 Fix Pack 4 is available only with DB2 9.7 and DB2 10.1.

1. Install DB2 and configure an instance in which the installation process can create the NCIM database.
2. If you are installing DB2 on a different server to the Network Manager IP Edition server, install the DB2 Runtime Client libraries on the Network Manager IP Edition server.

   The DB2 Runtime Client libraries are required on both the Network Manager core components server and the server where the Tivoli Integrated Portal and Web GUI are installed. This means the client libraries might need to be installed on two separate machines.
3. Change to the directory into which the instance was installed and then change to the `sqllib` subdirectory.
4. Set up the environment by typing the following command:

Shell	Command
Bourne	`. db2profile`
C	`source db2cshrc`

The Network Manager application wrapper scripts automatically set up the DB2 environment. For more information about how the wrapper scripts set up the environment, see "Example of how the wrapper scripts search for a file" on page 62.

5. Change to the `/PrecisionIP/scripts` directory of the extracted Network Manager installation image.
6. Optional: If you are setting up DB2 on a different server from Network Manager, copy the `create_db2_database.sh` script to the remote host where you installed DB2.
7. 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
   ```
8. When running the Network Manager installer later on, make sure you select the option to configure an existing DB2 database. The Network Manager installer can then create the tables in the database either on the local or a remote host, depending on where your database is installed.
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:
    a. Change to the `/PrecisionIP/scripts` directory of the extracted Network Manager installation image.
    b. Optional: If you are setting up DB2 on a different server to Network Manager, copy the `catalog_db2_database.sh` script to the remote host where you installed DB2.
    c. Run the `./catalog_db2_database.sh` *`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.

       The following command shows an example usage of the script:

       ```
       ./catalog_db2_database.sh ITNM db2server.ibm.com 50000
       ```
11. Optional: If you installed the Network Manager core components as a non-root user on AIX, you must manually create symbolic links in `/usr/lib` to the shared libraries, similar to the following example:

```
ln -s ${NCHOME}/precision/platform/aix5/lib/libNcpDbDb2.so /usr/lib/
libNcpDbDb2.so
ln -s ${NCHOME}/precision/platform/aix5/lib/libNcpDb.so /usr/lib/libNcpDb.so
ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2.a /usr/lib/libdb2.a
ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2osse.a /usr/lib/libdb2osse.a
ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2locale.a /usr/lib/libdb2locale.a
ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2g11n.a /usr/lib/libdb2g11n.a
ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2genreg.a /usr/lib/libdb2genreg.a
ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2osse_db2.a /usr/lib/
libdb2osse_db2.a
ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2install.a /usr/lib/libdb2install.a
ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2trcapi.a /usr/lib/libdb2trcapi.a
ln -s /home/${DB2INSTANCE}/sqllib/lib/libdb2dascmn.a /usr/lib/libdb2dascmn.a
```

12. Optional: After installing Network Manager, run the `NCHOME/precision/scripts/sql/db2/restrict_db2_privileges.sh` script as a user with system privileges. Use this script to put restrictions on the privileges the NCIM database user is given.

Example of how the wrapper scripts search for a file

Under the Bourne shell, when the wrapper scripts set up the environment variables for DB2, the scripts search for the following file and run it: `$ITNMHOME/.db2sqllib`.

This file is automatically created during the install, and it first checks for the existence of a file called `db2profile` with which to set up the DB2 environment. If the file exists, it is run as shown in the following example:

```
if [ -f /home/db2inst/sqllib/db2profile ] ; then
 . /home/db2inst/sqllib/db2profile
fi
```

The `$ITNMHOME/.db2sqllib` file is parsed by the **setup_run_as_setuid_root.sh** script to determine the location of the DB2 client libraries (see "Configuring the core components to run as non-root" on page 222).

Related concepts:

Fix Pack 4 "About NCIM topology database high availability" on page 276
Network Manager allows you to configure the Network Connectivity and Inventory Model (NCIM) topology database for high availability, minimizing the impact of computer or network failure. The following sections provide an overview of NCIM topology database high availability and explain how to configure it.

"Network Manager failover architecture (core processes)" on page 281
Failover of the Network Manager core processes can be implemented by setting up primary and backup Network Manager installations that run on different servers. Both installations can either connect to a single Tivoli Netcool/OMNIbus ObjectServer or to a virtual pair of ObjectServers.

Related information:

IBM DB2 Version 10.1 Information Center
For more information on DB2 10.1 HADR, search the IBM DB2 Version 10.1 Information Center. Suggested search terms include "high availability".

IBM DB2 Version 9.7 Information Center
For more information on DB2 9.7 HADR, search the IBM DB2 Version 9.7 Information Center. Suggested search terms include "high availability".

Oracle Database Online Documentation

Installing and configuring DB2 databases on Windows

To use a DB2 database as the topology database on Windows, you must install DB2, configure an instance, and create a database before Network Manager is installed.

The database is created by scripts that are contained in the `\PrecisionIP\scripts` directory of the extracted installation image. You must have uncompressed the installation package before you install DB2 and attempt to create the database.

The DB2 environment must be set up as the DB2 administrative user on the server hosting DB2. If the host is on a remote server then copy the database creation scripts to the remote server.

During installation of Network Manager, the NCIM topology database is installed on the DB2 database that you create.

For more information about how to install and configure DB2, see the information center for your DB2 version at http://www-01.ibm.com/support/docview.wss?uid=swg27009474.

1. Install DB2 and configure an instance in which the installation process can create the NCIM database.
2. If you are installing DB2 on a different server to the Network Manager IP Edition server, install the DB2 Runtime Client libraries on the Network Manager IP Edition server.

   The DB2 Runtime Client libraries are required on both the Network Manager core components server and the server where the Tivoli Integrated Portal and Web GUI are installed. This means the client libraries might need to be installed on two separate machines.
3. Open a Command window and change to the `\PrecisionIP\scripts` directory of the extracted installation image.
4. Optional: If you are setting up DB2 on a different server to Network Manager, copy the `create_db2_database.bat` script to the remote host where you installed DB2.
5. To create the database, type the following command: `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`.
6. When running the Network Manager installer later on, make sure you select the option to configure an existing DB2 database. The Network Manager installer can then create the tables in the database either on the local or a remote host, depending on where your database is installed.

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:
   a. Change to the `\PrecisionIP\scripts` directory of the extracted Network Manager installation image.
   b. Optional: If you are setting up DB2 on a different server to Network Manager, copy the `catalog_db2_database.bat` script to the remote host where you installed DB2.
   c. Run the `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.

      The following command shows an example usage of the script:`catalog_db2_database.bat ITNM db2server.ibm.com 50000`

After you run the commands, the DB2 database is created and cataloged.

Installing and configuring MySQL databases on UNIX

To use a MySQL database as the topology database on UNIX, you must install MySQL and create the necessary schema and user before Network Manager is installed.

The database schema and user are created by scripts that are contained in the `/PrecisionIP/scripts` directory of the extracted installation image. You must have uncompressed the installation package before you attempt to create the database.

During installation of Network Manager, the NCIM topology database is installed on the MySQL database that you create.

For information on how to install and configure MySQL, see your MySQL documentation.

1. Install a supported version of MySQL.
2. Change to the `/PrecisionIP/scripts` directory of the extracted Network Manager installation image.
3. Optional: If you are setting up MySQL on a different server to Network Manager, copy the `create_mysql_database.sh` script to the remote host where you installed MySQL.
4. Create the necessary tables by running the **`create_mysql_database.sh`** script using the following command:

   `create_mysql_database.sh` *`username password`*

   Where *username* is `mysql` or `root`, and *password* is the password for that user. The schema and user that Network Manager uses are created in the database.
5. When running the Network Manager installer later on, make sure you select the option to configure an existing MySQL database. You can run the installer on the server where the Network Manager components are to be installed, or on the server where the MySQL database is installed. Network Manager creates the tables in the database.

Installing and configuring MySQL databases on Windows

To use a MySQL database as the topology database on Windows, you must install MySQL and create the necessary schema and user before Network Manager is installed.

The database schema and user are created by scripts that are contained in the `\PrecisionIP\scripts` directory of the extracted installation image. You must have uncompressed the installation package before you attempt to create the database.

During installation of Network Manager, the NCIM topology database is installed on the MySQL database that you create.

For information on how to install and configure MySQL, see your MySQL documentation.

1. Install a supported version of MySQL.
2. Change to the `\PrecisionIP\scripts` directory of the extracted Network Manager installation image.
3. Optional: If you are setting up MySQL on a different server to Network Manager, copy the `create_mysql_database.bat` script to the remote host where you installed MySQL.
4. Run the **`create_mysql_database.bat`** script using the following command:

   `create_mysql_database.bat` *`username password`*

   Where *username* is `mysql` or an administrative Windows user, and *password* is the password for that user. The schema and user that Network Manager uses are created in the database.
5. When running the Network Manager installer later on, make sure you select the option to configure an existing MySQL database. You can run the installer on the server where the Network Manager components are to be installed, or on the server where the MySQL database is installed. Network Manager creates the tables in the database.

Installing and configuring Oracle databases on UNIX

To use an Oracle topology database on UNIX, you must install Oracle, configure a schema, and create a database before Network Manager is installed. During installation, the NCIM topology database is installed on the Oracle database that you create.

The database is created by scripts that are contained in the `/PrecisionIP/scripts` directory of the extracted installation image. You must have uncompressed the installation package before you attempt to create the database.

You need access to a command prompt that can use the Oracle SQL*Plus client to connect to the database.

For information on installing and configuring Oracle, refer to the Oracle documentation at http://docs.oracle.com/cd/E11882_01/index.htm.

The database creation script creates users for several Oracle users. Only the user `ncim` is granted permission to connect to the database. The `ncim` user is also granted permission to access the schemas of the other users. The default password for the `ncim` user created by this script is also `ncim`.

1. Install Oracle and configure a schema on which the installation process can create the NCIM database.

2. Make sure that the there are no port conflicts with the HTTP service of the Oracle XML database. The HTTP service of the Oracle XML database is configured to use the default port 8888.
3. Make sure that the Oracle TNS listener is running on the Oracle server by typing the following command: `$ORACLE_HOME/bin/lsnrctl status`.
4. If the Oracle TNS listener is not running, type the following command to start it: `$ORACLE_HOME/bin/lsnrctl start`.
5. As the Oracle `system` user, change to the `/PrecisionIP/scripts` directory of the extracted Network Manager installation image.
6. Optional: If you are setting up Oracle on a different server to Network Manager, copy the `create_oracle_database.sql` file to the remote host where you installed Oracle. This script is needed to prepare the environment for the NCIM topology database, and it needs to be run on the host system where the database is installed, as detailed in the following step.
7. To create the schema, run the following script: `sqlplus system/password < create_oracle_database.sql`. To change the password of the `ncim` user, edit the script and change the second occurrence of `ncim` on the following line: `CREATE USER ncim IDENTIFIED BY ncim`.
8. When running the Network Manager installer later on, make sure you select the option to connect to an existing Oracle database. The Network Manager installer can then create the tables in the database either on the local or a remote host, depending on where your database is installed.

   Note: Fix Pack 5 If you are installing Network Manager in an Oracle high availability environment using Real Application Clusters (RAC), install Network Manager first with a direct connection to a single node in the Oracle cluster. After installing Network Manager successfully, you can set up high availability for Network Manager using an Oracle Single Client Access Name (SCAN) address as described in "Configuring Network Manager to work with DB2 HADR or Oracle RAC" on page 313.
9. Optional: After installing Network Manager, run the `NCHOME/precision/scripts/sql/oracle/restrict_oracle_privileges.sh` *`user_name password`* script as a user with system privileges. Use this script to revoke the privileges the NCIM database user is given when the NCIM database schema is created, and to grant finer-grained privileges.

Installing and configuring Oracle databases on Windows

To host NCIM on an Oracle database on Windows, you must install Oracle, configure a schema, and create a database before Network Manager is installed. During installation, NCIM is installed on the Oracle database that you create.

The database is created by scripts that are contained in the `\PrecisionIP\scripts` directory of the extracted installation image. You must have uncompressed the installation package before you attempt to create the database.

You need access to a command prompt that can use the Oracle SQL*Plus client to connect to the database.

For information on installing and configuring Oracle, refer to the Oracle documentation.

On Windows, the Oracle TNS listener is a Windows Service that can be started and stopped from the Windows Control Panel.

The database creation script creates users for several Oracle users. Only the user `ncim` is granted permission to connect to the database. The `ncim` user is also granted permission to access the schemas of the other users. The default password for the `ncim` user created by this script is also `ncim`.

1. Install Oracle and configure a schema on which the installation process can create the NCIM database.
2. Make sure that the there are no port conflicts with the HTTP service of the Oracle XML DB. The HTTP service of the Oracle XML DB is configured to use the default port 8888.
3. Make sure that the Oracle TNS listener is running on the Oracle server by checking the Services application of the Windows Control Panel.
4. As the Oracle `system` user, change to the `\PrecisionIP\scripts` directory of the extracted Network Manager installation image.
5. Optional: If you are setting up Oracle on a different server to Network Manager, copy the `create_oracle_database.sql` file to the remote host where you installed Orcale.
6. To create the schema, run the following script: `sqlplus system/password < create_oracle_database.sql`. To change the password of the `ncim` user, edit the script and change the second occurrence of `ncim` on the following line: `CREATE USER ncim IDENTIFIED BY ncim`.
7. When running the Network Manager installer later on, make sure you select the option to configure an existing Oracle database. The Network Manager installer can then create the tables in the database either on the local or a remote host, depending on where your database is installed.

Setting up NCIM to handle multibyte characters

You must configure the NCIM database to handle multibyte characters, such as Simplified Chinese characters, if you want the NCIM database to store multibyte data. Such configuration is useful when, for example, you need to enter multibyte characters into the Description field of a poll definition.

If you are running the NCIM database on DB2 or Informix then ensure that you have the following settings:

DB2 If you are running Network Manager in a locale that supports multibyte characters, then there is no need to make any configuration changes. For example, both of the following locales support multibyte characters when NCIM is running on DB2:

- `LANG=zh_CN.gb18030`
  `LC_ALL=zh_CN.gb18030`
- `LANG=en_US.utf8`
  `LC_ALL=en_US.utf8`

Informix

If you use Informix, the database creation scripts and the Network Manager installer set the DB_LOCALE environment variable for you.

If you install Informix separately from Network Manager, make sure the DB_LOCALE environment variable of the NCIM Informix database matches the locale on the Network Manager server. Network Manager uses the setting DB_LOCALE=en_us.utf8 for Informix, so make sure you create the Informix databases using the environment variable setting of DB_LOCALE=en_us.utf8. Informix also requires Unicode support, so start Informix with the environment variable setting of GL_USEGLU=1. For

more information, see the *Informix GLS User's Guide* at http://www-01.ibm.com/support/knowledgecenter/SSGU8G_11.70.0/com.ibm.welcome.doc/welcome.htm.

Related information:

http://www-01.ibm.com/support/knowledgecenter/SSGU8G_11.50.0/com.ibm.glsug.doc/ids_gug_068.htm

Setting up NCIM to handle multibyte characters on a MySQL database:

Use this information to configure the NCIM database running on MySQL to handle multibyte characters.

By default, MySQL clients connect to the NCIM database using the latin1 character set, regardless of which character set the operating system is using. The latin1 character set is not capable of displaying multibyte characters correctly.

To configure NCIM to handle multibyte characters on a MySQL database:

1. Edit the MySQL configuration file. The name of this file varies depending on your operating system:
   - UNIX my.cnf
   - Windows my.ini

   The location of this file varies depending on whether you are running Network Manager in a single-server installation or in a multiserver installation.

   Single-server installation
   The MySQL configuration file is in `$MYSQL_HOME`.

   Multiserver installation
   Edit the MySQL configuration file on the server that hosts the NCIM MySQL database.
2. Update the `[client]` section of the MySQL configuration file with the relevant default character set property. Proceed as follows:
   - If there is no `[client]` section in the MySQL configuration file, then add two lines similar to the examples below and relevant to your locale.
   - If there is a `[client]` section in the MySQL configuration file but no default character set property, then append to the `[client]` section a default character set property similar to the properties given examples below and relevant to your locale.
   - If there is a `[client]` section in the MySQL configuration file with a default character set property that does not match your locale, then replace the default character set property with a property similar to the properties given examples below and relevant to your locale.

   The following table provides examples of locales and corresponding default multibyte character set properties.

Table 8. Example default character set properties

Locale	Default character set property
en_US.utf8	`[client]` `default-character-set=utf8`

Table 8. Example default character set properties (continued)

Locale	Default character set property
zh_CN.gb2312	`[client]` `default-character-set=gb2312`

A full set of supported MySQL character sets is available on the MySQL website.

Important: The character set gb18030 is not supported by MySQL 5.0. You will not be able to resolve this issue if you are running the NCIM database using MySQL 5.0 with gb18030 as the character set.

Related information:

http://dev.mysql.com/doc/refman/5.0/en/charset-mysql.html

Setting up NCIM to handle multibyte characters on an Oracle database:

Use this information to configure the NCIM database running on Oracle to handle multibyte characters.

To configure NCIM to handle multibyte characters on an ORACLE database:

1. Set the Oracle NLS_LANG environment variable to an appropriate value. For example, if the system is running under the zh_CN.gb18030 locale, change the NLS_LANG setting to the following value: `SIMPLIFIED CHINESE_CHINA.ZHS32GB18030`. A full set of NLS_LANG environment variable values for different locales is available on the Oracle website.
2. Set the Network Manager environment to pick up your changes after installation.
   - UNIX Go to the $NCHOME directory and issue the following command: `source env.sh`.
   - Windows Go to the %NCHOME% directory and run the `env.bat` script.

Related information:

http://www.oracle.com/technology/tech/globalization/htdocs/nls_lang%20faq.htm

Installing Tivoli Common Reporting

You must have Tivoli Common Reporting installed to run the network management reports provided by Network Manager.

Installing Tivoli Common Reporting 3.1

In order to run Tivoli Common Reporting reports from Network Manager using Tivoli Common Reporting 3.1, you must install Tivoli Common Reporting 3.1 on a separate server. If you use MySQL for the topology database, you can not use Tivoli Common Reporting V3.1 You must use Tivoli Common Reporting V2.1.1.

Tivoli Common Reporting 3.1 to Network Manager integration architecture:

Use this information to understand how to integrate Tivoli Common Reporting 3.1 on a separate server to the Network Manager server.

The following figure shows the Tivoli Common Reporting 3.1 to Network Manager integration architecture.

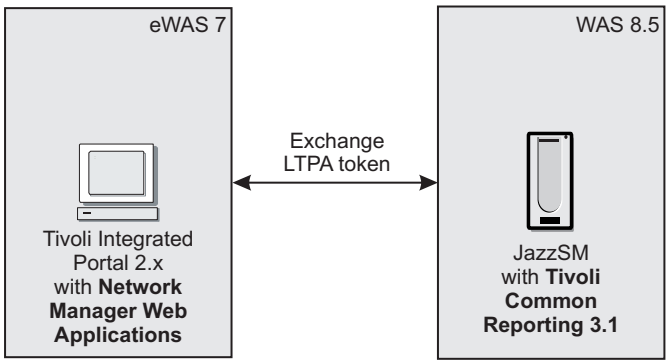

Figure 8. Tivoli Common Reporting 3.1 to Network Manager integration architecture

Requirements for the Tivoli Common Reporting 3.1 server

You must download and install the following software on the Tivoli Common Reporting 3.1 server machine:

- JazzSM
- WAS 8.5
- Tivoli Common Reporting 3.1.

Installation steps for Tivoli Common Reporting 3.1:

Follow these instructions to download and install Jazz for Service Management 1.1.0.3 with Tivoli Common Reporting 3.1.0.1

If you do not have Tivoli Common Reporting installed when installing Network Manager, you can install Tivoli Common Reporting at a later date and configure the reports then.

1. On the remote server, where you will be installing Tivoli Common Reporting 3.1, download Jazz for Service Management version 1.1.0.3, which includes Tivoli Common Reporting 3.1.0.3. Tivoli Common Reporting 3.1.0.3 is the version required for this integration. You can download Jazz for Service Management version 1.1.0.3 from FixPack Central, at http://www-933.ibm.com/support/fixcentral/.
2. Go to the Tivoli Common Reporting documentation for information about installing or upgrading to Tivoli Common Reporting 3.1.:

   Installing Tivoli Common Reporting 3.1
   http://www-01.ibm.com/support/knowledgecenter/SSEKCU_1.1.1.0/com.ibm.psc.doc_1.1.1.0/install/tcr_t_install.html?lang=en

   Upgrading to Tivoli Common Reporting 3.1
   http://www-01.ibm.com/support/knowledgecenter/SSEKCU_1.1.1.0/com.ibm.psc.doc_1.1.1.0/tcr_original/ctcr_upgrade.html?lang=en
3. Install Tivoli Common Reporting 3.1 on the remote server.

4. Once you have installed Network Manager, you must configure Tivoli Common Reporting 3.1.

Installing Tivoli Common Reporting 2.1.1

Perform these tasks to install Tivoli Common Reporting 2.1.1. Note that Tivoli Common Reporting 2.1.1 does not support Internet Explorer versions 10 or 11. Consequently, you cannot use the reporting feature if you are using Internet Explorer 10 or 11 to run the Network Manager GUI.

Network Manager installs the reports package required for network management reports on the server where the Network Manager GUI components are installed. If the chosen installation location for Network Manager already has existing Tivoli Integrated Portal and Tivoli Common Reporting instances, then Network Manager automatically configures the reports to be used with that Tivoli Common Reporting instance.

If you do not have Tivoli Common Reporting installed when installing Network Manager, you can install Tivoli Common Reporting at a later date and configure the reports then.

If you use Oracle V12c, you can not use Tivoli Common Reporting V2.1.1. You must use Tivoli Common Reporting V3.1.

Attention: If you have an existing Tivoli Common Reporting installation, ensure you have the required repository for user authentication set up before installing the Network Manager GUI components. You cannot change the user authentication method with the Network Manager installer. For example, if you are planning to use the ObjectServer-based authentication and it is not configured yet on the existing Tivoli Integrated Portal installation used by your Tivoli Common Reporting instance, then install the Tivoli Netcool/OMNIbus Web GUI (included in the Network Manager package) into the existing Tivoli Integrated Portal installation, and select the option to enable ObjectServer-based authentication. Then install the Network Manager GUI component into the existing Tivoli Integrated Portal.

To install Tivoli Common Reporting:

1. Download the Tivoli Common Reporting package. You can download Tivoli Common Reporting as an optional part from the Network Manager package. For more information, see the download document at http://www-01.ibm.com/support/docview.wss?rs=3117&uid=swg24035480.
2. Go to the Tivoli Common Reporting documentation for information about installing Tivoli Common Reporting: http://www.ibm.com/support/knowledgecenter/SSH2DF_2.1.1/ctcr_prodoverview.html
3. Install Tivoli Common Reporting on the host where the Network Manager GUI components will be installed.
4. Install Network Manager as described in “Installing Network Manager” on page 72. The Network Manager installation process automatically installs the network management reports package and configures the reports to work with Tivoli Common Reporting.

   Important: Stop Tivoli Common Reporting before installing Network Manager. As the user who installed Tivoli Common Reporting, run the following command from the `TCR_component_dir/bin` directory:
   `./stopTCRserver.sh <tip_admin_user> <password>`

5. Optional: If you do not install Tivoli Common Reporting before installing Network Manager, you can configure the network management reports at a later date after installing Network Manager as described in "Configuring reports for existing installations" on page 247.

Configuring Red Hat Linux Enterprise Edition

Before you install on Red Hat Linux Enterprise Edition, you must disable SELinux.

When Red Hat Enterprise Linux is installed, SELinux is optionally enabled. To disable SELinux, turn off SELinux enforcing by completing the following steps:

1. Open the following file:
   `/etc/sysconfig/selinux`
2. Find the following line:
   `SELINUX=enforcing`
3. Change it to `SELINUX=disabled`.
4. Restart the server.

Checking I/O Completion Port (IOCP) settings

If you are installing Network Manager on AIX and plan to connect to an Oracle database then you must make sure that the IOCP setting is correct.

You must perform the following steps as the root user.

1. Issue the following command
   `/usr/sbin/lsdev -c iocp -F status`

   Proceed as follows:
   - If this command returns the result `Available` then you do not need to complete any more steps in this task.
   - If the command returns something other than the result `Available`, for example, `Defined`, then complete the remaining steps in this task.
2. Issue the following command:
   `smitty iocp2`
3. Select `Change/Show Characteristics of I/O Completion Ports`.
4. Change `State to be configured at system restart` from `Defined` to `Available`.
5. Reboot the AIX server.

Installing Network Manager

You can install Network Manager in different modes, depending on your requirements. Use console mode to install Network Manager if you do not have access to a pointing device, such as a mouse.

UNIX Linux If you are logged in to the host computer as the root user but want to install Network Manager as a nonroot user, use the **su -** command to switch users. If you use the **su** command, errors can occur during the installation.

If you want to use an existing installation of Tivoli Netcool/OMNIbus, see "Configuring an existing Tivoli Netcool/OMNIbus installation" on page 51. The Network Manager installer can install onlyTivoli Netcool/OMNIbus V7.3.1.

Differences between basic and custom installation

Performing a custom installation gives you many more options than a basic installation.

Basic installation

Choose a basic installation if the following criteria apply.

- You are installing for demonstration or testing purposes.
- The installation is for a small network.
- You are installing all components on single server with default options.

Note: A basic installation automatically performs a network discovery after installing.

Custom installation

Choose a custom installation if any of the following criteria apply.

- The installation is for a medium or large network.
- You need to distribute an installation over several servers.
- The installation is for a network with advanced technologies such as Network Address Translation (NAT) or Multiprotocol Label Path Switching (MPLS).
- You want to use an existing installation of Tivoli Netcool/OMNIbus.
- You want to use an existing installation of Tivoli Integrated Portal.
- You require failover.
- You want to use an existing Informix database for topology data.
- You want to use a DB2, MySQL, or Oracle database for topology data.
- FIPS 140–2 compliance is important to you.

Note: A custom installation gives you the option to perform different types of network discoveries after installing.

About a FIPS 140-2 installation

Federal Information Processing Standard (FIPS) 140–2 is a US Federal cryptographic standard. You can install Network Manager using a restricted set of cryptographic algorithms.

Important: Network Manager cannot be said to be compliant with the FIPS 140–2 standard, and nothing in this information or in the product should be understood as making this claim. However, Network Manager can be installed in a mode that has been designed with FIPS 140–2 specifications taken into consideration.

You can install Network Manager using a restricted set of cryptographic algorithms by selecting the appropriate option from the Select Installation Options panel in the installation wizard.

Restriction:

If FIPS 140–2 compliance is important to you, you must use only version 7.3.1 or higher of IBM Tivoli Netcool/OMNIbus, and you must install IBM Tivoli Netcool/OMNIbus in FIPS mode. You must also ensure that all products integrating with Network Manager, such as IBM Tivoli Netcool/OMNIbus, have a

FIPS mode, and you must configure the products if necessary. You must also check that your operating system uses only FIPS 140–2 compliant modules.

Restriction: If you choose to install Network Manager using a restricted set of cryptographic algorithms, non-compliant features are not installed. You cannot change from a FIPS installation to a non-FIPS installation except by uninstalling and reinstalling the product. You also cannot change from a non-FIPS installation to a FIPS installation except by uninstalling and reinstalling the product.

Differences in a FIPS 140–2 installation of Network Manager

An FIPS 140–2 installation differs from a normal installation in the following ways:

- You cannot install Informix 11.5, which was included with Network Manager 3.9 in versions prior to Fixpack 1. Versions of Network Manager after Fixpack 1 include Informix 11.7, which is FIPS-compatible.
- You cannot use a remote MySQL as the topology database.
- The Telnet discovery agents do not use SSHv1 to interrogate devices. This might result in a failure to connect securely to a device if the device supports only SSHv1, or if the device only supports non-compliant SSHv2 algorithms.
- The SNMP Helper and the MIB browser cannot be configured to use MD5 or DES encryption.

Installing Network Manager using the wizard

The easiest way to install Network Manager is by using the wizard.

Before installing, ensure that you have performed any necessary pre-installation tasks, including checking that your servers are suitable for installing Network Manager.

Restriction: On AIX operating systems, you must install a supported Web browser in order to use the installation launchpad or the wizard.

Tip: The installation wizard takes focus when displaying windows. If you want to work in another window while the product is being installed, minimize the installation windows first.

To start the installation wizard, perform the following steps.

1. Start the installer wizard from the launchpad.
   - UNIX Run the **launchpad.sh** script.
   - Windows Run the **launchpad.exe** executable.
   a. Select the **Installing Network Manager** item from the menu.
   b. Select either a basic or custom installation by clicking the **Start Basic Installation** or **Start Custom Installation** button. A basic installation installs all components of the product onto a single server using default values. A basic installation is shorter and simpler than a custom installation and is suitable for small networks, small enterprise customers, and demonstration purposes. A basic installation automatically starts a network discovery when it finishes. A custom installation is suitable for medium to large networks, integrating with existing products, or multi-server installations. A custom installation gives you the option to start a network discovery when it finishes.

2. If you cannot start the launchpad, start the installation wizard from the command line.
   - UNIX Run the **install.sh** script.
   - Windows Run the **install.exe** executable.

   You have the option of choosing a basic or custom installation when the installation wizard starts, in the Select Installation Type wizard panel, which is the fourth wizard panel to be displayed.

   Note: Network Manager installs Tivoli Common Reporting by default if it is not present on the system. You can specify not to install the reporting feature and Tivoli Common Reporting at this time by entering the `-DinstallReports=0` option on the command line. You might need to do this if you are installing Network Manager on Red Hat Enterprise Linux 6.0, as Tivoli Common Reporting does not support RHEL 6.0. In such cases, you must install Tivoli Common Reporting on a separate host.

   For example, to install Network Manager without installing Tivoli Common Reporting, enter `./install.sh -DinstallReports=0` or `install.exe -DinstallReports=0` depending on your operating system.
3. Enter the appropriate values in the wizard panels to install the product.

Values for a basic installation

Use this information to understand what values to enter in the wizard panels for a basic installation.

A basic installation uses a restricted set of wizard panels to collect configuration information.

The following table describes the values that you must enter for each panel.

Note: The basic installation only installs the default Informix database. To use an existing instance of an Informix database, or to use a database other than Informix for Network Manager, choose the custom installation option.

Tip: Print out this table for ease of reference while you install the product. You can use this table to check that you have all the required information in advance, and to record important values that you enter.

Table 9. Wizard panels and their values

Wizard panel	Value/option	Description
Introduction	None	After reading the introductory text, click **Next**.

Table 9. Wizard panels and their values (continued)

Wizard panel	Value/option	Description
Validate system	None	This panel is only displayed if one or more of the system validation checks fail. If any error messages are displayed in this wizard panel, you must cancel the installation, fix the errors, and start the installation again. This system validation establishes whether the current server is suitable in general for installing network management software. The validation checks include checks for consistent DNS and for a minimum of available memory for the installation process itself.
Software License Agreement	I accept both the IBM and the non-IBM terms	Select this option to continue the installation.
	I do not accept the terms in the license agreement	If you select this option, you cannot continue installation.
Select Installation Location	Tivoli Network Manager install location	Use the default location or enter the location where you want Network Manager to be installed. **Restriction:** If you are upgrading Network Manager from a previous version, you must choose a different directory to the one that Network Manager is currently installed in. You cannot upgrade Network Manager by overwriting files. Permitted characters in the installation path are alphanumeric (A-Z, a-z, 0-9), dashes, underscores, periods, colons, slashes, and spaces.

Table 9. Wizard panels and their values (continued)

Wizard panel	Value/option	Description
Collect Default Installation Information	Netcool® Domain Name	Enter a name to be used as a network domain by Network Manager. Enter a descriptive name, for example, TESTNETWORK. The domain name must consist of between one and 11 characters (letters, numbers, or both), with the letters all capitals, no spaces, and no special characters. Make a note of the domain name, because it is used when starting components manually. Domain name:
	Administrative Password	Enter a password to be used as the Tivoli Netcool/OMNIbus ObjectServer root password, the topology database administrator password, and the password for the default user accounts itnmadmin and itnmuser. The password must consist of between four and eight ASCII characters, and must match any password requirements that are applicable on the machine where you are installing. If the Informix database account already exists on the operating system, enter the password used to access it. **Restriction:** The Informix password must not start with a dollar sign ($).
	Confirm Password	Re-enter the administrative password.

Table 9. Wizard panels and their values (continued)

Wizard panel	Value/option	Description
Collect Port Connection Information	Netcool/OMNIbus ObjectServer Port	Enter the port that you want to use for the ObjectServer, or accept the default value. If you are connecting to a failover pair of ObjectServers, specify details for the virtual Objectserver here.
	Tivoli Integrated Portal HTTP Port	Enter the port that you want to use for the Tivoli Integrated Portal, or accept the default value. Make a note of the port number, because you use this to connect to the Web applications. HTTP port:
	Informix database port	Enter the port that you want to use for the Informix database, or accept the default value.
Collect SNMP V1/V2 Community Strings	List of community strings	When the installation finishes, a simple discovery of the local subnet is started. Enter up to six SNMP community strings (passwords). These community strings are needed by the discovery process in order to get SNMP information from devices on your network. To reduce discovery time, list the community strings in order, from most frequently to least frequently used. `Public` is installed by default.
Pre-Installation Summary	None	Review the information about the components that will be installed. Click **Next** to run a final prerequisite check before installation.

Table 9. Wizard panels and their values (continued)

Wizard panel	Value/option	Description
Prerequisite Checking Results	None	Review the results of the prerequisite check. This prerequisite check establishes whether the current server is suitable for installing the specific components that you have chosen. If there are any serious errors, you must cancel the installation, fix the errors, and start the installation again. If there are no serious errors, click **Install** to install your chosen components. When prompted, accept any license agreements to continue.

Values for a custom installation

Use this information to understand what values to enter in the wizard panels for a custom installation.

A custom installation uses different panels to collect configuration information depending on the choices you make.

Attention: Using the Network Manager installer to configure an existing Tivoli Netcool/OMNIbus also installs the SNMP probe and the Netcool/OMNIbus Knowledge Library. If you do not want to overwrite your existing SNMP probe and Netcool/OMNIbus Knowledge Library customizations, you must select **Do not install or configure Tivoli Netcool/OMNIbus at this time** when prompted in panel **Select Components to Install**, under **Tivoli Netcool/OMNIbus**. After the installation of Network Manager, copy the installation package to the server where your existing Tivoli Netcool/OMNIbus installation is, and run the **`ConfigOMNI`** script to configure your Tivoli Netcool/OMNIbus, but ensure you do not select options to configure the SNMP probe or the Netcool/OMNIbus Knowledge Library.

The following table describes the values that you must enter for each panel.

Tip: Print out this table for ease of reference while you install the product. You can use this table to check that you have all the required information in advance, and to record important values that you enter.

Table 10. Wizard panels and their values

Wizard panel	When panel is displayed	Value/option	Description
Introduction	Always displayed.	None	After reading the introductory text, click **Next**.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Validate system	Displayed if the system fails validation.	None	This panel is only displayed if one or more of the system validation checks fail. Cancel the installation, fix the errors, and start the installation again. This system validation establishes whether the current server is suitable in general for installing network management software. The validation checks include checks for consistent DNS and for a minimum of available memory for the installation process itself.
Software License Agreement	Always displayed.	**I accept both the IBM and the non-IBM terms**	Select this option to continue the installation.
		I do not accept the terms in the license agreement	If you select this option, you cannot continue installation.
Select Installation Location	Always displayed.	**Tivoli Network Manager install location**	Use the default location or enter the location where you want Network Manager to be installed. **Restriction:** If you are upgrading Network Manager from a previous version, you must choose a different directory to the one that Network Manager is currently installed in. You cannot upgrade Network Manager by overwriting files. Permitted characters in the installation path are alphanumeric (A-Z, a-z, 0-9), dashes, underscores, periods, colons, slashes, and spaces.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Select Installation Options	Always displayed.	**Number of Servers** > **Single Server Installation**	Select this option to install Network Manager, the Informix topology database, and the GUI components (the Network Manager Web applications and the Tivoli Integrated Portal) on the current server. If you have obtained Tivoli Netcool/OMNIbus V7.3.1 and have the installation package available, you can also install Tivoli Netcool/OMNIbus V7.3.1 using this option.
		Number of Servers > **Multi-server Installation**	Select this option to choose which components to install on the current server.
		Default values > **Accept default settings**	Select this option to minimize the number of wizard panels displayed.
		Default values > **Customize settings**	Select this option to be able to customize every installation option.
		FIPS Compliance > **Use FIPS 140–2 compliant cryptographic routines**	Select this option if you want to install using cryptographic routines from a validated cryptographic module. If you select this option you cannot use Informix 11.5 or MySQL as the topology database, and there are other restrictions to the product functionality (as described in "About a FIPS 140-2 installation" on page 73).

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Select Components to Install	Displayed for multi-server installations.	**Core components**	Select whether to install the Network Manager network discovery, polling, root cause analysis and event enrichment components on this server.
		Web Applications	Also referred to in the documentation as "GUI components". Select this option if you want to install the Network Manager Web applications on this server. If the Tivoli Integrated Portal is not already installed, it is installed with the Web applications. If there is an existing installation of the Tivoli Integrated Portal on this server, you can choose to use it in a later panel.
Select Components to Install (continued)	Displayed for multi-server installations.	**Tivoli Netcool/OMNIbus**	The Network Manager installer looks for Tivoli Netcool/OMNIbus version 7.3.1 only. If it does not find the Tivoli Netcool/OMNIbus image (based on image name or part number), it asks for the file location. If you want the installer to install a supported Tivoli Netcool/OMNIbus version other than 7.3.1, then create a subdirectory called `OMNIbus` in the extracted Network Manager installation package, and extract the downloaded Tivoli Netcool/OMNIbus package into this directory. Linux Solaris The Network Manager installer cannot install or configure Tivoli Netcool/OMNIbus V7.4. For more information, see https://ibm.biz/BdRGK9.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Select Components to Install (continued)	Displayed for multi-server installations.	**Tivoli Netcool/OMNIbus (continued)**	To configure an existing Tivoli Netcool/OMNIbus installation, it must already be installed on this server. **Restriction:** To configure an earlier version of Tivoli Netcool/OMNIbus than 7.3.1, run the **ConfigOMNI** script before installing Network Manager, as described in "Configuring an existing Tivoli Netcool/OMNIbus installation" on page 51. To connect to an existing Tivoli Netcool/OMNIbus on another server, do not select the option to connect to an existing installation. Complete additional tasks as described in "Configuring Tivoli Netcool/OMNIbus for use with Network Manager" on page 155.
Select Components to Install (continued)	Displayed for multi-server installations.	**Topology database**	Choose to install a new Informix database for topology data or use an existing MySQL, DB2, Informix, or Oracle database. **Note:** Informix can only be installed by the root user. If you are installing Network Manager as non-root and want to use Informix, there is an additional post-installation step: You must log in as root after the installation has completed and install Informix on the system using the values provided during the Network Manager installation. See "Installing and configuring Informix after a non-root installation" on page 224

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Get Netcool/OMNIbus 7.3.1 Package Location	Displayed if you selected a single server installation or if you selected **Install event management software** in a multi-server installation.	**Choose directory containing Netcool/OMNIbus 7.3.1 package**	Enter the location of the downloaded package or installation media. You can only install V7.3.1 using the Network Manager installer.
Collect Default Installation Information	Displayed if you selected **Accept Default Settings**.	**Netcool Domain Name**	Enter a name to be used as a network domain by Network Manager. Enter a descriptive name, for example, TESTNETWORK. The domain name must consist of between one and 11 characters (letters, numbers, or both), with the letters all capitals, no spaces, and no special characters. Make a note of the domain name, because it is used when starting components manually. Domain name:
		Administrative Password	Enter a password to be used as the Tivoli Netcool/OMNIbus ObjectServer root password, the topology database administrator password, and the password for the default user accounts itnmadmin and itnmuser. The password must consist of between four and eight ASCII characters, and must match any password requirements that are applicable on the machine where you are installing.
		Confirm Password	Re-enter the administrative password.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Collect Port Connection Information	Displayed if you selected **Accept Default Settings**.	**Netcool/OMNIbus ObjectServer Port**	Enter the port that you want to use for the ObjectServer, or accept the default value.
		Tivoli Integrated Portal HTTP Port	Enter the port that you want to use for the Tivoli Integrated Portal, or accept the default value. Make a note of the port number, because you use this to connect to the Web applications. HTTP port:
		Informix database port	Enter the port that you want to use for the Informix database, or accept the default value.
Collect Netcool/OMNIbus Installation Details	Displayed if you chose to installTivoli Netcool/OMNIbus and selected **Customize Settings**.	**Netcool/OMNIbus ObjectServer name**	Enter a name to use for the ObjectServer that is being installed. The name must not contain spaces.
		Netcool/OMNIbus ObjectServer port	Enter a port to use for the ObjectServer that is being installed. The port must not currently be in use.
		Netcool/OMNIbus administrator account password	Enter a password for the administrator account.
		Confirm password	Confirm the password for the administrator account.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Configure existing ObjectServer	Displayed if you chose to configure an existing installation of Tivoli Netcool/OMNIbus.	**Netcool/OMNIbus installation location (OMNIHOME)**	The location on this server where Tivoli Netcool/OMNIbus is installed.
		Netcool/OMNIbus ObjectServer name	Enter the name of the ObjectServer that you want this installation to configure. If you are connecting to a failover pair of ObjectServers, specify the details of the virtual ObjectServer here.
		Netcool/OMNIbus ObjectServer port	Enter the port used by the ObjectServer. If you are connecting to a failover pair of ObjectServers, specify the details of the virtual ObjectServer here.
		Netcool/OMNIbus administrator account name	Enter the user name for the administrator account.
		Netcool/OMNIbus administrator account password	Enter the password for the administrator account.
		Confirm password	Confirm the password for the administrator account.
Connect to Existing ObjectServer	Displayed if you chose to connect to an existing installation of Tivoli Netcool/OMNIbus.	**Netcool/OMNIbus server host name**	Enter the name of the system where the Tivoli Netcool/OMNIbus installation to use is located.
		Netcool/OMNIbus ObjectServer name	Enter the name of the ObjectServer that you want this installation to connect to. If you are connecting to a failover pair of ObjectServers, specify the details of the virtual ObjectServer here.
		Netcool/OMNIbus port	Enter the port used by the ObjectServer. If you are connecting to a failover pair of ObjectServers, specify the details of the virtual ObjectServer here.
		Netcool/OMNIbus administrator account password	Enter the password for the administrator account.
		Confirm password	Confirm the password for the administrator account.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Select installation directory for TIP	Displayed if you selected **Install User Console** and **Customize Settings**.	**Choose an install folder**	Choose a location for the Tivoli Integrated Portal to be installed. Select this option if the Tivoli Integrated Portal is not already installed on this server.
		Reuse an existing install folder	Click **reuse**, and select the directory path of an existing installation of the Tivoli Integrated Portal. If the Tivoli Integrated Portal is not installed on the server, this option is not available. **Restriction:** You cannot install the Tivoli Netcool/OMNIbus Web GUI 7.3.1 over version 7.3.0. Choose a different installation folder.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Collect Tivoli Integrated Portal Installation Details	Displayed if you selected **Install User Console** and **Customize Settings**.	**TIP HTTP port**	Enter the port to be used for the Tivoli Integrated Portal. Make a note of the port number, because you use this to connect to the Web applications. HTTP port:
		TIP administrator account name	Enter a name to be used for the Tivoli Integrated Portal administrator account.
		TIP administrator account password	Enter a password to be used for the Tivoli Integrated Portal administrator account.
		Confirm password	Confirm the password for the administrator account.
		LDAP	Select this option to use LDAP authentication for Tivoli Integrated Portal users.
		ObjectServer	Select this option to use the ObjectServer for authentication for Tivoli Integrated Portal users. **Note:** To use a file-based repository for authentication for Tivoli Integrated Portal users, you must clear both the **LDAP** and the **ObjectServer** checkboxes.
LDAP Information	Displayed if you selected **Install User Console** and **Customize Settings** and you are using LDAP authentication for the Tivoli Integrated Portal.	**LDAP server host name**	Enter the host name of the LDAP server.
		LDAP port	Enter the port for the LDAP server.
		LDAP repository identifier	Enter the repository identifier for the LDAP server.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
LDAP Security Information	Displayed if you selected **Install User Console** and **Customize Settings** and you are using LDAP authentication for the Tivoli Integrated Portal.	**TIP administrative account name**	Enter the name of the Tivoli Integrated Portal administrator account. The default value is tipadmin.
		Bind Distinguished Name	Enter the bind name. The default value is cn=root. **Note:** If the bind name contains a space, then enclose the whole name in double quotation marks, for example, `"cn=Directory Manager"`.
		Bind Password	Enter the password for the bind name.
		Confirm Password	Confirm the bind password.
		Distinguished name of a base entry	Enter the distinguished name. The default value is o=IBM,c=US.
LDAP Entity Information	Displayed if you selected **Install User Console** and **Customize Settings** and you are using LDAP authentication for the Tivoli Integrated Portal.	**Person Account Entity Type**	This is preset to `PersonAccount`.
		Base Entry for PersonAccount	Enter the correct identifiers for your **o**rganization and **c**ountry.
		Group entity Type	This is preset to `Group`.
		Base Entry for Group	Enter the correct identifiers for your **o**rganization and **c**ountry.
		OrgContainer Entity Type	This is preset to `OrgContainer`.
		Base Entry for OrgContainer	Enter the correct identifiers for your **o**rganization and **c**ountry.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Collect Network Manager Installation Details	Displayed if Network Manager is being installed and you selected **Customize Settings**.	**Network Manager Domain Name**	Enter a name to be used as a network domain by Network Manager. Enter a descriptive name, for example, TESTNETWORK. The domain name must consist of between one and 11 characters (letters, numbers, or both), with the letters all capitals, no spaces, and no special characters. Make a note of the domain name, because it is used when starting components manually. Make a note of the domain name, because it is used when starting components manually. Domain name: **Attention:** The domain name is mandatory. You must enter a value.
		Discover subnet	Select this option if you want the installation process to start a network discovery of your local subnet.
		Seed Discovery from IBM Tivoli NetView Installation	Starts a discovery and uses data that was exported from an instance of IBM Tivoli NetView. **Important:** This option is not the most effective way of transitioning from the IBM Tivoli NetView product. The most effective way is to perform a fresh initial discovery without imported data from IBM Tivoli NetView. Scripts are provided that help you plan the transition. For more information, see "Transitioning from IBM Tivoli NetView" on page 151.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Collect Network Manager Installation Details (continued)	Displayed if Network Manager is being installed and you selected **Customize Settings**.	**Seed Discovery from other network management application**	Select this option if you want the installation process to start a network discovery using information from another network management application.
		None	Select this option if you want to complete the installation process without starting a discovery. If you choose not to start a discovery now, you can start a discovery later using the Discovery Status GUI. **Note:** The domain name is mandatory. You must enter a value under **Network Manager Domain Name** previously even if you do not want to start a discovery after installation.
Collect Initial Discovery Information	Displayed if you chose to discover your local subnet.	**IP address of the subnet to be discovered**	Enter the IP address of the subnet to be discovered. Only IPv4 addresses can be entered here.
		Netmask	Enter the netmask of the subnet. For a class C subnet, this is 255.255.255.0.
Collect SNMP V1/V2 Community Strings	Displayed if you chose to discover your local subnet.	List of community strings	Enter up to six SNMP community strings (passwords). These community strings are needed by the discovery process in order to get SNMP information from devices on your network. To reduce discovery time, list the community strings in order, from most frequently to least frequently used.
Get NetView Discovery Data	Displayed if you chose to use NetView® data to seed your discovery.	**Full name of the NetView migration script output**	Enter the location of the output of the IBM Tivoli NetView migration script that you ran from the Launchpad as part of the installation prerequisites.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Get Generic Discovery Data	Displayed if you chose to use information from another network management application to seed your discovery.	**Full name of the file containing the network nodes**	Enter the location of the file that contains a list of nodes in your network. The file must be in a format that can be parsed by the File finder, for example, a text file containing a list of IP addresses and hostnames separated by spaces.
		Full name of the file containing the SNMP community strings	Enter the location of the file that contains a list of community strings used in your network.
Collect Informix Installation Details	Displayed if an Informix database is being installed.	**Informix database port**	Enter a port to be used for connections to the Informix database. The port must not currently be in use. The default is 9088.
		Informix server name	Enter a name for use as the Informix server name. The default is `ITNM`.
		Informix server number	Enter the number of Informix databases already installed on this system. The default is zero.
		Informix database name	Enter a name for use as the Informix database name. The default is `itnm`.
		Informix database account name	Enter the name of the system account to be used to access the Informix database. The name must be in lowercase letters and numbers. The account is created if it does not already exist. The default is `ncim`.
		Informix database account password	Enter a password for the Informix database account. If the Informix database account already exists on the operating system, enter the password used to access it. If the account is created by the install, then this password is used to set the account password. **Restriction:** The Informix password must not start with a dollar sign ($).
		Confirm Password	Re-enter the database password.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Create Network Manager Topology database tables	Displayed if an Informix database is not being installed.	**Create tables to hold topology data in selected database**	Select this option to configure the selected topology database. You only need to do this once for any topology database. If you have already installed a component of Network Manager and selected this option in a previous installation, do not select this option now. **Note:** If you need to set up a database after installation for an existing Network Manager, for example, see the tasks about creating topology database schemas in the *IBM Tivoli Network Manager IP Edition Administration Guide*.
Connect to Existing MySQL Database	Displayed if an existing MySQL database is being used for topology data.	**MySQL database server host name**	Enter the name of the server on which the MySQL database is installed.
		MySQL database port	Enter the port that is used for connections to the MySQL database.
		MySQL database administrator account name	Enter the name of the MySQL administrator account.
		MySQL database administrator account password	Enter the password for the MySQL administrator account.
		Confirm Password	Re-enter the administrative password.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Connect to Existing DB2 Database	Displayed if an existing DB2 database is being used for topology data.	**DB2 database server host name**	Enter the name of the server on which the DB2 database is installed.
		DB2 database port	Enter the ports that is used for connections to the DB2 database.
		DB2 database name	Enter the name for the DB2 database.
		DB2 database account name	Enter the name of the DB2 administrator account.
		DB2 database account password	Enter the password for the DB2 administrator account.
		Confirm Password	Re-enter the administrative password.
		Local SQL Library Directory (separate panel)	Enter the path to the DB2 SQL libraries, for example `/export/home/db2inst1/sqllib`.
Connect to Existing Oracle Database	Displayed if an existing Oracle database is being used for topology data.	**Oracle database server host name**	Enter the name of the server on which the Oracle database is installed.
		Oracle database port	Enter the port that is used for connections to the Oracle database.
		Oracle database system identifier (SID)	Enter the system identifier for the Oracle database.
		Oracle database administrator account name	Enter the name of the Oracle administrator account.
		Oracle database administrator account password	Enter the password for the Oracle administrator account.
		Confirm Password	Re-enter the administrative password.

Table 10. Wizard panels and their values (continued)

Wizard panel	When panel is displayed	Value/option	Description
Connect to Existing Informix Database	Displayed if an existing Informix database is being used for topology data.	**Informix database server host name**	Enter the DNS host name or IP address of the server on which Informix is running.
		Informix database port	Enter the port that is used for connections to the Informix database.
		Informix server name	Enter the logical name given to the Informix database instance when it was installed.
		Informix database name	Enter the name of the Informix database.
		Informix database administrator account name	Enter the name of the Informix administrator account.
		Informix database administrator account password	Enter the password for the Informix administrator account.
		Confirm Password	Re-enter the administrative password.
Pre-Installation Summary	Always displayed.	None	Review the information about the components that will be installed. Click **Next** to run a final prerequisite check before installation.
Prerequisite Checking Results	Always displayed.	None	Review the results of the prerequisite check. This prerequisite check establishes whether the current server is suitable for installing the specific components that you have chosen. If there are any serious errors, you must cancel the installation, fix the errors, and start the installation again. If there are no serious errors, click **Install** to install your chosen components. When prompted, accept any license agreements to continue.

Installing Network Manager in console mode

If you cannot run the GUI-based installation wizard, then install Network Manager in console mode. You must use console mode to install the product if you do not have access to a pointing device, such as a mouse.

When you install in console mode, you specify installation options by responding to menus and prompts in a text-based user interface.

To run the installer in console mode, complete the following tasks:

1. Run the installation script with the **-i console** option.
   - UNIX Enter the following command:
     ```
     install.sh -i console
     ```
   - Windows Enter the following command:
     ```
     install.exe -i console
     ```

     Note: Network Manager installs Tivoli Common Reporting by default if it is not present on the system. You can specify not to install the reporting feature and Tivoli Common Reporting at this time by entering the `-DinstallReports=0` option on the command line. You might need to do this if you are installing Network Manager on Red Hat Enterprise Linux 6.0, as Tivoli Common Reporting does not support RHEL 6.0. In such cases, you must install Tivoli Common Reporting on a separate host.

     For example, to install Network Manager in console mode without installing Tivoli Common Reporting, enter `./install.sh -i console -DinstallReports=0` or `install.exe -i console -DinstallReports=0` depending on your operating system.
2. Follow the prompts, using the same values as for a GUI-based custom installation.
3. At any time, type `back` to return to the previous screen, or `quit` to exit the installer.

Related reference:

"Values for a custom installation" on page 79
Use this information to understand what values to enter in the wizard panels for a custom installation.

Installing Network Manager in silent mode

In silent mode, the installer reads the configuration information from a file, and does not prompt you for any information.

You can run the installer in silent mode if, for example, you want to deploy Network Manager with identical installation options on multiple machines, or when you are installing on a system that has no access to any GUI. You cannot cancel a silent installation once it has started.

The silent mode of installation is a two-step operation that requires you to define your installation settings in a response file and then run the installation program with the settings in this file.

To install in silent mode, complete the following steps.

1. Create a response file that defines the features you want to install. You have the following options to create the response file:

Option	Description
Create a response file using the launchpad	"Creating a response file using the launchpad"
Create a response file by editing the sample file provided	"Creating a response file using sample file" on page 98
Create a response file by running the installer in console mode	You can create a response file by running the installer in console mode and answering `yes` to the question `Generate Silent Response File?` when prompted. You can then create a silent response file interactively by answering on-screen questions without using a GUI. Console mode then creates a file named `silent-install.txt` in the directory you specify as the installation directory. The default is `/opt/IBM/tivoli/netcool`. See "Installing Network Manager in console mode" on page 96

2. After you have created the response file, start the installation script for your operating system:
   - Windows Start the **`install.exe`** command with the following options:

     `install.exe -i silent -f` *`path to response file`*

     If you do not want the install window to return control immediately, create a batch file to run the **`install.exe`** command.
   - UNIX Start the **`install.sh`** script using the following command:

     `install.sh -i silent -f` *`path to response file`*

   Note: Network Manager installs Tivoli Common Reporting by default if it is not present on the system. You can specify not to install the reporting feature and Tivoli Common Reporting at this time by entering the `-DinstallReports=0` option on the command line. You might need to do this if you are installing Network Manager on Red Hat Enterprise Linux 6.0, as Tivoli Common Reporting does not support RHEL 6.0. In such cases, you must install Tivoli Common Reporting on a separate host.

   For example, to install Network Manager in silent mode without installing Tivoli Common Reporting, enter `./install.sh -i silent -f` *`path to response file`* `-DinstallReports=0` or `install.exe -i silent -f` *`path to response file`* `-DinstallReports=0` depending on your operating system.

Creating a response file using the launchpad

You can create the response file for your silent installation using the launchpad.

To create the response file using the launchpad:

1. Go to the directory where you extracted the Network Manager installation package.
2. Start the launchpad.
   - UNIX Run the **`launchpad.sh`** script.
   - Windows Run the **`launchpad.exe`** executable.
3. Click **Installing Network Manager**.

4. Expand **Create a Response File for Silent Installation** and click **Generate a response file for a basic installation** or **Generate a response file for a custom installation** depending on whether you want to perform a basic or a custom installation silently later on.
5. Follow the instructions on the panels to enter values for the response file. The panels are the same as when you install Network Manager using the wizard.

   Tip: Check the values for basic or custom installation topics to understand the values to enter in the wizard panels.
6. Save the file.

Run the installation script with the silent command line option and full path to this file.

Related reference:

"Values for a basic installation" on page 75
Use this information to understand what values to enter in the wizard panels for a basic installation.

"Values for a custom installation" on page 79
Use this information to understand what values to enter in the wizard panels for a custom installation.

Creating a response file using sample file

You can create the response file for your silent installation by editing the sample file provided.

To create the response file by editing the sample:

1. Back up the sample response file. The sample response file, `ITNM-sample-response.txt`, is in the top level directory, wherever the installation package was extracted.
2. Edit the sample response file in a text editor.
   a. Uncomment any parameters that you want to use by removing the hash character # at the beginning of the line.
   b. Check the default values of the parameters and set new values as necessary.
   c. Replace all instances of `--UserInput--` with the appropriate values.
3. Save the file in a convenient location, for example, in the same directory as the Network Manager `INSTALL` script.

Run the installation script with the silent command line option and full path to this file.

Sample response file parameters for silent mode installation:

Use this information to understand how to edit the response file for a silent installation.

List of response file parameters

The following table lists the parameters provided in the default response file for silent installation in the order in which they appear in the file.

Table 11. Response file parameters

Parameter	Default value	Description
INSTALLER_UI	SILENT	Do not change this value or remove this line.
SingleServer	0	Do not change this value or remove this line.
DefaultValues	0	Do not change this value or remove this line.
$LICENSE_ACCEPTED$	false	To accept the license agreement, uncomment the variable and change the value to `true`. If the LICENSE_ACCEPTED is anything other than true, the installation will exit and no log will be produced and no indication of failure provided. By removing the # sign before #LICENSE_ACCEPTED=false and changing false to true you have signified acceptance of the Network Manager license agreement.
USER_INSTALL_DIR	C:\\IBM\\tivoli\\netcool	If you are installing on Windows, provide the fully qualified path to the directory where you want to install the product. **Note:** Windows considers the backslash \ character to be an escape character, so use a double backslash \\ when defining the path on Windows.
USER_INSTALL_DIR	/opt/IBM/tivoli/netcool	If you are installing on UNIX, provide the fully qualified path to the directory where you want to install the product.

Table 11. Response file parameters (continued)

Parameter	Default value	Description
installOMNI	0	Set the value as follows: • Set the value to 1 to install and configure Tivoli Netcool/OMNIbus, the necessary Tivoli Netcool/OMNIbus probes, and the IBM Tivoli Netcool/OMNIbus Knowledge Library. • Set the value to 2 to configure an existing Tivoli Netcool/OMNIbus that is already installed on this system. • Set the value to 3 to connect to an existing Tivoli Netcool/OMNIbus without configuring it. • Set the value to 0 if you do not want to install, configure, or connect to Tivoli Netcool/OMNIbus at this time. **Attention:** Using the Network Manager installer to configure an existing Tivoli Netcool/OMNIbus also installs the SNMP probe and the Netcool/OMNIbus Knowledge Library. If you do not want to overwrite your existing SNMP probe and Netcool/OMNIbus Knowledge Library customizations, you must set the **installOMNI** value to 0. After the installation of Network Manager, copy the installation package to the server where your existing Tivoli Netcool/OMNIbus installation is, and run the **ConfigOMNI** script to configure your Tivoli Netcool/OMNIbus, but ensure you do not select options to configure the SNMP probe or the Netcool/OMNIbus Knowledge Library. For more information, see "Configuring an existing Tivoli Netcool/OMNIbus installation" on page 51.
installTIP	0	Set the value to 1 to install and configure the Tivoli Integrated Portal, the Tivoli Netcool/OMNIbus Web GUI, and the Network Manager Web applications.
installITNM	0	Set the value to 1 to install and configure the Network Manager core components (the root cause analysis, event gateway, discovery and polling engines).
installNCIM	0	Set the value to 1 to install and configure Informix for use as the topology database.
complyFIPS	0	Set the value to 1 to use cryptographic routines that have been designed with FIPS 140–2 compliance in mind.
IALOCAL_ITNM_PASSWORD	--UserInput--	Provide a password for the default itnmadmin and itnmuser user accounts. If the Informix database account already exists on the operating system, enter the password used to access it.

Table 11. Response file parameters (continued)

Parameter	Default value	Description
PACKAGE.DIR. NCO	--UserInput--	If IBM Tivoli Netcool/OMNIbus is being installed on this system (in this case you would have set the installOMNI to 1 above) and the package is *not* in the same location as the install media, uncomment the PACKAGE.DIR.NCO variable, and change "--UserInput--" to the full path name where the Tivoli Netcool/OMNIbus package can be found on the system. Then uncomment the PACKAGE.NCO variable and change "--UserInput--" to the name of the directory or file containing Tivoli Netcool/OMNIbus. **Note:** The installer looks for the name plus a .tar, .tar.gz, .tar.Z or .zip suffix automatically, so do not add a suffix to the file name.
PACKAGE.NCO	--UserInput--	See the instructions for the PACKAGE.DIR.NCO parameter.
OMNIHOME	C:\\IBM\\tivoli\\ netcool\\omnibus	On Windows, if IBM Tivoli Netcool/OMNIbus is already installed on this system and you wish to configure it for use with Network Manager (in this case you would have set the installOMNI to 2 above), complete the following tasks. 1. Uncomment the OMNIHOME variable for a Windows directory. 2. Provide the full path name of the directory that contains Tivoli Netcool/OMNIbus.
OMNIHOME	/opt/IBM/tivoli/ netcool/omnibus	On UNIX, if IBM Tivoli Netcool/OMNIbus is already installed on this system and you wish to configure it for use with Network Manager (in this case you would have set the installOMNI to 2 above), complete the following tasks: 1. Uncomment the OMNIHOME variable for a UNIX directory. 2. Provide the full path name of the directory that contains Tivoli Netcool/OMNIbus.
IAGLOBAL_OBJE CTSERVER_PRI MARY_HOST	--UserInput--	If this installation will be connecting to an existing IBM Tivoli Netcool/OMNIbus (in this case you would have set the installOMNI to 0 above), then uncomment the IAGLOBAL_OBJECTSERVER_PRIMARY_HOST and provide the short name or IP address of the server where IBM Tivoli Netcool/OMNIbus is already installed.
IAGLOBAL_OBJE CTSERVER_PRI MARY_NAME	--UserInput--	Enter the name of the ObjectServer that is being installed, or that you want this installation to connect to.

Table 11. Response file parameters (continued)

Parameter	Default value	Description
IAGLOBAL_OBJECTSERVER_PRIMARY_PORT	4100	Enter the port for the ObjectServer that is being installed, or that you want this installation to connect to.
IAGLOBAL_OBJECTSERVER_USER	root	Enter the administrative user name for the ObjectServer that is being installed, or that you want this installation to connect to.
IALOCAL_OBJECTSERVER_PASSWORD	--UserInput--	Enter the administrative password of the ObjectServer that is being installed, or that you want this installation to connect to.
IAGLOBAL_WAS_defaulthost	16310	Enter the port to be used for the Tivoli Integrated Portal. Make a note of the port number, because you use this to connect to the Web applications.
IAGLOBAL_WASUserID	tipadmin	Enter a name to be used for the Tivoli Integrated Portal administrator account.
IALOCAL_WASPassword	--UserInput--	Enter a password to be used for the Tivoli Integrated Portal administrator account.
TIP_INSTALL_DIR	C:\\IBM\\tivoli\\tip	If you are installing on Windows, provide the fully qualified path to the directory where you want to install the Tivoli Integrated Portal. **Note:** Windows considers the backslash \ character to be an escape character, so use a double backslash \\ when defining the path on Windows.
TIP_INSTALL_DIR	/opt/IBM/tivoli/tip	If you are installing on UNIX, provide the fully qualified path to the directory where you want to install the Tivoli Integrated Portal.
IAGLOBAL_INSTALL_LOCATION_SELECTION	create	Set to create if you want to install the Tivoli Integrated Portal. Set to reuse if you want to use an existing Tivoli Integrated Portal.
authLDAP	1	Select this option to use LDAP authentication for Tivoli Integrated Portal users. If authLDAP and authOMNI are both uncommented, then LDAP will be used by default for new users. If neither authLDAP nor authOMNI are uncommented, then an internal file-based repository will be used.
authOMNI	1	Select this option to use the ObjectServer for authentication for Tivoli Integrated Portal users. If authLDAP and authOMNI are both uncommented, then LDAP will be used by default for new users. If neither authLDAP nor authOMNI are uncommented, then an internal file-based repository will be used.
IAGLOBAL_LDAP_NAME	--UserInput--	Enter the host name of the LDAP server.
IAGLOBAL_LDAP_PORT	389	Enter the port for the LDAP server.

Table 11. Response file parameters (continued)

Parameter	Default value	Description
IAGLOBAL_LDAP_REPOSITORY_ID	--UserInput--	Enter the repository identifier for the LDAP server.
IAGLOBAL_LDAP_PRIMARY_USER	tipadmin	Enter the name of the Tivoli Integrated Portal administrative user.
IAGLOBAL_LDAP_BIND_DN	"cn\=root"	Enter the bind name.
IALOCAL_LDAP_BIND_PASSWORD	--UserInput--	Enter the password for the bind name.
IAGLOBAL_LDAP_BASE_ENTRY	"o\=IBM,c\=US"	Enter the distinguished name.
IAGLOBAL_LDAP_GROUP_ENTITY	Group	Enter the group entity type.
IAGLOBAL_LDAP_GROUP_SUFFIX	"o\=IBM,c\=US"	Enter the correct identifiers for your **o**rganization and **c**ountry.
IAGLOBAL_LDAP_ORG_ENTITY	OrgContainer	Enter the organisation entity type.
IAGLOBAL_LDAP_ORG_SUFFIX	"o\=IBM,c\=US"	Enter the correct identifiers for your **o**rganization and **c**ountry.
IAGLOBAL_LDAP_USER_ENTITY	PersonAccount	Enter the person account entity type.
IAGLOBAL_LDAP_USER_SUFFIX	"o\=IBM,c\=US"	Enter the correct identifiers for your **o**rganization and **c**ountry.
IAGLOBAL_PRECISION_DOMAIN0	--UserInput--	Enter a name to be used as a network domain by Network Manager. Enter a descriptive name, for example, TESTNETWORK. The domain name must consist of between one and 11 characters (letters, numbers, or both), with the letters all capitals, no spaces, and no special characters. Make a note of the domain name, because it is used when starting components manually.
UI_Initial_Discovery	0	Set to 1 if you want the installation process to start a network discovery of your local subnet.
UI_Import_Netview	0	Set to 1 if you want the installation process to start a network discovery using information that you already exported from an IBM Tivoli NetView installation.
UI_Import_Other	0	Set to 1 if you want the installation process to start a network discovery using information from another network management application.

Table 11. Response file parameters (continued)

Parameter	Default value	Description
UI_No_Discovery	1	Set to 1 if you want to complete the installation process without starting a discovery. If you choose not to start a discovery now, you can start a discovery later the using the Discovery Configuration GUI.
UI_Subnet	--UserInput--	If you have selected to start a discovery, enter the IP address of the subnet to be discovered. Only IPv4 addresses can be entered here.
UI_Netmask	255.255.255.0	If you have selected to start a discovery, enter the netmask of the subnet. For a class C subnet, this is 255.255.255.0.
UI_SNMP_1	--UserInput--	If you have selected to start a discovery, you can enter up to six SNMP community strings (passwords).
UI_SNMP_2	--UserInput--	If you have selected to start a discovery, you can enter up to six SNMP community strings (passwords).
UI_SNMP_3	--UserInput--	If you have selected to start a discovery, you can enter up to six SNMP community strings (passwords).
UI_SNMP_4	--UserInput--	If you have selected to start a discovery, you can enter up to six SNMP community strings (passwords).
UI_SNMP_5	--UserInput--	If you have selected to start a discovery, you can enter up to six SNMP community strings (passwords).
UI_SNMP_6	--UserInput--	If you have selected to start a discovery, you can enter up to six SNMP community strings (passwords).
UI_Network_Nodes	--UserInput--	Enter the location of the output of the IBM Tivoli NetView migration script that you ran from the Launchpad as part of the installation prerequisites.
UI_Network_Nodes	--UserInput--	If you are seeding discovery from another Network Manager installation, enter the location of the file that contains a list of nodes in your network.
UI_SNMP_Strings	--UserInput--	If you are seeding discovery from another Network Manager installation, enter the location of the file that contains a list of community strings used in your network.
IAGLOBAL_NCIM_SERVER	informix	Enter the name of the server on which to install the NCIM topology database.
IAGLOBAL_NCIM_CREATE	yes	Set to no if you want to use an existing NCIM topology database.

Table 11. Response file parameters (continued)

Parameter	Default value	Description
IAGLOBAL_NCIM_PORT	3306	If you are using MySQL for the topology database, enter the port for the NCIM topology database.
IAGLOBAL_NCIM_USERNAME	ncim	If you are using MySQL for the topology database, enter the username for the administrator account for the NCIM topology database.
IALOCAL_NCIM_PASSWORD	--UserInput--	If you are using MySQL for the topology database, enter the password for the administrator account for the NCIM topology database.
connectMySQL	1	Uncomment this line if you want to use an existing MySQL database to hold the topology data.
connectDB2	1	Uncomment this line if you want to use an existing DB2 database to hold the topology data.
connectORACLE	1	Uncomment this line if you want to use an existing Oracle database to hold the topology data.
connectIDS	1	Uncomment this line if you want to use an existing Informix database to hold the topology data.
IAGLOBAL_NCIM_HOST	--UserInput--	If you are using an existing database to hold the topology data, enter the name or IP address of the host where the database is installed.
IAGLOBAL_NCIM_CREATE	yes	If you are using an existing database to hold the topology data, set this value to `yes` in order to create the NCIM database tables. Set this value to `no` if the NCIM database tables already exist.
IAGLOBAL_NCIM_PORT	3306	If you are using an existing MySQL database to hold the topology data, enter the port used by the database.
IAGLOBAL_NCIM_USERNAME	ncim	This is the user that the product uses to connect to the database. Do not change this value.
IALOCAL_NCIM_PASSWORD	--UserInput--	If you are using an existing MySQL database to hold the topology data, enter the password for the ncim user.
IAGLOBAL_NCIM_PORT	50000	If you are using an existing DB2 database to hold the topology data, enter the port used by the database.
IAGLOBAL_NCIM_DBNAME	--UserInput--	If you are using an existing DB2 database to hold the topology data, enter the name of the DB2 database instance that holds the topology data.

Table 11. Response file parameters (continued)

Parameter	Default value	Description
IAGLOBAL_NCIM_USERNAME	--UserInput--	If you are using an existing DB2 database to hold the topology data, enter the administrative username for the database
IALOCAL_NCIM_PASSWORD	--UserInput--	If you are using an existing DB2 database to hold the topology data, enter the password for the administrative user.
IAGLOBAL_NCIM_SQLLIB	--UserInput--	If you are using an existing DB2 database to hold the topology data, enter the local directory on this server that holds the DB2 client SQL commands. If this is a Windows installation, double backslashes // should be used between directories.
IAGLOBAL_NCIM_PORT	1521	If you are using an existing Oracle database to hold the topology data, enter the port used by the database.
IAGLOBAL_NCIM_DBNAME	--UserInput--	If you are using an existing Oracle database to hold the topology data, enter the system identifier used by the Oracle database holding the topology data.
IAGLOBAL_NCIM_USERNAME	--UserInput--	If you are using an existing Oracle database to hold the topology data, enter the administrative username for the database.
IALOCAL_NCIM_PASSWORD	--UserInput--	If you are using an existing Oracle database to hold the topology data, enter the password for the administrative user.
IAGLOBAL_NCIM_PORT	9088	If you are using an existing Informix database to hold the topology data, enter the port used by the database.
IAGLOBAL_IDS_SERVER_NAME	--UserInput--	If you are using an existing Informix database to hold the topology data, enter the Informix server name.
IAGLOBAL_IDS_DB_NAME	--UserInput--	If you are using an existing Informix database to hold the topology data, enter the Informix database name.
IAGLOBAL_NCIM_USERNAME	--UserInput--	If you are using an existing Informix database to hold the topology data, enter the administrative username for the database.
IALOCAL_NCIM_PASSWORD	--UserInput--	If you are using an existing Informix database to hold the topology data, enter the password for the administrative user.
StartDaemons	Start IBM Tivoli Network Manager before exiting	Uncomment this line if you want to start Network Manager before the installer exits.

Postinstallation tasks

After installing Network Manager, you might need to perform some postinstallation tasks.

Make sure you have successfully installed Network Manager.

To perform postinstallation tasks:

1. Ensure your Network Manager installation has completed.
2. Optional: If you use Tivoli Netcool/OMNIbus version 7.3.1 or earlier with Network Manager, you must follow additional post-installation steps to set up the automation for service-affected events (SAE), as described in "Configuring automations for service-affected events" on page 156.
3. Depending on the additional settings required, perform the steps in the following topics:

Option	Description
Non-root postinstallation tasks (UNIX only)	• Informix can only be installed by the root user. If you have installed Network Manager as non-root and want to use Informix, perform the steps described in "Installing and configuring Informix after a non-root installation" on page 224 • If you have a non-root installation and are installing Informix on a different server than where the GUI components are installed, you must install the Informix IConnect software as root on the GUI components server to use Cognos® reports. Perform the step described in "Configuring remote Informix for reporting" on page 225 • You can configure what user manages Network Manager processes, as described in "Configuring root/non-root permissions" on page 221
Postinstallation task for Informix on Windows	If you installed Network Manager with an Informix database on Windows, make sure you perform the steps described in "Configuring Informix disk space on Windows" on page 338
Postinstallation tasks for setting up Tivoli Common Reporting	If you want to use Informix, MySQL, or Oracle as the NCIM database, you must configure the databases before you can use Tivoli Common Reporting reports, as described in "Configuring NCIM for Tivoli Common Reporting" on page 256.
Upgrading from a previous Network Manager version	Follow steps described in "Upgrading and migrating to latest Network Manager" on page 127
Installing the Monitoring agent	If you want to use IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, follow the steps described in "Integrating with IBM Tivoli Monitoring" on page 210

Option	Description
For any further configuration tasks, check topics in:	Chapter 4, "Configuring Network Manager," on page 155
If you need to set up a topology database after installation for Network Manager.	For details of how to create the database schemas manually after installation, see the tasks about creating topology database schemas in the *IBM Tivoli Network Manager IP Edition Administration Guide*.
Fix Pack 4 Upgrading components for latest browser support	Fix Pack 4 To take advantage of the latest browser support, you might have to upgrade your Tivoli Integrated Portal level and apply the latest fix pack of Web GUI. For example, Network Manager 3.9 Fix Pack 4 includes Tivoli Integrated Portal 2.2.0.9 and Web GUI 7.4. However, to use Internet Explorer 10 or Mozilla Firefox 24 ESR, you need to upgrade to Tivoli Integrated Portal 2.2.0.13 and Web GUI Fix Pack 2. Fix Pack 4 To upgrade: 1. Go to the support site at http://www-933.ibm.com/support/fixcentral/ 2. Search for Tivoli Integrated Portal version 2.2.0.13 for your platform, and download it. 3. Search for Tivoli Netcool/OMNIbus 7.4 fix pack 2 (7.4.0.2) for your platform, and look for and download Web GUI Fix Pack 2 (also referred to as OMNIbus_GUI). 4. Follow the individual Fix Pack installation instructions to apply the Fix Packs.

Related tasks:

"Viewing the installation logs" on page 109
Viewing the installation logs can be useful for troubleshooting purposes.

Related reference:

"Postinstallation tasks run from launchpad fail on AIX 7" on page 115
When postinstallation tasks started from the launchpad on AIX 7 fail, make sure the X11 utilities (including xterm) are installed and set up properly to load graphical interfaces.

Troubleshooting the installation

Use this information to how to troubleshoot errors that might occur during the installation of Network Manager.

The following topics describe the types of error messages that you might encounter during the installation process, and the actions you can take to resolve these issues.

Viewing the installation logs

Viewing the installation logs can be useful for troubleshooting purposes.

Information about the success of the installation process is recorded in different log files. To view the installation log information, proceed as follows:

Consult the appropriate installation log:

Symptom	Action
For an overall idea about which part of the installation failed.	Examine the InstallAnywhere log file. 1. Go to the home directory of the user who ran the installer. 2. Open the InstallAnywhere log file. This has a filename like `IA-ITNM-Install-NN.log`, where *NN* is a number. Typically the file is called `IA-ITNM-Install-00.log`
The part of the installation that appears to have failed involves Tivoli Netcool/OMNIbus or the Network Manager core components	Examine the following logs: 1. Go to the directory `NCHOME/log/install` 2. Examine the logs in this directory: • `Configuration.log` shows errors encountered by post install setup tasks • Files with names of the form `ncp_create*.log` show errors that occurred during creation of the NCIM topology database • Windows `msi.log` shows errors encountered by Microsoft Installer. **Note:** If you install a new NCIM database on a remote server or use an existing database instance, the installation process generates a different set of log files than in the case of a single-server installation. In case of a remote or existing database installation, the following log and trace files are generated that are not created when installing a new database on the same server as Network Manager: • ncp_create_ncim_core_db.trace • ncp_create_ncim_pip_db.log • ncp_create_ncim_pip_db.trace • ncp_create_ncmib_db.trace • ncp_create_ncmonitor_db.trace • ncp_create_ncpgui_db.trace • ncp_create_ncpolldata_db.trace

Symptom	Action
For information about Tivoli Netcool/OMNIbus and Network Manager processes that run during the installation	Examine the following logs: • View information about the Tivoli Netcool/OMNIbus processes that were run during installation by reading the logs in this directory: `NCHOME/omnibus/log`. • View information about the Network Manager processes that were run during installation by reading the logs in this directory: `NCHOME/log/precision`.
The part of the installation which appears to have failed involves the Tivoli Integrated Portal	Examine the Composite Offering Installer (COI) logs: • The Composite Offering Installer (COI) logs are in *TIPHOME*`/_uninst/ITNM/plan/install/MachinePlan_localhost/*/logs`, where *TIPHOME* is the directory where the Tivoli Integrated Portal is installed. • There are separate logs for each step of the installation. You might be able to work out which step has had a problem from the InstallAnywhere log file, `~/IA-ITNM-Install-00.log`. • As a result of looking in the Composite Offering Installer (COI) log files, you might be able to determine whether the problem occurred in the IBM Autonomic Deployment Engine (DE), or Composite Offering Installer configuration steps.
The underlying problem with the Tivoli Integrated Portal installation might be in the IBM Autonomic Deployment Engine	Examine the Deployment Engine log files. You can locate these log files in the following locations: • If you are installing as root on UNIX, these will be in `/usr/ibm/common/acsi/logs/root`. • If you are installing as a non-root user on UNIX, these will be in `~/.acsi_$HOSTNAME/logs/$USER`. • If you are installing on Windows, these will be in `C:\Program Files (x86)\IBM\Common\acsi\logs\%USERNAME%`. • On 32 bit Windows, the directory is `C:\Program Files\IBM\Common\acsi\logs\%USERNAME%`.
The underlying problem with the Tivoli Integrated Portal installation might be in the Composite Offering Installer (COI) configuration steps	Examine the log files in *TIPHOME*`/logs`, where *TIPHOME* is the directory where the Tivoli Integrated Portal is installed.
It looks like the Tivoli Integrated Portal server itself has failed to start up successfully, even though there were no errors in any of the above log files,	Examine the log files in this directory: *TIPHOME*`/profiles/TIPProfile/logs/server1`. These log files contain information about the Tivoli Integrated Portal server status.
The part of the installation which appears to have problems involves Tivoli Common Reporting	Examine the following logs: • *TIP_components*`/TCRComponent/logs` • *TIP_components*`/TCRComponent/cognos/logs` **Note:** The default location for *TIP_components* is `/opt/IBM/tivoli/tipv2Components`.
The part of the installation which appears to have problems involves the BIRTExtension	Examine the logs in *TIP_components*`/BIRTExtension/logs`. **Note:** The default location for *TIP_components* is `/opt/IBM/tivoli/tipv2Components`.

Symptom	Action
The part of the installation which appears to have problems involves the ESSServer	Examine the logs in *TIP_components*/ESSServer/logs. **Note:** The default location for *TIP_components* is /opt/IBM/tivoli/tipv2Components.
There seem to be problems with installing the default Informix topology database	View information about the Informix processes that were run during installation by reading the logs in this directory: NCHOME/platform/*arch*/informix

TIPProfile_create log

Review the TIPProfile_create log when your installation ends in error.

Purpose

The TIPProfile_create log records the messages that result from the successful or failed completion of a task in the process of creating the Network Manager profile during installation.

Sample

This is a sample of the final records of a TIPProfile_create.log where errors were encountered.

```
<record>
  <date>2008-05-19T01:20:43</date>
  <millis>1211185243859</millis>
  <sequence>1007</sequence>
  <logger>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</logger>
  <level>INFO</level>
  <class>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</class>
  <method>areCommandLineArgumentsValid</method>
  <thread>10</thread>
  <message>Validation Error for profilePath: The profile path is not valid.
</message>
</record>
<record>
  <date>2008-05-19T01:20:43</date>
  <millis>1211185243859</millis>
  <sequence>1008</sequence>
  <logger>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</logger>
  <level>SEVERE</level>
  <class>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</class>
  <method>invokeWSProfile</method>
  <thread>10</thread>
  <message>Argument Validation Failed.</message>
</record>
<record>
  <date>2008-05-19T01:20:43</date>
  <millis>1211185243859</millis>
  <sequence>1009</sequence>
  <logger>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</logger>
  <level>INFO</level>
  <class>com.ibm.ws.profile.cli.WSProfileCLIModeInvoker</class>
  <method>invokeWSProfile</method>
  <thread>10</thread>
  <message>Returning with return code: INSTCONFFAILED</message>
</record>
<record>
  <date>2008-05-19T01:20:43</date>
  <millis>1211185243859</millis>
  <sequence>1010</sequence>
  <logger>com.ibm.wsspi.profile.WSProfileCLI</logger>
```

```
  <level>INFO</level>
  <class>com.ibm.wsspi.profile.WSProfileCLI</class>
  <method>invokeWSProfile</method>
  <thread>10</thread>
  <message>Returning with return code: INSTCONFFAILED</message>
</record>
```

Log files

Locate and review the logs and related files after an installation to confirm that the components were successfully installed.

Here are the logs created during a Network Manager installation. The installer creates a log called `IA-TIPInstall-xx.log`, which is located in the user's home directory. This should be the first log reviewed. It shows the installation as it progresses, giving tracing information. Each step that is executed in the installation creates a log in the *tip_home_dir*`/logs` directory.

Administrative console

```
createProfile.err
createProfile.out
createTIPService.err
createTIPService.out
deleteProfile.err (uninstall)
deleteProfile.out
enableAppSecurity.err
enableAppSecurity.out
extendJaveMemory.err
extendJaveMemory.out
modifyWASServiceName.err
modifyWASServiceName.out
removeTIPService.err (uninstall)
removeTIPService.out
```

Common Gateway Interface Server

```
CGIServer.err
CGIServer.out
configureIAuthzShLib.err
configureIAuthzShLib.out
deployiAuthzEar.err
deployiAuthzEar.out
```

Enterprise Storage Server®

```
deployESSApplication.err
deployESSApplication.out
ESSConfiguration.err
ESSConfiguration.out
osgiCfgInit.err
osgiCfgInit.out
```

IBM Tivoli Monitoring Web Service

```
ITMWebServiceEAR.err
ITMWebServiceEAR.out
```

Charting

```
assignChartAdminRole.err
assignChartAdminRole.out
TIPChartPortlet.err
TIPChartPortlet.out
```

Reporting Time Scheduling Services

```
TipTssEar.err
TipTssEar.out
TipTssEWASScheduler.err
TipTssEWASScheduler.out
```

TipTssJDBC.err
TipTssJDBC.out
TipTssSharedLibraries.err
TipTssSharedLibraries.out

Tivoli Common Reporting

tcr.err
tcr.out
tcrConfigClient.err
tcrConfigClient.out
tcrsPostConfig.err
tcrsPostConfig.out

Tivoli Integrated Portal

configureTIPTransformationShLib.err
configureTIPTransformationShLib.out
deployTIPChangePassdWar.err
deployTIPChangePassdWar.out
deployTIPRedirectorEar.err
deployTIPRedirectorEar.out
renameIdMgrRealm.err
renameIdMgrRealm.out

Virtual Member Manager

VMM.err
VMM.out

VMM LDAP Configuration

configureVMMLDAP.err
configureVMMLDAP.out

VMM ObjectServer Plugin

VMMObjectServerPlugin.err
VMMObjectServerPlugin.out

WebSphere

checkWAS.err
checkWAS.out
startWAS.err
startWAS.out

Viewing installed packages

Check that the installation worked by viewing the packages that the installer successfully installed. This check is useful for troubleshooting failed installations. Also, state the successfully installed and failed packages in the information that you submit to IBM Software Support as part of a service request.

1. Set the environment variables for the Deployment Engine (DE):
   - UNIX Linux Run `/var/ibm/common/acsi/setenv.sh`
   - Windows Run `C:\Program Files\IBM\Common\acsi\setenv.cmd`
2. To list the installed packages, run the command for your operating system and the user type that installed the product:

Operating system and user	Location
UNIX nonroot user	`/home/`*username*`/.acsi_`*username*`/bin/listIU.sh`
UNIX root user	`/usr/ibm/common/acsi/bin/listIU.sh`
Windows administrator user	`C:\Program Files\IBM\Common\acsi\bin\listIU.cmd`

Checking login URL and default ports

If you have trouble logging in, make sure you check the URL format and the ports you use after installation.

URL format

Check that your URL format entered is as follows (shows default ports):

- `https://`*`localhost`*`:16311/ibm/console` (secure access).
- `http://`*`localhost`*`:16310/ibm/console` (nonsecure access).

Where *localhost* is the fully-qualified host name or IP address of the Tivoli Integrated Portal server.

Default ports

16310 is the default nonsecure port number and 16311 is the default secure port number. If your environment was configured during installation with a port number other than the default, enter that number instead.

Dependency error messages

Dependency error messages are generated if the installation process cannot find a required Network Manager package or component.

If a dependency error message is displayed, follow the prompts and install the required components.

Running installation and maintenance procedures as root or non-root

The installation must be run by the same operating system user each time. Whichever user installs the first Tivoli Network Management product on a given workstation must also install, uninstall, or modify every subsequent Tivoli Network Management product on that workstation.

You can run the installation as a non-root user. However, certain Network Manager configuration actions must be performed by the `root` user. A wizard panel at the end of the installation wizard reminds you to log in as root and make these configurations manually.

Related concepts:

"Root and non-root installation" on page 221
On UNIX Network Manager can be installed as either the root user or a non-root user.

Related tasks:

"Configuring the core components to run as root" on page 222
On UNIX, if you installed Network Manager as a non-root user, you must perform additional configuration to run the core components as the root user.

Not enough disk space to complete the installation

If there is not enough disk space to complete the installation, an error message is displayed and the installation is aborted.

The error message is as follows:

```
There is not enough space in DIRECTORY to install the software
Please free up some space and re-run the installation
```

In this message, *DIRECTORY* refers to the specified root installation directory.

If you encounter this error message, clear space on the disk, or select a root directory on a partition with more space, and run the installation process again.

Console mode installation error

When installing Network Manager in console mode on UNIX systems, you might receive an error due to the DISPLAY environment variable being set.

If you receive the following error message when installing Network Manager in console mode on UNIX systems, you will need to remove the setting for the DISPLAY environment variable before starting the console mode installation:

```
Installing...

Invocation of this Java Application has caused an InvocationTargetException. This
application will now exit.

Stack Trace:
java.lang.NoClassDefFoundError: sun.awt.X11GraphicsEnvironment (initialization failure)
 at java.lang.J9VMIntervals.initialize(J9VMIntervals.java:140)
 at java.lang.Class.forNameImpl (Native Method)
 at java.lang.Class.forName(Class.java:136)
```

Use the following command: `unset DISPLAY`; then start the console install again.

Postinstallation tasks run from launchpad fail on AIX 7

When postinstallation tasks started from the launchpad on AIX 7 fail, make sure the X11 utilities (including xterm) are installed and set up properly to load graphical interfaces.

If you see the following error when starting postinstallation tasks from the launchpad:

```
Could not load program /usr/X11R7/bin/xterm:
Dependent module /usr/lib/libXpm.a(shr_64.o) could not be loaded.
Member shr_64.o is not found in archive
```

To correct the error, check where the `libXpm.a` library is pointing, for example:

```
ls -ln /usr/lib/libXpm.a
lrwxrwxrwx 1 0 0 26 May 17 10:06 /usr/lib/libXpm.a ->
/opt/freeware/lib/libXpm.a
```

In this example, `libXpm.a` is not pointing to the right location.

Make sure the `/usr/lib/libXpm.a` points to `/usr/lpp/X11/lib/R7/libXpm.a`. Use the following command to correct the link:

```
ln -s -f /usr/lpp/X11/lib/R7/libXpm.a /usr/lib/libXpm.a
```

Topology database fails to initialize

In case of memory and performance problems, the installation of the Informix database might fail with an error code 8 and the message `Informix failed to initialise`. To successfully install the database, you must increase the paging space, and set the timeout period for initialization to 600 seconds.

To increase the paging space to a total of 8 GB of memory, check the instructions for your operating system or contact your administrator.

To increase the timeout period and run the Informix installation again following an unsuccessful installation:

1. Set the Network Manager environment variables using `NCHOME/env.sh|.bat`, depending on your operating system.
2. Log in as the root user. Informix can only be installed by the root user.
3. Remove the Informix installation using the `NCHOME/bin/CleanSystem -i` script (the `-i` option removes the local Informix topology database).
4. Increase the timeout value in the Informix configuration script to 600 seconds by editing line 55 in `NCHOME/precision/install/scripts/install_ids_informix.ksh`.
5. Change to the `NCHOME/precision/install/scripts` directory.
6. Run the Informix installation script: `./install_ids_root|admin.ksh -f ../data/ids.properties`

Backing up and restoring the Deployment Engine

Use the Deployment Engine (DE) backup script before installing additional components or other products that are based on the Tivoli Integrated Portal platform. If you need to recover the original configuration after a failure, you can then run the Deployment Engine restore script.

The Deployment Engine performs the installation of new and upgraded products. It keeps track of the installed components and skips installing a given component if it is already present on the system. Perform the following steps to back up or restore the DE database.

1. From the command line, change to the `acsi` directory:
   - Windows `cd C:\Program Files\IBM\Common\acsi`
   - Linux UNIX For Linux and UNIX-based systems, the path to the `acsi` directory varies depending on whether you are installing as root or as a non-root user, as follows:
     - Installing as a non-root user, the path is relative to the user's home directory:
       <non-root user home directory>`/.asci_`*<user_name>*
     - Installing as root, the path is as follows:
       `/var/ibm/common/asci`
2. Initialize the Deployment Engine environment from the command line:
   - Windows `setenv.bat`
   - Linux UNIX `. setenv.sh`
3. Change to the `bin` directory:
   - Windows Change to the `bin` child directory, that is:
     `C:\Program Files\IBM\Common\acsi\bin`

- Linux UNIX For Linux and UNIX-based systems, the path to the `bin` directory varies depending on whether you are installing as root or as a non-root user, as follows:
  - For a non-root user, change to the `bin` child directory, that is: *<non-root user home directory>*`/.asci_`*<user_name>*`/bin`
  - For root, the path is as follows: `/usr/ibm/common/asci/bin`

4. Run the backup script to back up the Deployment Engine database, as follows:
   - Windows `de_backupdb.cmd`
   - Linux UNIX `de_backupdb`
5. If you need to restore the Deployment Engine database, from the `bin` directory run the restore script:
   - Windows `de_restoredb.cmd`
   - Linux UNIX `de_restoredb`

If you backed up the Deployment Engine database, you can run the installer now to add additional components or products. If you restored the Deployment Engine database, you can resume using the original installed environment.

Harmless installation messages

A review of the installation log might show error messages that are actually harmless.

After installing Network Manager, you might encounter a reflection error when reviewing the installation logs. The installation is successful, but the log shows variations of this error:

```
+++ Warning +++:   IWAV0003E Could not reflect methods for com.ibm.sec.iauthz.
InstanceAuthzServiceLocalHome because one of the methods references a type that
could not be loaded.
Exception: java.lang.NoClassDefFoundError: com.ibm.sec.iauthz.InstanceAuthorization
+++ Warning +++:   IWAV0002E Failed reflecting values
+++ Warning +++:   java.lang.NoClassDefFoundError: com.ibm.sec.
iauthz.InstanceAuthorization
```

This error can be safely ignored.

Insufficient disk space for install

Have enough space in the temporary directory for the installation or it will fail.

Your product installation requires at least 500 MB of disk space for the temporary files that are used during installation. On Linux and UNIX, allocate enough space in the /tmp or /opt directory of the computer.

Installation failure scenario

Review the IA-TIPInstall-xx.log for any errors that might have occurred during installation.

IA-TIPInstall-xx.log

Typically, the installation process stops when a failure occurs. But it can also appear to complete successfully and then later, such as when attempting to log in, you find that there is a problem. Review the IA-TIPInstall-xx.log in your home directory to confirm that the installation was successful. For example, if you are logged in as Administrator on a Windows system, then you would look in C:\Documents and Settings\Administrator.

Log review scenario

In this example on a Windows system, the ESSServerConfig.xml step failed and IA-TIPInstall-xx.log as shown here appears to have a COI (Composite Offering Installer) failure at line 134.

```
C:\IBM\tivoli\tip\_uninst\ITNM\plan\install\MachinePlan_localhost\
0011_IAGLOBAL_COI_STEP_ESSServerConfig\IAGLOBAL_COI_STEP_ESSServerConfig.xml:134:
xec returned: 105
 Wed May 28 15:25:54.078 EDT 2008 :  STDERR :
at org.apache.tools.ant.ProjectHelper.
addLocationToBuildException(ProjectHelper.java:539)
 Wed May 28 15:25:54.078 EDT 2008 :  STDERR :
at org.apache.tools.ant.taskdefs.Ant.
execute(Ant.java:384)
 Wed May 28 15:25:54.078 EDT 2008 :  STDERR :
at org.apache.tools.ant.Task.perform
(Task.java:364)
 Wed May 28 15:25:54.078 EDT 2008 :  STDERR :
at com.ibm.ac.coi.impl.utils.
AntHelper.ant(AntHelper.java:88)
 Wed May 28 15:25:54.078 EDT 2008 :  STDERR :  ... 3 more
```

The log provides you with the full path to the location of the failing file. Navigate to that location, open the file indicated, and check the line that failed. In this example you would navigate to:

```
C:\IBM\tivoli\tip\_uninst\ITNM\plan\install\MachinePlan_localhost\
00011_IAGLOBAL_COI_STEP_ESSServerConfig\IAGLOBAL_COI_STEP_ESSServerConfig.xml
```

and study line 134. At line 134 of target configureESS, the following command did not execute successfully

```
<target name="configureESS" depends="setProperties">
        <echo message="Start to configure Authentication Service..."/>
        <iaecho message="$ESSSERVER_CONFIGURING$"/>
                    ......................
line134:  <exec
dir="${IAGLOBAL_installLocation}/bin"
executable="${IAGLOBAL_installLocation}/bin/wsadmin${platform.script.ext}"
failonerror="true">
          <redirector output="${IAGLOBAL_installLocation}/logs/
ESSConfiguration.out" error="${IAGLOBAL_installLocation}/logs
/ESSConfiguration.err"/>
    ...
```

As you can see, the wsadmin call from Ant sends stdout to *tip_home_dir*/logs/ESSConfiguration.out and stderr to *tip_home_dir*/logs/ESSConfiguration.err. A review of the ESSConfiguration.out file shows that the Tivoli Integrated Portal Server (WAS) might have a problem:

```
WASX7209I: Connected to process "server1" on node TIPNode using SOAP connector;
The type of process is: UnManagedProcess
WASX7303I: The following options are passed to the scripting environment and
are available as arguments that are stored in the argv variable:
"[C:/IBM/tivoli/tip/logs/ltpaOutput.txt, 1ntegrate]"
WASX7017E: Exception received while running file "C:\IBM\tivoli\tip\bin
\configureESS.jacl";
exception information: com.ibm.bsf.BSFException: error while eval'ing
Jacl expression:
no accessible method "isESSConfigured" in class
com.ibm.ws.scripting.adminCommand.AdminTask
    while executing
"$AdminTask isESSConfigured"
    invoked from within
"set essCheck [$AdminTask isESSConfigured]"
```

Check the *tip_home_dir*/profiles/TIPProfile/logs/server1/SystemOut.log for any exceptions that might be related to the Authentication Service. If you are not able to assess this, ask the resident Tivoli Integrated Portal Server expert or gather the Network Manager logs, including SystemOut.log, and contact IBM Support.

Install fails after deployment engine upgrade

Running the installer on a computer that has an existing Tivoli Integrated Portal environment can fail if the deployment engine (DE) was upgraded from a very early version.

If you have an old version of the DE installed, the Tivoli Integrated Portal installer will upgrade it and continue with the installation. On rare occasions certain older versions of the DE might not be upgraded successfully. When this happens, the installation can fail. If you are aware that your product uses a very old version of the DE (such as Version 1.2), you can install on the same machine, but sign on to the portal with a different user name. If your old version of the DE was initially installed as root user on the Linux or UNIX operating system, consider uninstalling it if your new installation is failing after the DE upgrade.

Uninstalling Network Manager

You must use the scripts provided to uninstall the product.

On Windows, you must remove services for any additional domains before uninstalling the product.

Scripts are provided for you to uninstall either the whole product or certain components.

Important: You must always use the scripts to uninstall the product. Uninstalling the product by removing files and directories might result in problems reinstalling components.

Uninstalling on UNIX

On UNIX operating systems, use the uninstall script to uninstall the product. You can uninstall specific components or the entire product.

Attention: Do not attempt to remove any product by deleting files or directories. If you remove files or directories, problems can occur during reinstallation. Use the uninstall script that is provided with the product to uninstall Network Manager.

1. To remove any products that are integrated with Network Manager on the same server, remove them using their own uninstallers before you remove Network Manager. For example, remove Tivoli Netcool/OMNIbus by using the Tivoli Netcool/OMNIbus uninstaller. For information about uninstalling databases other than Informix, see the documentation for the database type.

   DB2 Before you remove a DB2 database, use the `uncatalog_db2_database` script to uncatalog the database. Also, ensure that you complete step 6 on page 121. A DB2 can be used as the NCIM topology database or as the Tivoli Data Warehouse. For more information about the use of DB2 as Tivoli Data Warehouse, see the *IBM Tivoli Monitoring for Tivoli Network Manager IP User's Guide*.
2. Source the environment by running the `$NCHOME/env.sh` command.
3. Run the uninstall script: `$NCHOME/Uninstall_ITNM`. This command starts the `$NCHOME/bin/CleanSystem` script. The command-line options are output on the interface. These options are described in the following table.

Table 12. **`Uninstall_ITNM`** *options*

Option	Description
`-p`	Stops all processes that are associated with the installation.
Informix `-i`	Removes the local topology database from the Network Manager installation. This option works only with the default Informix database that is included in the product. See step 5 on page 121 and complete this step applicable.
`-n`	Removes the Network Manager installation.
`-t`	Removes the Network Manager GUI and Tivoli Netcool/OMNIbus Web GUI components from the Tivoli Integrated Portal server. Use this option on the server where the Tivoli Integrated Portal is installed.
`-c`	Removes Tivoli Integrated Portal. The associated components Tivoli Common Reporting and Tivoli Netcool/OMNIbus Web GUI, the Composite Offering Installer (COI), and the IBM Autonomic Deployment Engine (DE) are also removed. **Note:** The use of the `-c` and `-a` options to remove Tivoli Integrated Portal, COI, and the DE can adversely affect other Tivoli products that are installed on the system. Ensure that no other Tivoli products on the system require those components before you use either option.

Table 12. **Uninstall_ITNM** *options (continued)*

Option	Description
`-a`	Removes all products and components that have files or data that is stored in NCHOME and TIPHOME locations, including backend and GUI components, Tivoli Netcool/OMNIbus, and Informix. **CAUTION:** **If you use this option, other products that are installed on the same server, such as Tivoli Netcool/OMNIbus, the Tivoli Netcool/OMNIbus Web GUI and IBM Tivoli Business Service Manager, might not function. Do not choose this option if you have any other Tivoli products that are installed on this server.**
`-h`	Use this option to specify the installation home directory if not using the default NCHOME.

4. Select the components that you want to remove by entering the appropriate option. You can specify more than one option.

   For example, to stop all processes and remove Network Manager and Tivoli Netcool/OMNIbus Web GUI components from the Tivoli Integrated Portal:

   ```
   ./Uninstall_ITNM -p -t
   ```

   Attention: Removing components can cause other dependent products to fail. Removing the core components or the topology database causes errors in the Network Manager web components.

5. Informix To remove an instance of Network Manager that was installed by a nonroot user and that uses an Informix database that was installed on the same server, run the **Uninstall_ITNM** script twice, as the root and nonroot user.
   a. Run `./Uninstall_ITNM -i` as the root user to remove the Informix database.
   b. As root user, ensure the `$NCHOME/netcool/platform/linux2x86/informix` directory is removed. If not, then delete it manually.
   c. Run `./Uninstall_ITNM -a` as the nonroot user that installed Network Manager.
6. DB2 After uninstallation and reinstallation of a DB2 database, recatalog the database. Use the `catalog_db2_database` script.
7. To reinstall Network Manager after it is removed, use a new shell window. Do not use the shell that was used to uninstall the previous Network Manager.

Related information:

Uninstalling Tivoli Netcool/OMNIbus V7.3.1 on UNIX

IBM DB2 information center

Uninstalling on Windows

You have several options to uninstall Network Manager on Windows operating systems.

Uninstalling using the wizard

To uninstall Network Manager using a GUI wizard on Windows operating systems, you must run the uninstall script with the swing option. You can uninstall specific components or the entire product in a command line mode.

If you want to remove any products that are integrated with Network Manager on the same server, remove them using their own uninstallers before removing Network Manager. For example, if you use a DB2 database for storing topology, you must remove it using the DB2 uninstaller.

Attention: Do not attempt to remove any component or product by deleting files or directories. This can cause problems reinstalling components. You must use the uninstall script provided with the product to uninstall Network Manager.

To uninstall all or part of Network Manager using the wizard, perform the following tasks:

1. Source the environment by running the `%NCHOME%\env.bat` command.
2. Run the `%NCHOME%\Uninstall_ITNM.exe` command with the `-i swing` option. The installation wizard starts and displays the components to be uninstalled. All components that were installed by the Network Manager installer are selected for removal.
3. Select the components that you want to remove.

   Attention: Removing components can cause other products that rely on those components to fail. For example, removing Tivoli Netcool/OMNIbus causes IBM Tivoli Business Service Manager to fail. Removing the core components or the topology database causes errors in the Network Manager Web components.

   CAUTION:
   If you remove the Network Manager web components from the Tivoli Integrated Portal, the Tivoli Netcool/OMNIbus Web GUI components are also removed.

   CAUTION:
   If you select the box to remove all components, the installation framework, and the Tivoli Integrated Portal, other products installed on the same server, such as Tivoli Netcool/OMNIbus, the Tivoli Netcool/OMNIbus Web GUI, and IBM Tivoli Business Service Manager, might not function. Do not choose this option if you have any other Tivoli products installed on this server.
4. Click **Next** to uninstall the components. If you are prompted to restart the server, you must restart the server before reinstalling any component of Network Manager.
5. DB2 Optional: If you are using a DB2 database for NCIM, you must uncatalog the database when you uninstall and catalog it again if you reinstall.

   Use the following command: Windows

   `%NCHOME%\precision\scripts\sql\db2\uncatalog_db2_database.bat` *database_name*

   where *database_name* is the name of the NCIM database.
6. DB2 Optional: If you are using a DB2 database as the Tivoli Data Warehouse database, you must uncatalog the database when you uninstall and catalog it again if you reinstall. For instructions, see the *IBM Tivoli Monitoring for Tivoli Network Manager IP User's Guide*.

Uninstalling in console mode

To uninstall Network Manager in console mode on Windows operating systems, you must run the uninstall script with the console option. You can uninstall specific components or the entire product in a command line mode.

If you want to remove any products that are integrated with Network Manager on the same server, remove them using their own uninstallers before removing Network Manager. For example, if you use a DB2 database for storing topology, you must remove it using the DB2 uninstaller.

Attention: Do not attempt to remove any product by deleting files or directories. This can cause problems reinstalling components. You must use the uninstall script provided with the product to uninstall Network Manager.

To uninstall all or part of Network Manager using the console mode, perform the following tasks:

1. Source the environment by running the `%NCHOME%/env.bat` command.
2. Run the `%NCHOME%\Uninstall_ITNM.exe` command with the `-i console` option.
3. Select the components that you want to remove and follow the on-screen prompts.

   Attention: Removing components can cause other products that rely on those components to fail. For example, removing Tivoli Netcool/OMNIbus causes IBM Tivoli Business Service Manager to fail. Removing the core components or the topology database causes errors in the Network Manager Web components.

   CAUTION:
   If you remove the Network Manager web components from the Tivoli Integrated Portal, the Tivoli Netcool/OMNIbus Web GUI components are also removed.

   CAUTION:
   If you select the option to remove all components, the installation framework, and the Tivoli Integrated Portal, other products installed on the same server, such as Tivoli Netcool/OMNIbus, the Tivoli Netcool/OMNIbus Web GUI and IBM Tivoli Business Service Manager, might not function. Do not choose this option if you have any other Tivoli products installed on this server.

4. DB2 Optional: If you are using a DB2 database for NCIM, you must uncatalog the database when you uninstall and catalog it again if you reinstall.

   Use the following command: Windows

   `%NCHOME%\precision\scripts\sql\db2\uncatalog_db2_database.bat` *`database_name`*

   where *database_name* is the name of the NCIM database.

5. DB2 Optional: If you are using a DB2 database as the Tivoli Data Warehouse database, you must uncatalog the database when you uninstall and catalog it again if you reinstall. For instructions, see the *IBM Tivoli Monitoring for Tivoli Network Manager IP User's Guide*.
6. If you are prompted to restart the server, you must restart the server before reinstalling any component of Network Manager

Uninstalling in silent mode

To uninstall Network Manager in silent mode on Windows operating systems, you must set up the response file and run the uninstall script with the silent option. You can uninstall specific components or the entire product in a command line mode.

If you want to remove any products that are integrated with Network Manager on the same server, remove them using their own uninstallers before removing Network Manager. For example, if you use a DB2 database for storing topology, you must remove it using the DB2 uninstaller.

Attention: Do not attempt to remove any product by deleting files or directories. This can cause problems reinstalling components. You must use the uninstall script provided with the product to uninstall Network Manager.

To uninstall all or part of Network Manager in silent mode, perform the following tasks:

1. Change to the installation directory.
2. Back up and edit the `ITNM-uninstall-response.txt` file.
3. To remove Network Manager, uncomment the following line and ensure that it is set to 1:

   ```
   #DEL.NCP.BOOLEAN=1
   ```

   Important: Removing Network Manager causes errors in the Network Manager Web components.
4. To remove the Network Manager Web Applications and Tivoli Netcool/OMNIbus Web GUI components (but not the Tivoli Integrated Portal), uncomment the following line and ensure that it is set to 1:

   ```
   #DEL.TIP.BOOLEAN=1
   ```
5. To remove Tivoli Netcool/OMNIbus, uncomment the following line and ensure that it is set to 1:

   ```
   #DEL.NCO.BOOLEAN=1
   ```

   Attention: Removing Tivoli Netcool/OMNIbus causes other products that rely on Tivoli Netcool/OMNIbus, such as IBM Tivoli Business Service Manager, to fail.
6. To remove all components in the NCHOME and TIPHOME directories, including the installation framework, uncomment the following line and ensure that it is set to 1:

   ```
   #DEL.ALL.BOOLEAN=1
   ```

   CAUTION:
   If you select the option to remove all components, the installation framework, and the Tivoli Integrated Portal, other products installed on the same server, such as Tivoli Netcool/OMNIbus, the Tivoli Netcool/OMNIbus Web GUI, and IBM Tivoli Business Service Manager, might not function. Do not choose this option if you have any other Tivoli products installed on this server.
7. Save the `ITNM-uninstall-response.txt` file.
8. Source the environment by running the `%NCHOME%\env.bat` command.
9. Run the `%NCHOME%\`**`Uninstall_ITNM.exe`** command with the `-i silent -f` *`path to response file`* option. For example:

   ```
   Uninstall_ITNM.exe -i silent -f C:\temp\ITNM-uninstall-response.txt
   ```

Important: If the response file is not specified or not found, the uninstaller removes those components that were installed the last time that the installer was run.

10. If you are prompted to restart the server, you must restart the server before reinstalling any component of Network Manager.
11. DB2 Optional: If you are using a DB2 database for NCIM, you must uncatalog the database when you uninstall and catalog it again if you reinstall.

    Use the following command: Windows

    ```
    %NCHOME%\precision\scripts\sql\db2\uncatalog_db2_database.bat database_name
    ```

    where *database_name* is the name of the NCIM database.
12. DB2 Optional: If you are using a DB2 database as the Tivoli Data Warehouse database, you must uncatalog the database when you uninstall and catalog it again if you reinstall. For instructions, see the *IBM Tivoli Monitoring for Tivoli Network Manager IP User's Guide*.

Installing fix packs

To obtain the latest fixes, apply fix packs. Fix packs are available for the Network Manager product and also for other products and components such asTivoli Integrated Portal and the Tivoli Netcool/OMNIbus Web GUI. You can download fix packs from IBM Fix Central. Ensure that you keep the fix pack level up to date.

A fix pack consists of the installation image, and install file and readme files. The installation images are named by product, operating system, and fix pack level, for example `3.9.0-TIV-ITNMIP-zLinux-FP0003`. Fix packs are cumulative. For example, fix pack 3 includes all fixes from earlier fix packs.

For information about which versions of Tivoli Integrated Portal are supported with Network Manager, see the Tivoli Integrated Portal certification matrix on IBM DeveloperWorks. For example, certain versions of Tivoli Integrated Portal V2.2.0.x are supported only with Network Manager fix pack versions.

Important: The refresh of the Network Manager full product image (build level 3.9.0.71, which was released 2012 September 14) includes all fixes in fix pack 2 and also contains changes to the base image. You can apply fix packs that are released after fix pack 2 to the base GA image and to the refresh of the full product image.

Note: Fix Pack 5 If you are installing Network Manager V3.9 Fix Pack 5, and you want to use Oracle 12c for your topology database, then you must perform the installation in the following order:

1. Install Network Manager V3.9 Fix Pack 5, as described in this topic.
2. Create and populate your Oracle 12 database.
3. Reconfigure Network Manager core and GUI to connect to the new Oracle 12c database, as described in Changing the NCIM access details.

1. To identify the current version of Network Manager processes, run the processes with the `-version` option.
2. Download the fix pack from Fix Central at http://www-933.ibm.com/support/fixcentral/. Then, extract the fix pack installation image.
3. Read the information in the files that are associated with the fix pack. A Network Manager fix pack includes information in the following files. Other products and components have different files.
   - `README.1ST`: Gives the location of the `INSTALL` and `README` files.

- `INSTALL`: Gives important information about installing the fix pack, including preinstallation, installation, and postinstallation steps, and restrictions and requirements.
- `README`: Describes the fixes and enhancements that are included in the fix pack.

4. Stop any running Network Manager processes. For more information about stopping the product, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.
5. Install the fix pack as described in the `INSTALL` file.
6. Fix Pack 4 After the fix pack is installed, perform the following tasks if applicable for your deployment:
   - Check the `$NCHOME/log/install/manuallyUpdate.log` file, which lists configuration files that need to be manually changed. During the installation of the fix pack, the installer checks these files for changes from the defaults. If changes are found, these files are not overwritten. In these files, replace all instances of all occurrences of `list type text` with `list type undef`. For example, the following statement needs to be changed:

     ```
     connects&1 = "eval(list type text, '&RelatedTo')",
     ```

     This sample statement needs to be changed so that it reads as follows:

     ```
     connects&1 = "eval(list type undef, '&RelatedTo')",
     ```

   - Copy the `CleanSystem` script from the `$NCHOME/precision/install/scripts` directory to the `$NCHOME/precision/bin` directory. These scripts are updated in this fix pack.
   - For 64-bit distributed environments that are secured by SSL: On the Network Manager host, change the JRE level of the **`nc_common`** utility. Edit `$NCHOME/bin/nc_common` and change all `NCO_JRE` entries to `NCO_JRE_64_32`. This change is not required in single-server environments.
   - If your installation of Tivoli Netcool/OMNIbus is at V7.4 fix pack 2 or later, uncomment the following line in the `$NCHOME/probes/`*`arch`*`/nco_p_ncpmonitor.props` file, where *arch* represents your operating system. Then, restart the **`nco_p_ncpmonitor`** process.
     - UNIX `NHttpd.ConfigFile: "$NCHOME/omnibus/etc/libnhttpd.json"`
     - Windows `NHttpd.ConfigFile: "%NCHOME%\\omnibus\\etc\\libnhttpd.json"`
   - Run the **`ncp_mib`** command with the `-override` option. This command loads any changes to MIB files.
7. In the `README` file, check for known problems with the fix pack and make any changes that are necessitated by APAR fixes.

Related information:

Tivoli Integrated Portal certification matrix on IBM DevelopWorks

Chapter 3. Upgrading and migrating

Read about upgrading your version of Network Manager and migrating existing installations.

Note: The default ports for logging into the application server are different across versions. The nonsecure access redirects you to the secure port unless you configured it otherwise (see "Configuring access for HTTP and HTTPS" on page 205). The default ports for the Network Manager V3.9 release are as follows:

- `https://localhost:16311/ibm/console` (secure access).
- `http://localhost:16310/ibm/console` (nonsecure access).

Restriction: Only the following configurations are supported when upgrading to Network Manager V3.9 from V3.7 or V3.8, or when copying an existing V3.9 installation:

- You can migrate from any UNIX system to any other UNIX system, but migrating from UNIX systems to Windows systems, or the reverse, is not supported.
- The source and target machines must use the same database type. The only exception is if you migrate from the previously default MySQL source to the default Informix in V3.9 on the target system.
- The source and target systems must both be either FIPS or non-FIPS installations. Migration from a FIPS installation to a non-FIPS installation, or the reverse, is not supported.

Attention: If you have multiple Tivoli products that use the Tivoli Integrated Portal framework, see the *Cross Product Migration Reference* at https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/Tivoli%20Business%20Service%20Manager1/page/Migration for dependencies and considerations when upgrading and migrating.

Upgrading and migrating to latest Network Manager

You can upgrade to Network Manager V3.9 from versions 3.7 or 3.8.

Upgrading and migrating to the latest version of Network Manager involves collecting data from your existing Network Manager installation, exporting the data, installing the new version of Network Manager, and importing the data to your new installation.

Note: You must run the export-import scripts as the same user that installed the product.

The different versions of Network Manager and related components use different directory structures and have configuration files in different locations. This is mainly due to changes in the framework over releases. For example, Network Manager V3.8 uses Tivoli Integrated Portal 1.1.x, Network Manager V3.9 uses Tivoli Integrated Portal V2.1, and Network Manager V3.7 uses Netcool GUI Foundation. For an overview of where to find files, see Table 13 on page 128.

As a reference, the following table contains an overview of how the default location of configuration files has changed over the releases.

Table 13. Default locations of configuration files

Item	Location in version 3.7	Location in version 3.8	Location in version 3.9
NCHOME	• UNIX `/opt/IBM/tivoli` • Windows `C:\IBM\tivoli`	• UNIX `/opt/IBM/tivoli/netcool` • Windows `C:\IBM\tivoli\netcool`	• UNIX `/opt/IBM/tivoli/netcool` • Windows `C:\IBM\tivoli\netcool`
ITNMHOME	Not applicable	Not applicable	• UNIX `/opt/IBM/tivoli/netcool/precision` • Windows `C:\IBM\tivoli\netcool\precision` **Note:** By default, PRECISION_HOME is set to the same location as ITNMHOME, but is used by other parts of the product.
TIPHOME	Not applicable	• UNIX `/opt/IBM/tivoli/tip` • Windows `C:\IBM\tivoli\tip`	• UNIX `/opt/IBM/tivoli/tipv2` • Windows `C:\IBM\tivoli\tipv2`
GUI properties files	NCHOME/etc/precision	TIPHOME/profiles/TIPProfile/etc/tnm	ITNMHOME/profiles/TIPProfile/etc/tnm
Dynamic view templates	NCHOME/etc/precision/dynamictemplates	TIPHOME/profiles/TIPProfile/etc/tnm/dynamictemplates	ITNMHOME/profiles/TIPProfile/etc/tnm/dynamictemplates
Right-click menu and tool definition files	NCHOME/etc/precision/menus	TIPHOME/profiles/TIPProfile/etc/tnm/menus	ITNMHOME/profiles/TIPProfile/etc/tnm/menus
	NCHOME/etc/precision/tools	TIPHOME/profiles/TIPProfile/etc/tnm/tools	ITNMHOME/profiles/TIPProfile/etc/tnm/tools
GUI icon files	NCHOME/etc/precision/resource	TIPHOME/profiles/TIPProfile/etc/tnm/resource	ITNMHOME/profiles/TIPProfile/etc/tnm/resource
WebTools configuration files	NCHOME/etc/precision/tools	TIPHOME/profiles/TIPProfile/etc/tnm/tools	ITNMHOME/profiles/TIPProfile/etc/tnm/tools

Upgrading and migrating overview

Use this information as a step-by-step guide to upgrading Network Manager and migrating existing settings to the upgraded version.

Upgrading and migrating steps from Network Manager V3.8

Moving to the latest version of Network Manager from V3.8 involves several steps. The process uses separate scripts for moving the core and the GUI component settings across to the new installation.

To upgrade to Network Manager V3.9 from V3.8 and migrate your settings and customizations, perform the steps discussed in the following table.

Table 14. Upgrading and migrating tasks from Network Manager V3.8

Action	Step
1. Prepare your existing system.	"Preparing for upgrade" on page 131
2. Export core customization data.	"Exporting customization data" on page 132
3. Export GUI configuration data.	"Exporting V3.8 GUI data" on page 133
4. Install Network Manager V3.9.	Chapter 2, "Installing," on page 51 **Important:** If you are installing V3.9 on the same server as an existing installation of V3.8, you must perform the following extra tasks: • Use a new directory to install V3.9. • Do not change the existing directory used by V3.8, even if you plan to remove V3.8 later. • Install V3.9 using the same user account that was used to install V3.8. • Choose different ports for V3.9 to avoid conflicts. • On non-Windows platforms, use separate terminal windows for any migration and installation steps as well as for all commands for running the products. • Ensure that you use the correct environment variables for the appropriate version. Note that on Windows, you cannot run V3.8 after installing V3.9
5. Install IBM Tivoli Netcool/OMNIbus	You can install IBM Tivoli Netcool/OMNIbus as part of your Network Manager installation. For information about upgrading and migrating IBM Tivoli Netcool/OMNIbus, see the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*. **Note:** If you installed a new instance of IBM Tivoli Netcool/OMNIbus as part of the Network Manager installation, the ObjectServer name you provided during the installation is stored in `NCHOME/etc/precision/ConfigItnm.Network_Manager_Domain_Name.cfg`

Table 14. Upgrading and migrating tasks from Network Manager V3.8 (continued)

Action	Step
6. Import previous core configuration data into your new installation.	"Importing customization data" on page 135 **Note:** Any configuration files exported from your previous V3.8 installation and imported into Network Manager V3.9 that contain passwords or other strings originally encrypted using V3.8 encryption tools, will be reencrypted using FIPS 140–2 compliant encryption tools as part of this upgrade. Version 3.9 files that are replaced by migrated V3.8 files during the update process are backed up with the name *filename*_39, where *filename* is the name of the original version 3.9 file.
7. Due to changes in the product, some core configuration settings must be migrated manually to the new system.	"Importing customization data - manual steps" on page 137
8. Import previous GUI configuration data into your new installation	"Importing V3.8 GUI data" on page 143
9. Due to changes in the product, some GUI configuration settings must be migrated manually to the new system.	"Importing V3.8 GUI data - manual steps" on page 144
10. Identify modifications made to the NCIM topology database schema	"Identifying NCIM topology database customizations" on page 146
11. Stop and start Network Manager, including the Tivoli Integrated Portal.	Starting and stopping Network Manager

Upgrading and migrating steps from Network Manager V3.7

Moving to the latest version of Network Manager from V3.7 involves several steps. The process uses one export script to collect all data and one import script to add the collected data to the new installation. You need to run the scripts on all machines if you have a distributed environment with Network Manager components installed on multiple servers.

To upgrade to Network Manager V3.9 from V3.7 and migrate your settings and customizations, perform the steps discussed in the following table.

Table 15. Upgrading and migrating tasks from Network Manager V3.7

Action	Step
1. Prepare your existing system.	"Preparing for upgrade" on page 131
2. Export core and GUI customization data.	"Exporting customization data" on page 132
3. Install Network Manager V3.9.	Chapter 2, "Installing," on page 51
4. Install IBM Tivoli Netcool/OMNIbus	You can install IBM Tivoli Netcool/OMNIbus as part of your Network Manager installation. For information about upgrading and migrating IBM Tivoli Netcool/OMNIbus, see the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*. **Note:** If you installed a new instance of IBM Tivoli Netcool/OMNIbus as part of the Network Manager installation, the ObjectServer name you provided during the installation is stored in `NCHOME/etc/precision/ConfigItnm.Network_Manager_Domain_Name.cfg`

Table 15. Upgrading and migrating tasks from Network Manager V3.7 (continued)

Action	Step
5. Import previous core and GUI configuration data into your new installation.	"Importing customization data" on page 135 **Note:** Any configuration files exported from your previous V3.7 installation and imported into Network Manager V3.9 that contain passwords or other strings originally encrypted using V3.7 encryption tools, will be reencrypted using FIPS 140–2 compliant encryption tools as part of this upgrade. Version 3.9 files that are replaced by migrated V3.7 files during the update process are backed up with the name *filename*_39, where *filename* is the name of the original version 3.9 file.
6. Due to changes in the product, some configuration settings must be migrated manually to the new system.	"Importing customization data - manual steps" on page 137
7. Identify modifications made to the NCIM topology database schema	"Identifying NCIM topology database customizations" on page 146
8. Stop and start Network Manager, including the Tivoli Integrated Portal.	Starting and stopping Network Manager

Preparing for upgrade

Prepare your existing system for upgrade by copying over the files required for the upgrading and migrating process. The Network Manager installation package contains all files required.

If you want to upgrade to Network Manager V3.9 Fixpack 5, you must first update the following import and export scripts: `$NCHOME/precision/install/scripts/nmExport`, `$NCHOME/precision/install/scripts/nmImport`, and `$NCHOME/scripts/upgrade/ITNMExportNetworkViews.pl`. After you install Network Manager Fixpack 5, copy the `nmExport` and `nmImport` scripts to the `scripts` directory in the location where you uncompressed the installation file for the major version of Network Manager. Alternatively, if you are using `ExportPackage.tar`, copy the scripts to the `scripts` directory where you uncompressed the `.tar` file. You cannot run these scripts from an existing installation or from a Fixpack installation. Also copy the `ITNMExportNetworkViews.pl` script to the `migration/bin/` directory of the same location.

Prepare for the upgrade:

1. Go to where you placed your Network Manager V3.9 installation package.
2. Locate the UNIX `ExportPackage.tar` or Windows `ExportPackage.zip` depending on your operating system.
3. Copy the compressed file to your existing Network Manager installation. If you have core and GUI components on more than one server, then copy the file to each of them.
4. Extract the files to a temporary location. The files and utilities required for the upgrading and migrating process are available after extracting the compressed file. The main items that require attention are as follows:
   - The `launchpad` utility: Use this utility to start the launchpad GUI from where you can run a data collection on your previous installation. The data collected then can be exported for applying to new installations. An import utility is also provided for use on your new installation. You can use a GUI or command line to start and use this utility.

Note: You can use the export utility to collect data on Network Manager versions 3.7, 3.8, or even 3.9 installations. If you have a Network Manager version 3.7 installation, the utility also exports the Netcool GUI Foundation data.

- The `Preupgrade.tar` or `Preupgrade.zip` file: Contains utilities for exporting previous GUI settings on Network Manager V3.8 and then importing them into your new installation.

  Note: This file is only needed for the export-import of V3.8 GUI component data.

5. Poll policy names and poll definition names must be unique. In previous releases of Network Manager, a known limitation allowed duplicate poll policy names or duplicate poll definition names to be created. In Network Manager V3.9, duplicate poll policy names or poll definition names are not allowed. If you have created poll policies or poll definitions with the same name on your previous V3.7 or V3.8 installation, then you must rename one of each duplicate pair to make sure that each poll policy and each poll definition name is unique on your system. You must do this before performing any data export.

   Note: The poller must be running when you perform the rename operation. This is required for the names to be propagated appropriately to database fields requiring this information (for example, historical poll data when migrating from a V3.8 system).

Exporting customization data

You must collect and export your previous version's customization data to make it available for importing to your Network Manager V3.9 installation.

To use the launchpad, you need a supported browser installed on the server. Make sure you have copied the UNIX `ExportPackage.tar` or Windows `ExportPackage.zip` file from the Network Manager V3.9 installation package to each server where your existing Network Manager installation has components.

To export customization data, perform the following steps:

1. On each server where components of your previous version are installed, go to where you extracted `ExportPackage`, and run the data export script:
   - To run the script from the installer launchpad, start the launchpad by running the UNIX **`launchpad.sh`** script on UNIX or the Windows **`launchpad.exe`** executable on Windows, select the **Preinstallation and Migration** menu item, expand the **Upgrading from an existing Network Manager** section, and click **Export Network Manager Data**.
   - To run the script from the command line, run the UNIX **`nmExport`** script on UNIX or the Windows **`nmExport.bat`** script on Windows from the `scripts` subdirectory.

   Note: You must run the script as the same user that installed the product.

   Restriction: Historical polling data is not collected when exporting data from V3.7 systems. Exporting historical polling data from V3.8 systems is optional. The export and import of historical polling data from V3.8 systems can be time consuming depending on the amount of data being migrated.

2. Provide the answers to the prompts. Depending on the version of your previous Network Manager installation, the following data is extracted and saved into an export file in a location of your choice (`.pkg` on UNIX systems or `.zip` on Windows systems):
   - For version 3.7: domain data, configuration files, cache files, extra MIB files, GUI-specific configurations including Netcool GUI Foundation pages and network views, poll policies, reports, and passwords.
   - For version 3.8: domain data, discovery configuration data, network views, and poll policies.

     Note: For V3.7 installations, all core and GUI component data is collected. For V3.8 installations, only core component data is collected. To collect version 3.8 GUI component data, you must run another script, as described in "Exporting V3.8 GUI data." You do not need to run this script for V3.7.

   Note: The export process creates its own log files. If successful, all related log files are bundled into the `.pkg` or `.zip` export package file, making them available on the updated system. If the process fails, the package is not created and the logs are saved to the user's home directory:
   - UNIX `$HOME/itnmExportLogs`
   - Windows `%UserProfile%\itnmExportLogs`
3. If you are installing Network Manager V3.9 on a different server, copy all the exported data to that server, or servers, making the data available for importing to the new systems.
4. If you are also exporting Netcool/OMNIbus customization data, copy all the exported data to the server where you want to install Netcool/OMNIbus.

After exporting customization data, you must install Network Manager V3.9 and then import the customization data.

Related reference:

"Supported browsers for the installer launchpad" on page 43
To run the installer launchpad, ensure that a supported browser is installed. The supported browsers for the installer launchpad are not necessarily the same as the supported browsers for the web applications.

Exporting V3.8 GUI data

You must export your previous V3.8 GUI customization data before installing Network Manager V3.9.

To use the launchpad, you need a supported browser installed on the server. Make sure you have copied the UNIX `ExportPackage.tar` or Windows `ExportPackage.zip` file from the Network Manager V3.9 installation package to the server where your existing V3.8 GUI components are installed.

Restriction: The upgrade process does not export unmanaged device data. When you have completed network discovery on your target system, you must manually set the relevant devices to unmanaged state again.

To export GUI customization data, perform the following steps:

1. On each server where GUI components of your previous V3.8 system are installed, go to where you extracted `ExportPackage`.

2. Extract the UNIX `Preupgrade.tar` or Windows `Preupgrade.zip` file to `TIPHOME/profiles/TIPProfile`.
3. Run the GUI data export script:
   - To run the script from the installer launchpad, start the launchpad by running the UNIX **`launchpad.sh`** script on UNIX or the Windows **`launchpad.exe`** executable on Windows, select the **Preinstallation and Migration** menu item, expand the **Upgrading from an existing Network Manager** section, and click **Export Network Manager GUI Data**.
   - To run the script from the command line, change to the `scripts` subdirectory and depending on your operating system, run the UNIX **`nmGuiExport`** or the Windows **`nmGuiExport.bat`** command as follows:

     ```
     nmGuiExport | bat -u TIP administrator user name -p password for TIP
     administrator -d location of the TIP installation to be migrated
     ```

     Note: If no values are provided, you are prompted to enter values. If the location of the Tivoli Integrated Portal installation to be migrated is not provided, the environment variable `TIPHOME` is used. If `TIPHOME` does not exist, you are prompted to enter a location.

   Note: You must run the script as the same user that installed the product. The following data is extracted and saved into the `TIPHOME/profiles/TIPProfile/upgrade/data/upgradeData.zip` export file:
   - User roles: The export saves the roles for users that existed in V3.8, and applies the roles to the same user if the same user exists in V3.9.

     Note: Actual users defined for the V3.9 environment need to be created separately in the appropriate repository (LDAP or ObjectServer).
   - Custom Tivoli Integrated Portal Pages, Views, and Roles.
   - Reports.

   The export process creates its own log files in the following directories:
   - `TIPHOME/profiles/TIPProfile/upgrade/logs`
   - `TIPHOME/profiles/TIPProfile/logs`
4. Create users for V3.9 as required in the appropriate repository (LDAP or ObjectServer).
5. If you are installing Network Manager V3.9 GUI components on a different server, copy the `upgradeData.zip` export file to that server, making the data available for importing to the new system. If you are installing on separate servers, make sure you copy the relevant data to the server where you want to install the component.

After exporting customization data, you must install Network Manager V3.9 and then import the customization data.

Importing customization data

After installing Network Manager V3.9, you can import your previous version's customization data.

Before you can import customization data, you must export the data from your previous installation and install version 3.9.

Important: You must run ncp_mib if you have copied over custom MIBs as part of this data migration. If you do not do this then processes such as the SNMP helper, ncp_dh_snmp, will not start up when you start Network Manager.

To import customization data, perform the following tasks:

1. Log in to your previous installation. If you had a distributed setup, you must log in to each server containing components of your previous installation and repeat the following steps for each server.
2. Copy the export file (`.pkg` on UNIX systems or `.zip` on Windows systems) to the server where you installed Network Manager V3.9. You might have more than one export file depending on whether you had a distributed environment.
3. On your new installation, make sure that the Network Manager core components for each domain are running. To do this, use the Windows Services GUI on Windows systems, or use the following command on UNIX systems: **`itnm_start`** `ncp -domain` *`DOMAIN`*. For example, to start the `NCOMS` domain, type: `itnm_start ncp -domain NCOMS` . This ensures that Network Manager is fully initialized and the domain tables are populated. You must stop the core components again to do the import itself, as described in the next step.
4. Stop the Network Manager core components for each domain on your new installation using the Windows Services GUI on Windows systems, or using the following command on UNIX systems: **`itnm_stop`** `ncp -domain` *`DOMAIN`*. For example, to stop the `NCOMS` domain, type: `itnm_stop ncp -domain NCOMS`

   Note: If you do not specify a domain name with **`itnm_stop`**, it stops the default domain created at installation.
5. On your new installation, go to where you placed your installation package.

   Note: If you are migrating from V3.7, the Tivoli Integrated Portal server must be running to import GUI component data.
6. Run the data import script using one of the following methods:
   - To run the script from the installer launchpad, start the launchpad by running the UNIX **`launchpad.sh`** script on UNIX or the Windows **`launchpad.exe`** executable on Windows, select the **Postinstallation** menu item, expand the **Upgrading from an existing Network Manager** section, and click **Import Network Manager Data**.
   - To run the script from the command line, run the UNIX **`nmImport`** script on UNIX or the Windows **`nmImport.bat`** script on Windows from the `scripts` subdirectory of the installation media.

   Note: You must run the script as the same user that installed the product.
7. When prompted, provide the path to the `.pkg` or `.zip` file that contains the customization data that you previously exported.
8. Answer the various other questions the import process asks.

   Note: The following question requires special attention:

```
Allocate new entityIds during import [ N ]
```

Each device in the system has an entityId. The import process can preserve the entityIds or allocate new entityIds. If you answer no, then each device maintains the entityId from the previous installation. This is necessary when you have links to external systems that use Network Manager data, for example, Tivoli Data Warehouse.

If you answer yes, devices are allocated new entityIds.

To preserve entityIds, the target system needs to be empty. If the target system is not empty (for example, due to a previous data import or discovery), preserving entityIds might become a complex operation due to potential clashes between existing entityIds and the ones being imported, and the results may be unpredictable. Therefore, merging of domain data is not supported.

Attention: If you have a domain on the target system that has the same name as on your previous system, then make sure the domain on the target system does not contain data. Domain names cannot be changed during the migration process.
The exported data is imported into the new installation. Your passwords are unencrypted, imported, and re-encrypted.

Important: The data imported depends on the version of your previous Network Manager installation. For V3.7 installations, the import of all previous data is handled by this script. For V3.8 installations, core component data is imported, while GUI component data is imported by the script described in "Importing V3.8 GUI data" on page 143.

The import process creates its own log files. Logs from the import process are saved to NCHOME/log/precision:

- ITNMDataImport.log
- ITNMImportHistoricalData.log
- get_policies.*domain name*.log
- ITNMImportNetworkViews.log

The export-import process automatically detects and recreates the domains from a previous install. The import script detects the potential domains from the previous system based on the data files. Using the **domain_create.pl** script, the process automatically creates domains on the new installation using the domain names from the previous system. After the domains have been created, the main topology and policy data are imported for each.

The **domain_create.pl** script creates the discovery configuration files for the new domains in NCHOME/etc/precision using the values in the configuration files of the default domain. The import process saves the imported files in the NCHOME/etc/precision/migration directory as read-only files. You can use the imported files to manually update the newly created files in NCHOME/etc/precision.

Attention: You might receive warning messages referencing deprecated data types. These warning messages indicate planned changes in data types between releases and can be ignored. The following is an example:

```
Level: INFO Message: ncp_config command:- "/opt/IBM/tivoli/netcool/
precision/bin/ncp_config" -domain CC -read_schemas_from
"/opt/IBM/tivoli/netcool/var/precision/export/importPending"
-write_schemas_to "/opt/IBM/tivoli/netcool/etc/precision" -schema
DiscoCollectorFinderSchema.cfg
Sun Oct 3 05:48:30 2010 Warning: A generic non-fatal error has occurred
found in file RivOQL.y at line 2552 - Deprecated type 'long' in OQL
statement will be evaluated as type 'time'
```

After importing your previous system data, you might need to perform manual settings on the new system. The export-import process provides guidance on what files require attention and manual editing to fully complete the upgrading and migrating process.

Related tasks:

"Loading updated MIB information" on page 244
To ensure that the MIB browser reflects the most up-to-date MIB information, load updated MIB information by running the **ncp_mib** command-line application.

Importing customization data - manual steps

Due to changes in the product and potential user customizations, you must migrate some core configuration settings manually to the new system. Review the following tasks to determine what additional manual adjustments you need to make to your new system.

Make sure you have performed a data collection and export on your previous system and have imported the data to your new installation.

To perform manual migration steps:

1. Log in to your new installation.
2. Review the `NCHOME/log/precision/ITNMCompareSystemsFinal.txt` file for information on what manual changes might be required. This log lists the changes between the previous and new system, including:
   - Files that have changed only due to modifications within the product from one release to the next. Such files are marked with the phrases `Different` and `System`, for example, `Different,,System,precision/aoc/CiscoNonRoutingSwitch.aoc`.

     Note: These files do not require your attention, the log lists them for informational purposes only.
   - Files that have changed only due to customizations users have made on the previous installation. Such files are marked with the phrases `Different` and `User`, for example, `Different,User,,etc/precision/DbLogins.NCOMS.cfg`.

     Note: These files do not require your attention, the log lists them for informational purposes only.
   - Files that have changed due to both modifications in the product across releases and customizations users have made on the previous installation. Such files are marked with the phrases `Different` and `User,System`, for

example, `Different,User,System,etc/precision/CtrlServices.cfg`. These are the files that require attention as any user customizations need to be reviewed and applied again manually.

- Files that did not exist on the previous system, but exist on the new installation are marked with the phrase `Inserted`, for example, `Inserted ,,,etc/precision/DiscoDNSHelperSchema.NCOMS.cfg`.
- Files that existed on the old system, but are no longer required and are obsolete are marked with the phrase `Removed`, for example, `Removed ,,,etc/precision/AmosSchema.cfg`
- Files that have not changed are marked with the phrase `Same`, for example, `Same,,,etc/precision/ClassSchema.cfg`.

Note: There are three `CompareSystems` files:

- `ITNMCompareSystemsTgt.log`
- `ITNMCompareSystemsFinal.log`
- `ITNMCompareSystemsFinal.txt`

The first two are work files and you can ignore them. The one that requires attention is only the third one, `ITNMCompareSystemsFinal.txt`, as described above.

Tip: For a detailed report on the export-import migration process, see `NCHOME/log/precision/ITNMDataImport.log`. This file is for debugging and support purposes.

3. All files from the previous installation that might require manual adjustments are archived to `NCHOME/etc/precision/migration`. Based on information in the `ITNMCompareSystemsFinal.txt` file, inspect and adjust settings in the following archived files as necessary:
   - Any device class `*.aoc` file.
   - Any agent `*.agnt` file.
   - Any stitcher `*.stch` file.
   - Any MIB `*.mib` file.
   - `SnmpStackSecurityInfo.`*`DOMAIN`*`.cfg`
   - `TelnetStackPasswords.`*`DOMAIN`*`.cfg`
   - `ModelNcimDb.`*`DOMAIN`*`.cfg`
   - `CtrlServices.`*`DOMAIN`*`.cfg`

     Note:
     - If you have migrated `CtrlServices.`*`DOMAIN`*`.cfg` files that were used to configure failover, there might be a conflict between the `-primaryDomain`, `-backupDomain`, `-virtualDomain`, `-backup`, and `-server` command-line options in the `CtrlServices.`*`DOMAIN`*`.cfg` file, and the settings in the `ConfigItnm.`*`DOMAIN`*`.cfg` file. The command-line options in the `CtrlServices.`*`DOMAIN`*`.cfg` file take precedence, by default, and a warning will be logged. You can disable usage of a migrated `CtrlServices.`*`DOMAIN`*`.cfg` file by renaming it (for example, to `CtrlServices.OLD.cfg`), which causes the system to default to using the `CtrlServices.cfg` file.
     - If your migrated `CtrlServices.`*`DOMAIN`*`.cfg` file contains other customized settings for the defined processes (for example, `-latency` and `-debug`), you will need to reconfigure these settings in the default `CtrlServices.cfg` file.
   - `NcoGateInserts.`*`DOMAIN`*`.cfg`

- NcoGateSchema.*DOMAIN*.cfg
- VirtualDomainSchema.*DOMAIN*.cfg
- DbEntityDetails.cfg

  Note: You must also recreate any new NCIM tables.
- DiscoCollectorFinderSeeds.*DOMAIN*.cfg
- DiscoFileFinderParseRules.*DOMAIN*.cfg
- DiscoPingFinderSeeds.*DOMAIN*.cfg
- DiscoScope.*DOMAIN*.cfg

  Note: The DiscoSchema.*DOMAIN*.cfg has been split into two files in Network Manager V3.9. The insert statements in this file have been moved to the new DiscoConfig*DOMAIN*.cfg file. This provides a way of separating any user customizations from the fixed schema definitions.

Depending on your previous system setup, you might need to perform further manual tasks like adjusting multiple domain settings, copying DLA properties, manually applying poll and report settings, or reviewing event management settings and understanding the changes in the way event enrichment and correlation works in Network Manager V3.9.

Note: After you have finished importing configuration data and reconciling customizations manually, make sure you start your domains before using Network Manager. The default domain specified at installation is started when starting Network Manager, but if you have multiple domains, then start each using the **itnm_start** ncp -domain *DOMAIN* command.

Migrating DLA properties

If you use the Discovery Library Adapter (DLA) to collect data on network resources and have DLA properties files that you set up on your previous system, the settings need to be migrated manually.

To migrate DLA settings:

1. Log in to your new installation.
2. Go to NCHOME/var/precision/export and locate the DLA properties files the export-import process archived on your previous system and copied over. Each domain has an ncp_dla.properties.*domain name* file archived by the export-import process.
3. Use the archived DLA properties files for each domain to recreate the same DLA settings on your new installation:
   a. Go to NCHOME/precision/adapters/ncp_dla.
   b. Using the preconfigured ncp_dla.properties file, create an equivalent DLA properties file based on each previous domain's DLA file, naming the files after each domain, for example, ncp_dla.properties.NCOMS.
   c. Open the archived DLA properties file for each domain and make the same settings in the new respective domain-specific file as in the previous archived ncp_dla.properties.*domain name* file, thus recreating the DLA file for each respective domain on the new system.

      CAUTION:
      Do not copy-paste the previous file content as is into the new file, but copy over settings that have been modified on the previous system. The new file contains new parameters that did not exist in previous versions, and might not function properly if the content is overwritten.

4. Save and close each DLA properties file.

Related tasks:

"Configuring the DLA" on page 182
The Discovery Library Adapter (DLA) requires a configuration properties file in order to determine the data source to connect to, the domain to query, the target directory for Discovery Library books and logging parameters.

Migrating event handling customizations

Event enrichment and correlation has changed substantially in Network Manager V3.9. If you made customizations to event management, you need to understand how event enrichment and correlation changed and re-implement your customizations in the new installation.

To understand the changes and re-implement them:

1. Log in to your new installation.
2. Review the changes you made to the `NcoGateSchema.DOMAIN.cfg` and `NcoGateInserts.DOMAIN.cfg` files and make changes as necessary:
   a. Go to `NCHOME/etc/precision/migration`.
   b. Locate the `NcoGateSchema.DOMAIN.cfg` and `NcoGateInserts.DOMAIN.cfg` files for each domain you have made customizations.
   c. Understand the event tables to determine how to reapply any customizations to the config.precedence, config.eventMap, config.ncp2nco, and config.nco2ncp tables. For more information, see the *IBM Tivoli Network Manager IP Edition Management Database Reference*

   Note: The probe rules populate the NmosEventMap field of alerts.status for all Network Manager events raised by the poller. The config.precedence table entries are not required unless you wish to override the event map or change the default precedence value.
3. If you made customizations to the config.ncp2nco or config.nco2ncp tables, then read about the stitchers in the `NCHOME/precision/eventGateway/stitchers` directory and understand how they work in the current release in order to re-implement event enrichment customizations. For more information on stitchers, see the *IBM Tivoli Network Manager IP Edition Event Management Guide*

Migrating poll settings

To use your previous polling customizations in version 3.9, you must define the scope for each poll policy manually after finishing the import.

Custom poll policies and poll definitions are moved to your new system by the export-import process. The scope is imported to a network view, which needs to be set manually for each policy. This is due to the changes in the way the scope (the network entities a policy is set to poll) is defined:

- In V3.7, the scope is defined by device class and device filter set in the poll policy.
- In V3.8, the scope is defined by device class, device filter, and interface filter set in the poll policy.
- In V3.9, the scope is defined by the network view it applies to and can be further refined by setting class and interface filters at the poll definition level. Poll policies can also have device filters set, but they are restricted to the mainNodeDetails table, and are aimed at providing device filtering to support the MIB Grapher and poll policies created through network views for right-click menus.

In V3.9, the primary method of setting a scope is by using a network view. You can assign one or more network views to a poll policy to define the device scope to be polled. To understand poll policies in V3.9, create new policies and set their scope using network views.

Note: A poll policy can be associated with multiple poll definitions in V3.9, while in V3.8 you can only have one definition per policy. This can be useful, for example, when you want to poll information that is specific to the device vendor. In such cases you need to set up a poll definition for each vendor (as each vendor might have different MIBs), but have only one policy with all poll definitions added to get the data from across your network.

The export-import process creates network views based on your previous poll policy scopes and names the network views after the poll policy. You have to edit each poll policy and select the appropriate network view for each after importing data to your new system. You can also select a device filter in the poll policy, or create an even more granular scope using the device class and interface filter settings of poll definitions.

To migrate poll settings, complete the following steps.

1. Log in to your V3.9 installation.
2. Make sure the network views exist for your system: click **Availability** > **Network Availability** > **Network Views**.
3. Click **Administration** > **Network** > **Network Polling**.
4. Select a policy that was available on your previous system by clicking the name of the poll policy. The Poll Policy Editor is displayed for the policy you selected and its settings are automatically loaded into the fields.
5. Go to the **Network Views** tab and select the network view with the same name as the policy. This sets the scope of the policy to the devices in the network view that is based on your previous system's settings.

   Note: The poll policies from your previous system that were set up for all devices will not have a network view. In such cases, make sure **All Devices** is selected in the **Network Views** tab.
6. Optional: You can further refine the scope of the policy by creating a more restricted filter in the **Device Filter** tab. Also, the poll definitions attached to the policy can contain more granular filtering based on device class and interface filters.

   Tip: If a class or interface filter was set up in your previous system for a poll policy, those settings are defined in the poll definitions in V3.9. The export-import process takes care of moving the device class settings over to the new installation by creating the device class filter setting from V3.8 at the poll definition level in V3.9.
7. Click **Save**.
8. Repeat the steps for each poll policy from your previous system.

Migrating 3.7 reports

If you have modified or created reports in Network Manager 3.7, you must migrate those reports manually.

Before performing this task, you must first export the 3.7 customization data, which includes the reports, using the **nmExport** script. This script places the reports in a compressed file of your choice.

To migrate customized 3.7 reports, complete the following steps:

1. Import the 3.7 reports to the BIRT Designer.
   a. Copy the compressed file that contains the 3.7 reports (which you created using the **nmExport** script) to the server where the BIRT Designer is installed. You can download the BIRT Report Designer at http://www.ibm.com/developerworks/spaces/tcr.
   b. Start the BIRT Report Designer by running **eclipse.exe**. You are prompted for a workspace folder to hold your projects.
   c. Create a project by clicking **File** > **New** > **Project** > **Business Intelligence and Reporting Tools** > **Report Project**.
   d. Name the project. for example, ANZ Reports.
   e. From the Navigator window, right click the project you just created and select **Import** > **Select Archive File**.
   f. Choose the compressed file that contains the reports and click **Finish**.
2. Edit any reports that you want to migrate to 3.9.
   a. In the **Navigator** tree, rename the **ITNM** folder under the project you created in step 1 to `resources`.
   b. Set the report library for the report.
      1) Click **Window** > **Preferences**.
      2) In the tree on the left side, click **Report Design** > **Resource**.
      3) Browse to the directory with the `.rptlibrary` file, for example C:/username/workspace/ANZ Reports/resources/itnm/lib/ and click OK.
   c. In the **Outline** tab, double click each of the data sources under **itnm_data_source.rptlibrary** > **Data Sources** and change the data sources to point to the machine or database you want to use to test your reports within BIRT Designer.
   d. Fix the errors in the reports shown by BIRT designer.
3. To import the reports to Tivoli Common Reporting, run a command similar to the following:

   ```
   NCHOME/../tipv2Components/TCRComponent/bin/trcmd.sh -import -design
   report_filename -reportSetBase destination_report_set -resourceDir
   ITNM39 -username admin_username -password admin_password
   ```

   Where

   - *report_filename* is the filename of the report to move.
   - *destination_report_set* is the 3.9 report set where you want the report to be moved to. Possible values are:
     - "/content/package[@name='Network Manager']/folder[@name='Asset Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Current Status Reports']"

- "/content/package[@name='Network Manager']/folder[@name='Network Technology Reports']"
- "/content/package[@name='Network Manager']/folder[@name='Network Views Reports']"
- "/content/package[@name='Network Manager']/folder[@name='Path View Reports']"
- "/content/package[@name='Network Manager']/folder[@name='Performance Reports']"
- "/content/package[@name='Network Manager']/folder[@name='Network Technology Reports']"
- "/content/package[@name='Network Manager']/folder[@name='Summary Reports']"
- "/content/package[@name='Network Manager']/folder[@name='Troubleshooting Reports']"
- "/content/package[@name='Network Manager']/folder[@name='Utility Reports']"

• *admin_username* is the username of a Tivoli Integrated Portal administrator.
• *admin_password* is the password for the administrative user.

The following command moves a 3.7 report called itnm_usa_vlan_summary to the Network Technology Reports report set:

```
NCHOME/../tipv2Components/TCRComponent/bin/trcmd.sh -import -design
itnm_usa_vlan_summary.rptdesign -reportSetBase "/content/
package[@name='Network Manager']/folder[@name='Network Technology
Reports']" -resourceDir ITNM39 -username tipadmin -password netcool
```

4. Review the reports that you have moved into a 3.9 report set. If a report uses the ncmonitor or ncpolldata database, check the SQL commands against similar commands in the default 3.9 reports. The database schemas might have changed.

   Important: Any parameters that were saved with reports are not preserved.

Importing V3.8 GUI data

After installing Network Manager V3.9, you can import your previous V3.8 GUI data.

Before you can import GUI data, you must export the data from your previous 3.8 installation and install version 3.9.

To import GUI data, perform the following tasks:

1. Log in to the server where the GUI components of your previous V3.8 system are installed.
2. Copy the `TIPHOME/profiles/TIPProfile/upgrade/data/upgradeData.zip` export file to the server where you installed Network Manager V3.9 GUI components.
3. On your new installation, go to where you placed your installation package.

   Note: The Tivoli Integrated Portal server must be running during the GUI data import.
4. Run the GUI data import script using one of the following methods:
   • To run the script from the installer launchpad, start the launchpad by running the UNIX **launchpad.sh** script on UNIX or the Windows **launchpad.exe** executable on Windows, select the **Postinstallation**

menu item, expand the **Upgrading from an existing Network Manager** section, and click **Import Network Manager GUI Data**.

- To run the script from the command line, change to the `scripts` subdirectory and depending on your operating system, run the UNIX **nmGuiImport** or the Windows **nmGuiImport.bat** command as follows:

  ```
  nmGuiImport | bat -u TIP administrator user name -p password for TIP
  administrator -f path to GUI data export .zip file -d location of the
  TIP installation
  ```

  Note: If no values are provided, you are prompted to enter values. If the location of the Tivoli Integrated Portal installation is not provided, the environment variable `TIPHOME` is used. If `TIPHOME` does not exist, you are prompted to enter a location.

Note: You must run the script as the same user that installed the product.

The exported GUI data is imported into the new installation.

The GUI data import process creates its own log files in the following directories:

- `TIPHOME/profiles/TIPProfile/logs/upgrade.log`
- `TIPHOME/profiles/TIPProfile/logs/tipcli.log`
- `NCHOME/log/install/itnm_gui_migration.log`

Note: The `itnm_gui_migration.log` is a migration report file, and provides information about files that are imported, backed up, and require manual reconciliation steps on the new system.

After importing your previous GUI data, you might need to perform manual settings on the new system. The export-import process provides guidance on what files require attention and manual editing to fully complete the upgrading and migrating process.

Importing V3.8 GUI data - manual steps

Due to changes in the product, you must migrate some GUI configuration settings manually to the new system. Review the following tasks to determine what additional manual adjustments you need to make to your new system.

Make sure you have performed the GUI data collection and export on your previous system and have imported the GUI data to your new installation.

To ensure all GUI settings are migrated:

1. Log in to your new installation.
2. You must manually reconcile the Tivoli Integrated Portal files listed in `ITNMHOME/profiles/TIPProfile/etc/tnm/migration` and `ITNMHOME/profiles/TIPProfile/etc/tnm/*/migration`. The archived files are saved by the export-import process.
3. Use the `NCHOME/log/install/itnm_gui_migration.log` migration report file to check what files require manual editing to be suitable for use on the new system.
4. Any customized WebTool under `NCHOME/precision/scripts/webtools` are not migrated. You must manually save them on your previous installation, and reimplement them on the new system. An example of such customization is the settings to launch into TADDM.

5. To preserve any new or customized reports from your previous installation, you must perform extra configuration steps.

Related tasks:

"Configuring Network Manager to start IBM Tivoli Application Dependency Discovery Manager" on page 194
Optional: To enable Network Operators to launch the IBM Tivoli Application Dependency Discovery Manager GUI from Network Manager, you must add the TADDM menu options to Network Manager.

Migrating 3.8 reports

If you have modified or created reports in Network Manager 3.8, you must migrate those reports manually.

Before performing this task, you must first import the 3.8 GUI data, which includes the reports.

The 3.8 GUI data import script, **nmGuiImport**, puts all customized 3.8 reports into the **Tivoli Products** > **ITNM Reports** report set. To migrate customized 3.8 reports, complete the following steps:

1. Log in to Network Manager 3.9 and click **Reporting** > **Common Reporting** > **Tivoli Products** > **ITNM Reports**.
   - If this report set does not contain any new or customized reports, you do not need to do this task. You can delete the **Tivoli Products** > **ITNM Reports** report set.
   - If the report set does contain new or customized reports, choose which reports you want to migrate to 3.9.
2. On the server where Tivoli Common Reporting is installed, navigate to the directory where the imported 3.8 custom report designs are located: `NCHOME/../tipv2Components/TCRComponent/data/design`.
3. To move a report from the 3.8 group to a 3.9 report group, run a command similar to the following:

   ```
   NCHOME/../tipv2Components/TCRComponent/bin/trcmd.sh -import -design
   report_filename -reportSetBase destination_report_set -resourceDir
   ITNM39 -username admin_username -password admin_password
   ```

   Where
   - *report_filename* is the filename of the report to move.
   - *destination_report_set* is the 3.9 report set where you want the report to be moved to. Possible values are:
     - "/content/package[@name='Network Manager']/folder[@name='Asset Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Current Status Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Network Technology Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Network Views Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Path View Reports']"
     - "/content/package[@name='Network Manager']/ folder[@name='Performance Reports']"
     - "/content/package[@name='Network Manager']/folder[@name='Network Technology Reports']"

- "/content/package[@name='Network Manager']/folder[@name='Summary Reports']"
- "/content/package[@name='Network Manager']/folder[@name='Troubleshooting Reports']"
- "/content/package[@name='Network Manager']/folder[@name='Utility Reports']"

- *admin_username* is the username of a Tivoli Integrated Portal administrator.
- *admin_password* is the password for the administrative user.

The following command moves a 3.8 report called itnm_usa_vlan_summary to the Network Technology Reports report set:

```
NCHOME/../tipv2Components/TCRComponent/bin/trcmd.sh -import -design
itnm_usa_vlan_summary.rptdesign -reportSetBase "/content/
package[@name='Network Manager']/folder[@name='Network Technology
Reports']" -resourceDir ITNM39 -username tipadmin -password netcool
```

4. Review the reports that you have moved into a 3.9 report set. If a report uses the ncmonitor or ncpolldata database, check the SQL commands against similar commands in the default 3.9 reports. The database schemas might have changed.

   Important: Any parameters that were saved with reports are not preserved.

Related tasks:

"Configuring data sources for BIRT" on page 248
If you use reports based on the BIRT data model, you must configure data sources. If you also use reports based on the Cognos data model, you must configure Cognos data sources separately.

Identifying NCIM topology database customizations

The upgrade scripts do not migrate customizations made to the NCIM topology database schema. However, Network Manager provides a tool to identify customizations you made on your previous database, so that you can recreate them in the new installation's database. To migrate NCIM customizations, you must first use the **ncp_ncim_diff.pl** script to identify the differences between your previous installation's NCIM topology database schema and the new installation's NCIM schema, and then manually update the new NCIM topology database schema with these modifications.

You must install the new database and run the Network Manager create database schema scripts to set up the tables and schemas.

Before you run the **ncp_ncim_diff.pl** script, make sure that the `DbLogins.DOMAIN.cfg` files from the previous installation have been migrated to your new installation. The export-import process for the customization data provides this. The `DbLogins.DOMAIN.cfg` file contains the options for connecting to your NCIM database.

Note: The migration process combined with a new discovery of the network populates the database. You only need to run **ncp_ncim_diff.pl** script if you have customized changes in your previous database.

To compare the topology database schemas:

1. Log in to your new Network Manager installation.
2. Change to the following directory:

- UNIX: UNIX: $NCHOME/precision/scripts/perl/scripts
- Windows: Windows: %NCHOME%\precision\scripts\perl\scripts

3. Enter the following command: ./ncp_ncim_diff.pl -domain *DOMAIN* -password *NCIM_database_password*

   Where *DOMAIN* is the name of your previous Network Manager installation's domain whose NCIM structure you want to compare to the new installation's schema. You need to use the DbLogins.*DOMAIN*.cfg file from your previous installation so that the script connects to the previous database and compares the schema there with the schema on the new installation. The following is an example of the output of the command for a domain named NCOMS.

```
67  NCIM tables and views found in Domain NCOMS
66  NCIM tables and views found in  Default NCIM structure for ITNM v3.9


***********************************************************
 Additional elements in Domain NCOMS

        Table CUSTOM

***********************************************************

1 differences found between  Domain NCOMS and  Default NCIM structure
for ITNM v3.9
```

4. Optional: You can specify a file name to where the output is saved with the optional -dumpToFile *file name*.xml parameter.

Related tasks:

"Setting up a topology database" on page 56
Apart from the default Informix database, you can use a DB2, MySQL, or Oracle database to store your topology. Unless you are installing the default Informix database bundled with Network Manager, you must configure an existing database or install and configure a new one before installing Network Manager.

Copying an existing V3.9 installation

You can copy the customizations and data of an existing V3.9 installation to another V3.9 installation.

If you want to clone or migrate an installation of Network Manager to Network Manager V3.9 Fixpack 5, you must first update the following import and export scripts: $NCHOME/precision/install/scripts/nmExport, $NCHOME/precision/install/scripts/nmImport, and $NCHOME/scripts/upgrade/ITNMExportNetworkViews.pl. After you install Network Manager Fixpack 5, copy the nmExport and nmImport scripts to the scripts directory in the location where you uncompressed the installation file for the major version of Network Manager. Alternatively, if you are using ExportPackage.tar, copy the scripts to the scripts directory where you uncompressed the .tar file. You cannot run these scripts from an existing installation or from a Fixpack installation. Also copy the ITNMExportNetworkViews.pl script to the migration/bin/ directory of the same location.

Using the export-import scripts provided with Network Manager you can make a copy of a V3.9 installation and use it recreate the same setup on a another system, restore settings later, or move from test system to a production environment.

To copy an existing V3.9 installation, complete the following steps:

1. Access the source system where you have the Network Manager installation you want to make a copy of. If you have a distributed setup, you need to access each system to collect all data.
2. Go to where you extracted the installation package.
3. Run the data export script using one of the following methods:
   - To run the script from the installer launchpad, start the launchpad by running the UNIX **launchpad.sh** script on UNIX or the Windows **launchpad.exe** executable on Windows, select the **Preinstallation and Migration** menu item, expand the **Upgrading from an existing Network Manager** section, and click **Export Network Manager Data**.
   - To run the script from the command line, run the UNIX **nmExport** script on UNIX or the Windows **nmExport.bat** script on Windows from the `scripts` subdirectory.

   Note: You must run the script as the same user that installed the product.

   Provide the answers to the prompts. The export script extracts data and saves it to an export file in a location of your choice (`.pkg` on UNIX systems or `.zip` on Windows systems).

   Restriction: Historical polling data is not moved over when copying between V3.9 releases.
4. Run the GUI data export script using one of the following methods:
   - To run the script from the installer launchpad, start the launchpad by running the UNIX **launchpad.sh** script on UNIX or the Windows **launchpad.exe** executable on Windows, select the **Preinstallation and Migration** menu item, expand the **Upgrading from an existing Network Manager** section, and click **Export Network Manager GUI Data**.
   - To run the script from the command line, change to the `scripts` subdirectory and depending on your operating system, run the UNIX **nmGuiExport** or the Windows **nmGuiExport.bat** command as follows:

     nmGuiExport | bat -u *TIP administrator user name* -p *password for TIP administrator* -d *location of the TIP installation to be migrated*

     Note: If no values are provided, you are prompted to enter values. If the location of the Tivoli Integrated Portal installation to be migrated is not provided, the environment variable `TIPHOME` is used. If `TIPHOME` does not exist, you are prompted to enter a location.

   Note: You must run the script as the same user that installed the product.

   GUI data is extracted and saved into the `TIPHOME/profiles/TIPProfile/upgrade/data/upgradeData.zip` export file.
5. Log in to the Network Manager installation where you want to copy the setup.
6. On your new installation, make sure that the Network Manager core components for each domain are running. To do this, use the Windows Services GUI on Windows systems, or use the following command on UNIX systems: **itnm_start** `ncp -domain` *DOMAIN*. For example, to start the `NCOMS` domain, type: `itnm_start ncp -domain NCOMS` . This ensures that Network

Manager is fully initialized and the domain tables are populated. You must stop the core components again to do the import itself, as described in the next step.

7. Stop the Network Manager core components for each domain on your new installation using the Windows Services GUI on Windows systems, or using the following command on UNIX systems: **itnm_stop** ncp -domain *DOMAIN*. For example, to stop the NCOMS domain, type: itnm_stop ncp -domain NCOMS

   Note: If you do not specify a domain name with **itnm_stop**, it stops the default domain created at installation.

8. Run the data import script using one of the following methods:
   - To run the script from the installer launchpad, start the launchpad by running the UNIX **launchpad.sh** script on UNIX or the Windows **launchpad.exe** executable on Windows, select the **Postinstallation** menu item, expand the **Upgrading from an existing Network Manager** section, and click **Import Network Manager Data**.
   - To run the script from the command line, run the UNIX **nmImport** script on UNIX or the Windows **nmImport.bat** script on Windows from the scripts subdirectory of the installation media.

   Note: You must run the script as the same user that installed the product.

9. When prompted, provide the path to the .pkg or .zip file that contains the customization data that you previously exported.
10. Answer the various other questions the import process asks to copy the data over.

    Note: The following question requires special attention:

    ```
    Allocate new entityIds during import [ N ]
    ```

    Each device in the system has an entityId. The import process can preserve the entityIds or allocate new entityIds. If you answer no, then each device maintains the entityId from the previous installation. This is necessary when you have links to external systems that use Network Manager data, for example, Tivoli Data Warehouse.

    If you answer yes, devices are allocated new entityIds.

    To preserve entityIds, the target system needs to be empty. If the target system is not empty (for example, due to a previous data import or discovery), preserving entityIds might become a complex operation due to potential clashes between existing entityIds and the ones being imported, and the results may be unpredictable. Therefore, merging of domain data is not supported.

    Attention: If you have a domain on the target system that has the same name as on your previous system, then make sure the domain on the target system does not contain data. Domain names cannot be changed during the migration process.

    The import process creates its own log files. Logs from the import process are saved to NCHOME/log/precision:

    - ITNMDataImport.log
    - get_policies.*domain name*.log
    - ITNMImportNetworkViews.log

The export-import process automatically detects and recreates the domains from a previous install. The import script detects the potential domains from the previous system based on the data files. Using the **domain_create.pl** script, the process automatically creates domains on the new installation using the domain names from the previous system. After the domains have been created, the main topology and policy data are imported for each.

The **domain_create.pl** script creates the discovery configuration files for the new domains in NCHOME/etc/precision using the values in the configuration files of the default domain. The import process saves the imported files in the NCHOME/etc/precision/migration directory as read-only files. You can use the imported files to manually update the newly created files in NCHOME/etc/precision. When copying from an existing V3.9 installation, the files can be copied directly into NCHOME/etc/precision, but they need to be given write permissions to be able to be edited from the Discovery Configuration GUI.

11. Check whether there are any files in the NCHOME/etc/precision/migration directory. Any user changes made in the files listed here might need to be reviewed and applied again manually.
12. Run the GUI data import script using one of the following methods:
    - To run the script from the installer launchpad, start the launchpad by running the UNIX **launchpad.sh** script on UNIX or the Windows **launchpad.exe** executable on Windows, select the **Postinstallation** menu item, expand the **Upgrading from an existing Network Manager** section, and click **Import Network Manager GUI Data**.
    - To run the script from the command line, change to the scripts subdirectory and depending on your operating system, run the UNIX **nmGuiImport** or the Windows **nmGuiImport.bat** command as follows:

      ```
      nmGuiImport | bat -u TIP administrator user name -p password for TIP
      administrator -f path to GUI data export .zip file -d location of the
      TIP installation
      ```

      Note: If no values are provided, you are prompted to enter values. If the location of the Tivoli Integrated Portal installation is not provided, the environment variable TIPHOME is used. If TIPHOME does not exist, you are prompted to enter a location.

    Note: You must run the script as the same user that installed the product. The Tivoli Integrated Portal server must be running during the GUI data import.
13. You must manually reconcile the Tivoli Integrated Portal files listed in ITNMHOME/profiles/TIPProfile/etc/tnm/migration and ITNMHOME/profiles/TIPProfile/etc/tnm/*/migration. The archived files are saved by the export-import process.
14. Use the NCHOME/log/install/itnm_gui_migration.log migration report file to check what files require manual editing to be suitable for use on the new system.
15. If you have made any customizations to the NCIM topology database schema on the system you are copying from, follow the steps in "Identifying NCIM topology database customizations" on page 146.
16. If you have changed the database configuration used for Tivoli Common Reporting, or defined a new database for the target system where the target

system is different from the source system, configure the data sources for reporting using the instructions in the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Note: As both the ncmonitor and polling schema are the same when copying between the same release, the reports do not require manual modification for schema changes.

17. Stop and start Network Manager, including the Tivoli Integrated Portal, as described in Starting and stopping Network Manager. The default domain is started by the start process, but if you have multiple domains then start each using the **itnm_start** ncp -domain *DOMAIN* command.

Transitioning from IBM Tivoli NetView

Because Network Manager has capabilities that are not available in IBM Tivoli NetView, no automated migration path is supported between the two products. Instead, transition to Network Manager by installing the product and configuring it to discover and visualize the network. To help you plan the transition, Network Manager includes scripts that you can use to extract useful data from IBM Tivoli NetView.

You can transition to Network Manager from IBM Tivoli NetView V7.1.4 and V7.1.5.

The high-level procedure for transitioning from IBM Tivoli NetView is as follows:

1. Extract the data from IBM Tivoli NetView. You can run a script from the command-line interface or select an option from the launchpad.
2. Install Network Manager V3.9. In the installer program, ignore the **Seed Discovery from IBM Tivoli NetView Installation** option. You can achieve better results by planning the configuration of Network Managerwith the help of the data that you extracted in step 1.
3. Plan and then run the discovery. Use the extracted data to help you.
4. After the discovery finishes, re-create the IBM Tivoli NetView locations in network views.
5. Uninstall IBM Tivoli NetView. For more information, search for *Uninstalling the Tivoli NetView program* at http://www-01.ibm.com/support/knowledgecenter/SS3HLM_7.1.1.16/com.ibm.tivoli.tpm.osd.doc_7.1.1.16/welcome/osdlanding.html.

Related tasks:

Chapter 1, “Planning for installation,” on page 1
Read about deployment considerations and system requirements for Network Manager.

Extracting data from IBM Tivoli NetView

To help you plan the transition to Network Manager, you can extract useful network data from IBM Tivoli NetView. You can use the output of the script to configure the network discovery by Network Manager.

The following data can be extracted:

- Host names and IP addresses of all discovered nodes
- Nodes and their associated SNMP community strings
- Community names
- Unmanaged nodes
- Device groupings (location containers)

Before you extract the data:

- Ensure that Perl is installed on the host.
- For the launchpad, ensure that a supported browser is installed.

A script to extract the data is included in the Network Manager installation package. Alternatively, an option to run the script is available on the launchpad.

- To extract the data by running the script:
  1. Decompress the Network Manager installation package and change to the `scripts` directory.
  2. Copy the `ExportPackage` package to any working directory on your IBM Tivoli NetView installation and decompress the package.
  3. Run the **`exportNVData`** script.
- To extract the data by using the launchpad, select **Pre-Installation & Migration** from the menu. Then, expand **Collect IBM Tivoli NetView Data for Seeding Discovery** and click **Extract NetView Migration Data**.

The IBM Tivoli NetView data is extracted and saved to a `nvMigrationData` package.

Decompress the `nvMigrationData` package and use the data to help you plan the discovery.

Related reference:

"Supported browsers for the installer launchpad" on page 43
To run the installer launchpad, ensure that a supported browser is installed. The supported browsers for the installer launchpad are not necessarily the same as the supported browsers for the web applications.

Creating network views from the IBM Tivoli NetView `location.conf` file

The `location.conf` configuration file is used to create topology maps for locations that are based on defined IP address ranges. Network Manager can use a subset of the syntax of the `location.conf` file and the IP address ranges that are defined in the file to replicate the topology maps in network views.

For more information about the subset of the `location.conf` syntax that is supported by Network Manager, see Creating IP filtered views.

You can run an auto-provisioning script that converts the `location.conf` file to a dynamic network view node. The node that has a set of network views that

correspond to the content of the location.conf file. A domain can be specified. The network views can be assigned to users or groups.

1. Copy the location.conf file to ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision.
2. Change to ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision/examples and copy the example_netview_migration.xml file to ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision.
3. In ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision, open your copy of the example_netview_migration.xml file. At a minimum, edit the following parameters.

   accessID
   Specify the user or group that you want to access the network views.

   domain
   Specify the domain to which you want to add the network views.

   netViewMigration file
   Specify the location of the location.conf file. If the file is not in ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision, specify the relative path to the file.

   See "Example" for a sample file.
4. Run the script.

Every 60 seconds, the ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision directory is monitored for new autoprovision scripts. When a new script is detected, it is read and processed and the dynamic view is created.

Example

The following sample generates a view that is called MigratedLocation.conf. Based on the data in the ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision/location.conf file, a set of network views are created underneath MigratedLocation.conf. The generated view is assigned to the itnmadmin user. The views are created in the NCOMS domain.

```
<autoProvision name="MigratedLocation.conf" domain="NCOMS" accessLevel="user"
accessId="itnmadmin">
        <netViewMigration file="location.conf" endNodes="true" connectivity=
"ipsubnets"/>
</autoProvision>
```

Chapter 4. Configuring Network Manager

After installing Network Manager, you must configure Network Manager for your environment and your requirements. If your environment or your requirements change at a later time, or if you want to integrate Network Manager with other products, you might need to perform additional configuration tasks.

Click the following link to retrieve technotes about known configuration issues in version 3.9 of Network Manager:
http://www-01.ibm.com/support/search.wss?word=ow
&wfield=configure+configuration+configuring&rs=3118&tc=SSSHRK
&atrn=SWVersion&atrv=3.9&ibm-go.x=18&ibm-go.y=12

Configuring integrations with other products

You can set up Network Manager to work with a number of Tivoli® products. Read about necessary configuration tasks required to set up the available integrations.

Related reference:

"Requirements for other products" on page 30
Make sure that you meet the requirements for the products that are integrated with Network Manager.

Configuring Tivoli Netcool/OMNIbus for use with Network Manager

If you have installed Tivoli Netcool/OMNIbus not using the Network Manager installation, then you must perform a number of configuration tasks.

Tivoli Netcool/OMNIbus handles events provided by Network Manager and other event sources, and can also be used as an authentication source. See **Related information** below for links to relevant topics.

To use Tivoli Netcool/OMNIbus, you must modify a table in the ObjectServer. If you are running Network Manager in a FIPS 140–2 installation, you must make additional configuration to the Tivoli Netcool/OMNIbus JRE.

For detailed information about Tivoli Netcool/OMNIbus, including post-installation configuration and FIPS 140–2 considerations, see the Tivoli Netcool/OMNIbus information centre at http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

For more information about Tivoli Netcool/OMNIbus, including post-installation configuration and FIPS 140–2 considerations, see the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* and the *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Related tasks:

- Changing user registries after installation
- Adding ObjectServers as user registries
- Using SSL for communication with ObjectServer

"Configuring VMM for the ObjectServer" on page 208
When your Tivoli Netcool/OMNIbus ObjectServer is in a federated repository, use the script provided with Tivoli Integrated Portal to configure the Virtual Member Manager adapter for the ObjectServer.

"Configuring data source failover for the Tivoli Netcool/OMNIbus Web GUI" on page 304
If you have a failover pair of ObjectServers to which the Web GUI should connect, you can configure data source failover by using the `ncwDataSourceDefinitions.xml` data source configuration file in your Web GUI installation.

Changing the password for the connection to the ObjectServer

Configuring automations for service-affected events

Fix Pack 4

Configure automations in Tivoli Netcool/OMNIbus to support the generation of service-affected events (SAEs). The steps in this task differ, depending on the complexity of the Tivoli Netcool/OMNIbus installation. This task is required if you want to configure cross-domain discoveries in environments in which Tivoli Netcool/OMNIbus V7.3.1 or earlier is running.

For complex Tivoli Netcool/OMNIbus installations, including multitiered architectures, follow the guidelines in the *Tivoli Netcool/OMNIbus Best Practices Guide*, which is available at https://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli%20Netcool%20OMNIbus/page/Best%20Practices. Ensure that SAE triggers run only on the acting primary ObjectServer and that the SAE triggers are disabled on all other ObjectServers. The default triggers that are included in Network Manager are configured to run only on the primary aggregation ObjectServers.

Use the following steps to set up the automation and the SAE plug-in in the Event Gateway (**ncp_g_event**). The steps describe the configuration for a multitiered architecture. No configuration is required for collection layer ObjectServers. If your Tivoli Netcool/OMNIbus installation does not run on a multitiered architecture, only step 3 is required. For more information about how to stop and start Network Manager, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

1. Log in to the host where Tivoli Netcool/OMNIbus is installed.
2. Stop the **ncp** processes.
3. Configure the aggregation layer ObjectServers:
   a. Run the `NCHOME/precision/scripts/drop_sae_automation.sql` script to remove existing tables. For example, for the AGG_A ObjectServer and the user OMNIUser:
      ```
      $NCHOME/omnibus/bin/nco_sql -server AGG_A -user OMNIUser -password
       password < $NCHOME/precison/scripts/drop_sae_automation.sql
      ```
   b. Run the `NCHOME/precision/scripts/create_sae_automation.sql` script to install the SAE trigger and add the tables, including the `NmosDomainName` column. For example:
      ```
      $NCHOME/omnibus/bin/nco_sql -server AGG_A -user OMNIUser -password
       password < $NCHOME/precison/scripts/create_sae_automation.sql
      ```
   c. Ensure that the SAE automation runs only on the acting primary ObjectServer and not on the backup ObjectServer. Edit the `create_sae_automation.sql` file and verify or add the following line:
      ```
      WHEN get_prop_value('ActingPrimary') %= 'TRUE'
      ```

d. In the aggregation layer ObjectServers, enable the SAE triggers. Use the following command:

```
ALTER TRIGGER GROUP sae SET ENABLED TRUE;
```

e. Update the mapping for the aggregation layer ObjectServers. In the NCHOME/omnibus/etc/AGG_GATE.map file, add CREATE statements for the tables that were created by the create_sae_automation.sql script at the bottom of the file.

The CREATE statement might look like the following example. Copy the exact table definitions from the script to avoid errors.

```
CREATE MAPPING EntityServiceMap
(
 'NmosEntityId'  = '@NmosEntityId' ON INSERT ONLY,
 'ServiceEntityId' = '@ServiceEntityId' ON INSERT ONLY,
 'NmosDomainName' = '@NmosDomainName' ON INSERT ONLY
);

CREATE MAPPING ServiceDetailsMap
(
 'ServiceEntityId' = '@ServiceEntityId' ON INSERT ONLY,
 'Type'   = '@Type' ON INSERT ONLY,
 'Name'   = '@Name' ON INSERT ONLY,
 'Customer'  = '@Customer',
 'NmosDomainName' = '@NmosDomainName' ON INSERT ONLY
);
```

f. Update the Gateway for the aggregation ObjectServers. Edit the NCHOME/omnibus/etc/AGG_GATE.tblrep.def file and add the following REPLICATE statements for the tables that were created by the create_sae_automation.sql script at the bottom of the file.

```
REPLICATE ALL FROM TABLE 'precision.entity_service'
       USING MAP 'EntityServiceMap'
       INTO 'precision.entity_service';

REPLICATE ALL FROM TABLE 'precision.service_details'
       USING MAP 'ServiceDetailsMap'
       INTO 'precision.service_details';
```

4. Configure any display layer ObjectServers. See steps 3a on page 156 and 3b on page 156 for examples of how to run the drop_sae_automation.sql and create_sae_automation.sql scripts.

a. Run the NCHOME/precision/scripts/drop_sae_automation.sql script to remove existing tables.

b. Run the NCHOME/precision/scripts/create_sae_automation.sql script to install the SAE trigger and add the tables, including the NmosDomainName column.

c. In the display layer ObjectServers, disable the SAE triggers to prevent them running on the display layer. Use the following command:

```
ALTER TRIGGER GROUP sae SET ENABLED FALSE;
```

d. Ensure the precision.entity_service and precision.service_details tables in the display layer ObjectServers have the same schema as the tables in the aggregation layer ObjectServers.

e. Update the mapping for the display layer ObjectServers. Edit the NCHOME/omnibus/etc/A_TO_D_GATE.map files and add CREATE statements for the tables that were created by the create_sae_automation.sql script at the bottom of the file. This mapping must be identical to the mapping in the aggregation layer gateway. If you later change the mapping in the bidirectional gateway for the aggregation layer ObjectServers, you must replicate those changes here.

```
CREATE MAPPING EntityServiceMap
(
'NmosEntityId' = '@NmosEntityId' ON INSERT ONLY,
'ServiceEntityId' = '@ServiceEntityId ON INSERT ONLY,
'NmosDomainName' = '@NmosDomainName' ON INSERT ONLY
);
CREATE MAPPING ServiceDetailsMap
(
'ServiceEntityId' = '@ServiceEntityId' ON INSERT ONLY,
'Type' = '@Type' ON INSERT ONLY,
'Name' = '@Name' ON INSERT ONLY,
'Customer' = '@Customer',
'NmosDomainName' = '@NmosDomainName' ON INSERT ONLY
);
```

f. Update the Gateway for the display layer ObjectServers. Edit the `NCHOME/omnibus/etc/A_TO_D_GATE.tblrep.def` file and add the following REPLICATE statements for the tables that were created by the `create_sae_automation.sql` script to the bottom of the file. This mapping must be identical to the mapping in the aggregation layer gateway. If you later change the mapping in the bidirectional gateway for the aggregation layer ObjectServers, you must replicate those changes here.

```
REPLICATE ALL FROM TABLE 'precision.entity_service'
USING MAP 'EntityServiceMap'
INTO 'precision.entity_service';

REPLICATE ALL FROM TABLE 'precision.service_details'
USING MAP 'ServiceDetailsMap'
INTO 'precision.service_details';
```

5. Delete all previous Network Manager events from the alerts.status table in the ObjectServers. Use an appropriate SQL command to delete the events. For more information, see the Tivoli Netcool/OMNIbus documentation at http://www-01.ibm.com/support/knowledgecenter/SSSHTQ_7.4.0/com.ibm.netcool_OMNIbus.doc_7.4.0/omnibus/wip/admin/concept/omn_adm_sql_objservsqlcommands.html.
6. Restart the ObjectServer Gateways.
7. Restart the **ncp** processes.

Changing the Tivoli Netcool/OMNIbus Web GUI data source name

To connect to a different Web GUI data source than the one specified during installation, change the data source name.

To connect to a different data source than the one that you specified during installation:

1. Edit the `NCHOME/etc/precision/ModelNcimDb.cfg` file.
2. Change the m_WebTopDataSource property to the new data source name.
3. Restart the ncp_model process.

Tivoli Netcool/OMNIbus Web GUI data sources:

A data source is another term for an ObjectServer or ObjectServer failover pair used by the Web GUI for event information.

The Tivoli Netcool/OMNIbus Web GUI was known as Netcool/Webtop in versions 2.2 and below. Some deployments contain many ObjectServers, and the Web GUI can contain events from several different ObjectServers. You can configure the Web GUI for one data source during installation. After installation, you might need to change this data source, or add new data sources.

Data sources and network topology

To display device status, the Network Views and the Hop View correlate the topology record for a device with any events on that device. To perform this correlation, the Web applications must have access to the name of each data source used by the Web GUI.

Data sources and the NCIM database

Information about the Web GUI data sources is held in the database table ncim.domainMgr in the NCIM topology database.

For more information on configuring the Web GUI data sources, see the *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide*.

Configuring topology event types for the Active Event List (AEL)

To integrate the topology views and filtered AEL views, the view name and type must match. If you change the defaults in the AEL, you must configure the name and type in Network Manager.

In a filtered AEL view, you can configure the name and view type. If you change the view name and type from the default values of `Default` and `global`, then the AEL cannot communicate with the Network Views and right-click tools.

If the default values have been changed, you must change the values on the Network Manager server to match.

To edit the view name and type used for communicating with the AEL, complete the following steps:

1. Back up and edit the file `topoviz.properties`.
2. Change the values of the following properties:

```
# AEL view descriptions.
topoviz.webtop.view.name=Default
topoviz.webtop.view.type=global
```

Adding event fields

To use Tivoli Netcool/OMNIbus version 7.1, you must add additional database fields to the alerts.status table and to any Tivoli Netcool/OMNIbus gateway map files.

Tip: You do not need to perform this task if you are using Tivoli Netcool/OMNIbus version 7.2 or later.

The required fields are as follows:

NmosDomainName
The name of the Network Manager domain that is managing the event. By default, this field is only populated for events which are generated by Network Manager polls. To populate this field for other event sources such as the ones from Tivoli Netcool/OMNIbus probes, you have to modify the rules files.

NmosEntityId
A unique numerical ID which identifies the topology entity that the event has been associated with. This field is similar to the NmosObjInst field, but contains more detailed information. For example, it can include the ID of an interface within a device.

NmosManagedStatus
The managed status of the network entity the event was raised for. When a network entity is unmanaged, the Network Manager polls are suspended, and events from other sources are tagged as unmanaged. This field allows you to filter out events from unmanaged entities.

BSM_Identity
The unique identifier of the resource from where the event originates, and is used to correlate the event to that resource in IBM Tivoli Business Service Manager (TBSM).

NmosEventMap
The event map name and optional precedence for the event, which indicates how Network Manager should process the event; for example, PrecisionMonitorEvent.910. The optional precedence number can be concatenated to the end of the value, following a period (.). If the precedence is not supplied, it is set to 0.

Note: This value can be overridden by an explicit insertion into the Event Gateway config.precedence table, which provides the same data.

To add the fields to the alert.status database table, run the following SQL script against each ObjectServer in your deployment:

- UNIX

```
$NCHOME/omnibus/bin/nco_sql -server objectserver_name -user username -password
password < $NCHOME/precision/scripts/ncp_configure_omnibus.sql
```

- Windows

```
"%NCHOME%\omnibus\bin\isql.bat" -S objectserver_name -U username -P password -i
"%NCHOME%\precision\scripts\ncp_configure_omnibus.sql"
```

For more information about administering Tivoli Netcool/OMNIbus, see the *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Installing and configuring probes

If you did not install Tivoli Netcool/OMNIbus as part of the Network Manager installation, and you are using an existing Tivoli Netcool/OMNIbus installation, you must configure certain probes.

To ensure that your Tivoli Netcool/OMNIbus installation receives events from the network, you must configure the relevant Tivoli Netcool/OMNIbus probes. At a minimum you must install and configure the SNMP probe (also known as the mttrapd probe). You can use the **ConfigOMNI** script, for more information, see "Configuring an existing Tivoli Netcool/OMNIbus installation" on page 51.

For more information about probe installation and configuration, see the relevant probe reference guide, available from the Information Center at http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/common/kc_welcome-444.html.

Installing the Knowledge Library

If you did not install Tivoli Netcool/OMNIbus as part of the Network Manager installation, and you are using an existing Tivoli Netcool/OMNIbus installation, you must install the Netcool/OMNIbus Knowledge Library.

The Netcool/OMNIbus Knowledge Library is a set of rules files written to a common standard and is available with your Tivoli Netcool/OMNIbus installation. You can use the **ConfigOMNI** script to install the library, see "ConfigOMNI command-line options" on page 53.

For more information, see the Netcool/OMNIbus Knowledge Library Release Notes®.

Tivoli Netcool/OMNIbus integration reference

Read about settings for additional interaction between Network Manager and Tivoli Netcool/OMNIbus.

Network Manager event categories:

The events that are raised by Network Manager fall into two categories: events about the network being monitored and events about Network Manager processes.

These events are stored in the Tivoli Netcool/OMNIbus ObjectServer. The Probe for Tivoli Netcool/OMNIbus (**nco_p_ncpmonitor**) is used to process and forward the event data to the alerts.status table in the ObjectServer.

The following figure shows the flow of events from Network Manager to the ObjectServer.

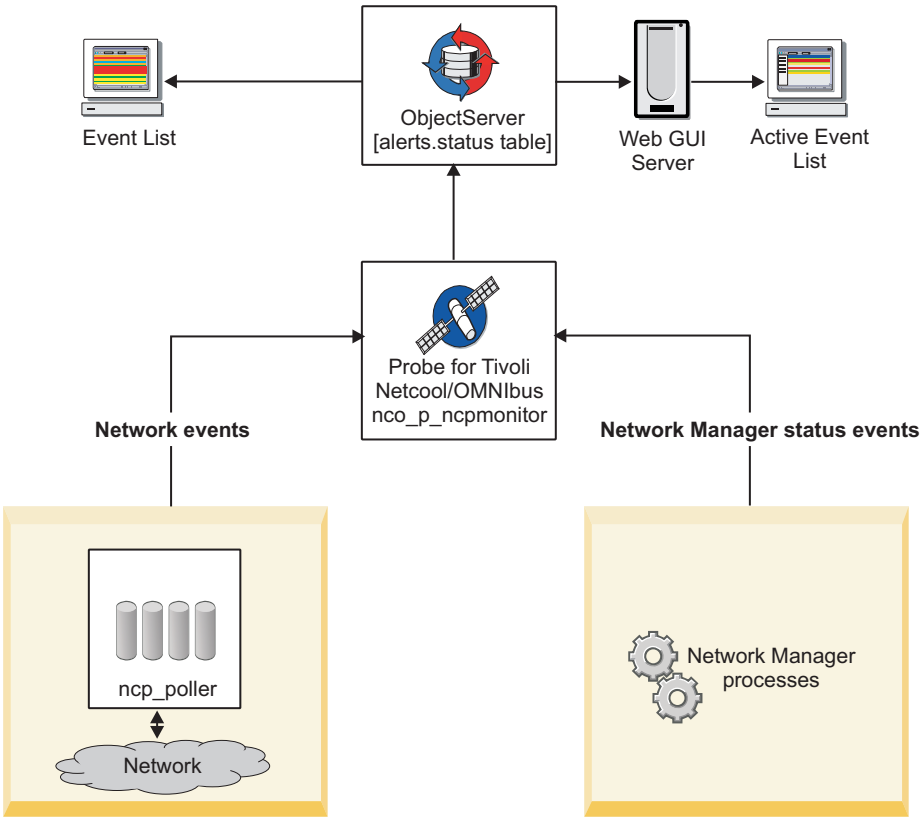

Figure 9. Flow of events from Network Manager to Tivoli Netcool/OMNIbus

Network Manager network events:

The Polling engine, **ncp_poller**, generates events about the state of the network. These events can be used to identify network problems, and are configurable by using the Network Polling GUI (go to **Administration** > **Network** > **Network Polling**). These events are known as network events and have the alerts.status AlertGroup field value of `ITNM Monitor`.

Each network event is raised on a single entity, such as an interface or a chassis, and the event data is dependent on the type of poll. When network events are forwarded to the ObjectServer for insertion into the alerts.status table, they are allocated an AlertGroup value of `ITNM Monitor`.

An unlimited set of event identifiers is available for network events. Events that are generated when an SNMP poll fails are specifically allocated an EventID value of `NmosSnmpPollFail` in the alerts.status table.

Network events in the ObjectServer are pulled back into Network Manager through the Event Gateway to perform event enrichment, including root cause analysis.

Related reference:

"alerts.status fields used by Network Manager" on page 174
The alerts.status table in the ObjectServer contains status information about problems that have been detected by probes.

Network Manager status events:

Network Manager can generate events that show the status of various Network Manager processes. These events are known as Network Manager status events and have the alerts.status AlertGroup field value of `ITNM Status`.

When these status events are forwarded to the ObjectServer for insertion into the alerts.status table, they are allocated an AlertGroup value of `ITNM Status`.

Status event types

A set of event identifiers is used to identify Network Manager status events by type. The following list identifies the EventId values that are inserted in the alerts.status table, and describes how each associated status event is generated.

ItnmDatabaseConnection
This type of event is generated to indicate loss of connection to NCIM. This event is generated by the managed status polling thread in the **`ncp_model`** process. The raising of this event depends on the time period configured in the managed status polling interval in model. A problem event is raised if the connection is lost, and a corresponding resolution event is raised if the connection is restored, or at startup to clear any failures from a previous operation. This event type allows the backup domain to take over when failover is configured. The virtual domain process reacts to this event as defined in the filter for NCIM in the `NCHOME/etc/precision/VirtualDomainSchema.cfg` file.

ItnmDiscoAgentStatus
This type of event is generated by **`ncp_disco`** when a discovery agent transitions to a new state. At the end of a discovery, an information event is forwarded to the ObjectServer, for each agent that was used during the discovery.

You can use this information to identify the state of each agent. In the alerts.status table, the LocalPriObj field is used to store the name of the agent.

Discovery agent events in the ObjectServer are overwritten when a subsequent discovery is run.

ItnmDiscoFinderStatus
This type of event is generated by **`ncp_disco`** when a discovery finder transitions to a new state. At the end of a discovery, an information event is forwarded to the ObjectServer, for each finder that was used during the discovery.

You can use this information to identify which finders are running and their state. In the alerts.status table, the LocalPriObj field is used to store the name of the finder.

Discovery finder events in the ObjectServer are overwritten when a subsequent discovery is run.

ItnmDiscoPhase
This type of event is generated by **`ncp_disco`** when the discovery process transitions to a new phase. At the end of the discovery, five information events should be present in the ObjectServer, to show the looped transitions from phase 0 (standby) to phases 1, 2, and 3 (data collection) to phase -1 (data processing). An event is raised for each of the following phase changes in a single discovery:

- 0 to 1
- 1 to 2
- 2 to 3
- 3 to -1
- -1 to 0

You can use this information to determine the length of each phase. In the alerts.status table, the LocalPriObj field is used to store the phase to which the discovery is transitioning, and the LocalSecObj field stores the previous phase of the discovery.

Tip: The string values for the phases are also shown in the discovery log file when the **ncp_disco** process is run in debug mode.

Discovery phase events in the ObjectServer are overwritten when a subsequent discovery is run.

ItnmDiscoStitcherStatus

The discovery process is made up of a data collection stage and a data processing stage, during which the topology is created. ItnmDiscoStitcherStatus events are generated by the Discovery engine, **ncp_disco**, when a major phase is reached in the data processing stage. At the end of the discovery, an information event is forwarded to the ObjectServer, for each major discovery stitcher that was used during the discovery.

You can use this information to identify what phase in the data processing stage the discovery is in. In the alerts.status table, the LocalPriObj field is used to store the name of the stitcher corresponding to this phase.

ItnmDiscoStitcherStatus events are raised when the following stitchers begin executing:

- BuildFinalEntityTable
- BuildContainment
- BuildLayers
- MergeLayers
- PostLayerProcessing

Subsequently events are raised during the topology creation phase when the following stitchers are run.

- CreateScratchTopology
- PostScratchProcessing
- SendTopologyToModel

Discovery stitcher events in the ObjectServer are overwritten when a subsequent discovery is run.

ItnmEntityCreation

If configured in the `$NCHOME/etc/precision/ModelSchema.cfg` file, this type of information event is generated by **ncp_model**, for each new chassis or IP interface entity (EntityType = 1) that is inserted into the NCIM database.

You can configure `ModelSchema.cfg` by setting the value of the RaiseEntityEvent column to 1 in the INSERT statement for the model.config table. For example:

```
create table model.config
(
LingerTime int not null primary key,          // default value 3 (discoveries)
```

```
RaiseEntityEvent int type boolean not null,    // default value 0 ( off )
DiscoveryUpdateMode int not null,              // default value 0 - full discovery,
                                               //               1 - partial
unique(LingerTime)
);
insert into model.config values (3, 1, 0);
```

Note: For the configuration changes to take effect and enable the events, the **ncp_model** process must be restarted. The process reads the configuration settings at start-up.

ItnmEntityDeletion

If configured in the `$NCHOME/etc/precision/ModelSchema.cfg` file, this type of information event is generated by **ncp_model**, for each chassis or IP interface entity (EntityType = 1) that is deleted from the NCIM database.

You can configure `ModelSchema.cfg` by setting the value of the RaiseEntityEvent column to 1 in the INSERT statement for the model.config table, as shown in the preceding description for the ItnmEntityCreation EventId.

ItnmFailover

This type of event is generated by **ncp_virtualdomain** when a Network Manager domain within a failover pair fails over or fails back.

A problem event is generated when failover occurs and a resolution event is generated on failback.

In the alerts.status table, the Summary field description indicates whether the domain is the primary or backup, and whether it is in an active or a standby mode.

ItnmFailoverConnection

This type of event is generated by **ncp_virtualdomain** to indicate when the backup domain in a failover pair connects to, or disconnects from, the primary domain.

When Network Manager runs in failover mode, a resolution event is generated when the primary and backup domains set up their TCP socket connection. This socket connection is required to transfer the topology updates from the primary domain because the discovery process (**ncp_disco**) does not run in the backup domain. If the connection is subsequently lost, a problem event is generated.

Note: The status of the connection does not determine whether failover is triggered. Failover is triggered only when health check events are transferred (via the ObjectServer) across domains, and provided a socket connection has, at some point, been established.

ItnmHealthChk

Health check events govern Network Manager failover. Each domain in the failover pair generates health check resolution events while that domain is healthy.

Health check problem events for a domain can be generated in two ways:

- By the local domain: The local domain detects a failure of one of its processes, as configured in the `$NCHOME/etc/precision/VirtualDomainSchema.cfg` file.
- By the remote domain: One domain detects that the other domain has not generated a health check resolution event in the configured amount of time, and generates a synthetic health check problem event on behalf of the remote domain.

When a health check problem event is generated for the primary domain, failover is initiated, and the backup domain becomes active.

Health check events were previously allocated an EventID value of NcpHealthChk. For compatibility with earlier versions of Network Manager, you can substitute NcpHealthChk in place of ItnmHealthChk in the probe rules file.

Note: Health check events are handled by the Network Manager Event Gateway, which requires the Node value to be the domain to which the event refers. This need not be the domain raising the event, since one domain can raise failure events on behalf of the other.

ItnmMaintenanceState

If configured in the `$NCHOME/etc/precision/ModelSchema.cfg` file, this type of event is generated by the Topology manager, **ncp_model**, for maintenance status changes to a chassis or an IP interface.

You can configure `ModelSchema.cfg` by setting the value of the RaiseEntityEvent column to 1 in the INSERT statement for the model.config table, as shown in the preceding description for the ItnmEntityCreation event.

A problem event is generated when the chassis or IP interface entity is in maintenance, and a resolution event is generated when the entity is out of maintenance.

Note: An individual interface event is sent only if the change does not apply at the chassis level; when a device changes, a chassis event and a series of interface events are not collectively generated.

ItnmServiceState

This type of event is generated when a process starts or ends, and signifies whether a process has failed to start or has stopped during runtime. (Note that process state events are not generated when processes are stopped at system shutdown.)

A resolution event is generated when **ncp_ctrl** starts a process. If a process fails to start or if it stops during runtime, a problem event is generated.

In the alerts.status table, the Summary field description includes the process name, the PID, and an indication of whether the process has:

- Started (and successfully initialized)
- Stopped (that is, it has been deleted from the **ncp_ctrl** database table named services.inTray)
- Terminated (that is, it stopped, but will be restarted by **ncp_ctrl**)
- Failed to start
- Failed and will not be restarted (that is, it stopped and the number of retries configured for the process has been exceeded)

ItnmTopologyUpdated

This type of information event is generated by **ncp_model** when the update of the NCIM topology database is completed at the end of a discovery cycle. This information is useful if you intend to program scripts or procedures to run after the NCIM database is updated.

Note: If the feedback option is on, or large subnets are pinged, there might be multiple discovery cycles and thus multiple events of this type, one

event for each discovery cycle. To determine if discovery has finally finished, the following OQL query can be made to the Ping Finder service:

```
select * from pingFinder.status where m_Completed <> 1;
```

This query looks for any subnets that the Ping finder is still pinging. If there are no outstanding ping sweeps and the discovery is in phase 0, this means that the discovery is complete.

Related concepts:

"About failover" on page 275
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.

Related tasks:

"Enabling failover" on page 275
You can enable failover in your Network Manager environment to ensure that the different components are kept running and available.

Related reference:

"alerts.status fields used by Network Manager" on page 174
The alerts.status table in the ObjectServer contains status information about problems that have been detected by probes.

Configuration of the Probe for Tivoli Netcool/OMNIbus:

The 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.

The Probe for Tivoli Netcool/OMNIbus is installed in the `$NCHOME/probes/`*arch* directory, where *arch* represents an operating system directory. You can configure the probe by using its configuration files, which are as follows:

- Properties file: `nco_p_ncpmonitor.props`
- Rules file: `nco_p_ncpmonitor.rules`

Note: The executable file (or **nco_p_ncpmonitor** command) for the probe is also installed in the `$NCHOME/probes/`*arch* directory. The probe is, however, configured to run under the domain process controller CTRL, by default, and the **nco_p_ncpmonitor** command should be run manually only for troubleshooting purposes.

The events raised in Network Manager are domain-specific. When Network Manager runs in failover mode, the probe uses the virtual domain name by default, provided the name is configured in the `$NCHOME/etc/precision/ConfigItnm.cfg` file.

For more information about probe concepts, see the *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* in the Tivoli Netcool/OMNIbus information centre at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Related tasks:

"Configuring failover using the ConfigItnm.cfg file" on page 308
When you use the $NCHOME/etc/precision/ConfigItnm.*DOMAIN*.cfg file to configure failover, the Network Manager processes will read the file on startup to identify whether they are running in the primary or backup domain. Similarly, the **ncp_model** process will identify whether NCIM replication is in use, and run appropriately for that configuration.

About the nco_p_ncpmonitor.props file:

The $NCHOME/probes/*arch*/nco_p_ncpmonitor.props file defines the environment in which the Probe for Tivoli Netcool/OMNIbus runs.

The properties file is formed of name-value pairs that are separated by a colon. The default properties file lists a subset of the properties that the probe supports; these properties are commented out with a number sign (#) at the beginning of the line. The standard set of common probe properties, which are applicable for the version of Tivoli Netcool/OMNIbus being run, can be specified for the Probe for Tivoli Netcool/OMNIbus, where relevant.

A suggested practice for changing the default values of the properties is that you add a name-value line for each required property at the bottom of the file. To specify a property, ensure that the line is uncommented and then modify the value as required. String values must be enclosed in quotation marks; other values do not require quotation marks. For example:

```
Server            :    "VIRTUAL"
RulesFile         :    "$NCHOME/probes/solaris2/nco_p_ncpmonitor.rules"
Buffering         :    1
BufferSize        :    15
```

For troubleshooting purposes, you can alternatively configure probe properties from the command line by running the **nco_p_ncpmonitor** command with the relevant command-line options.

For information about the properties that are common to probes, see the *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* in the Tivoli Netcool/OMNIbus information centre at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

About the nco_p_ncpmonitor.rules file:

The $NCHOME/probes/*arch*/nco_p_ncpmonitor.rules file defines how the Probe for Tivoli Netcool/OMNIbus should process Network Manager event data to create a meaningful Tivoli Netcool/OMNIbus event.

nco_p_ncpmonitor.rules configuration reference:

The rules file maps Network Manager event data to ObjectServer fields, and can be used to customize the behavior of the probe. Knowledge of the Tivoli Netcool/OMNIbus probe rules syntax is required for rules file configuration.

The probe uses tokens and elements, and applies rules, to transform Network Manager event source data into a format that the ObjectServer can recognize. The raw event source data is converted to tokens, which are then parsed into elements. The rules file is used to perform conditional processing on the elements, and to map them to ObjectServer alerts.status fields. In the rules file, elements are

identified by the $ symbol and alerts.status fields are identified by the @ symbol. The rules file configuration maps elements to fields, as shown in the following sample code:

```
@Summary=$Description
```

In this example, @Summary identifies the alerts.status field, and $Description identifies the Network Manager input field.

Where the Network Manager ExtraInfo field is used with nested fields to store additional data on entities (for example, ExtraInfo->ifIndex), these fields are available in the following format in the rules file:

```
$ExtraInfo_variable
```

Where *variable* represents a Management Information Base (MIB) variable (for example, ifIndex), or other data (for example, column names in NCIM tables). MIB variables are specified in mixed case characters, and other data, in uppercase characters. For example:

```
$ExtraInfo_ifIndex
$ExtraInfo_MONITOREDENTITYID
```

To configure the rules file for the Probe for Tivoli Netcool/OMNIbus, it is necessary to have an understanding of:

- The Network Manager event source data that is available for use in the probe rules file
- The set of alerts.status fields that can be populated with event data from Network Manager
- The data mapping between the Network Manager and alerts.status fields

For information about the syntax used in probe rules files, see the *IBM Tivoli Netcool/OMNIbus Probe and Gateway Guide* in the Tivoli Netcool/OMNIbus information centre at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Example of rules file processing:

This example shows how source data from Network Manager is processed by the rules file to generate the output data that is inserted in the alerts.status table.

The following sample code shows a Network Manager event data record that is passed to the Probe for Tivoli Netcool/OMNIbus for processing. In this record, a resolution event was created when **ncp_ctrl** started the **ncp_store** process.

```
{
 EventName='ItnmServiceState';
 Severity=1;
 EntityName='BACKUP';
 Description='ncp_store process [15299] has started';
 ExtraInfo={
  EVENTTYPE=2;
  SOURCE='ncp_ctrl';
  ALERTGROUP='ITNM Status';
  EVENTMAP='ItnmStatus';
  SERVICE='ncp_store';
  PID=15299;
  };
}
```

The following excerpt from the probe rules file shows the syntax used to process and map these input fields to alerts.status fields:

```
...
    #
    # populate some standard fields
    #
    @Severity = $Severity
    @Summary = $Description
    @EventId = $EventName
    @Type = $ExtraInfo_EVENTTYPE
    @AlertGroup = $ExtraInfo_ALERTGROUP
    @NmosEventMap = $ExtraInfo_EVENTMAP
    @Agent = $ExtraInfo_SOURCE

    if (exists($ExtraInfo_ACCESSIPADDRESS))
    {
        @Node = $ExtraInfo_ACCESSIPADDRESS
    }
    else
    {
        @Node = $EntityName
    }

    #
    # Stamp the event with the name of its originating domain
    #
    @NmosDomainName = $Domain
    @Manager = "ITNM"
    @Class = 8000

    #
    # populate fields for RCA
    #
    @LocalNodeAlias = @Node

...

    #
    # Now set the AlertKey and Identifier
    #
    if (match(@AlertGroup, "ITNM Status"))
    {
        switch ($EventName)
        {
            case ...
...
            case "ItnmServiceState":
                @LocalPriObj = $ExtraInfo_SERVICE
...
            case ...
....
        }
    }

    #
    # Both the Identifier and the AlertKey contain the domain name. This ensures
    # that in a multi-domain setup, events are handled on a per-domain basis
    #

    #
    # Include the LocalPriObj in the AlertKey or the link-downs on
    # all interfaces will cleared by a link-up on any interface
    #
    @AlertKey = $EntityName + @LocalPriObj + "->" + $EventName + @NmosDomainName

    #
    # Set up deduplication identifier and include the LocalPriObj
    # so we can correctly handle de-duplication of events raised on interfaces
    #
    @Identifier = $EntityName + @LocalPriObj + "->" + $EventName + @Type + @NmosDomainName
}
```

When rules file processing is complete, the output data that is forwarded to the ObjectServer takes the following form:

```
CMonitorProbeApp::ProcessStatusEvent
{
 AlertGroup='ITNM Status';
 EventId='ItnmServiceState';
 Type=2;
 Severity=1;
 Summary='ncp_store process [15299] has started';
 Node='BACKUP';
 NmosDomainName='PRIMARY';
 LocalNodeAlias='BACKUP';
 LocalPriObj='ncp_store';
 LocalRootObj='';
 RemoteNodeAlias='';
 AlertKey='BACKUPncp_store->ItnmServiceStateVIRTUAL';
 Identifier='BACKUPncp_store->ItnmServiceState2VIRTUAL';
 Class=8000;
 Agent='ncp_ctrl';
 LastOccurrence=1267122089;
}
```

Based on the rules file processing in this example, it can be seen that the Network Manager input fields map to the alerts.status fields as follows:

Network Manager field	alerts.status field
EventName	EventId
Severity	Severity
EntityName	Node
Description	Summary
ExtraInfo->EVENTTYPE	Type
ExtraInfo->SOURCE	Agent
ExtraInfo->ALERTGROUP	AlertGroup
ExtraInfo->EVENTMAP	NmosEventMap
ExtraInfo->SERVICE	LocalPriObj

Related reference:

"alerts.status fields used by Network Manager" on page 174
The alerts.status table in the ObjectServer contains status information about problems that have been detected by probes.

Network Manager event data fields:

When events are generated in Network Manager, the event data is inserted into a number of fields (or columns) in the Network Manager tables. Although each event uses only a subset of the possible fields, a number of fields are common to all event types.

The following table lists all the Network Manager field names that are available for use in the probe rules file, and describes the event data stored in each field. The table also identifies which of the Network Manager fields are common to all events, and therefore always available in the rules file.

Table 16. Network Manager fields that populate events

Network Manager field name	Field content	Always available?
Description	A brief description of the event.	Yes

Table 16. Network Manager fields that populate events (continued)

Network Manager field name	Field content	Always available?
Domain	The current domain. If Network Manager is configured for failover mode, this will be the primary domain.	Yes (provided the map file is not modified)
EntityName	For network events, this is the entityName field from the NCIM entityData table for the entity against which the event is raised. For status events, this is always the name of the domain about which the event is generated.	Yes
EventName	The event identifier. For example, ItnmDiscoPhase.	Yes
ExtraInfo_ACCESSIPADDRESS	If the main node or interface entity identified by the EntityName input field has a directly-accessible IP address (the accessIPAddress field from the NCIM interface or chassis tables), then it is supplied here. Applicable to network events only.	No
ExtraInfo_AGENT	The agent responsible for a discovery agent (ItnmDiscoAgentStatus) event.	Yes (for ItnmDiscoAgentStatus events)
ExtraInfo_ALERTGROUP	The alert group of the event. For Network Manager status events, the alert group is `ITNM Status`, and for network events, the value is `ITNM Monitor`.	Yes
ExtraInfo_ENTITYCLASS	The name of class assigned to the entity, as identified the NCIM entityClass and classMembers tables.	Yes (for network and ItnmEntityCreation events)
ExtraInfo_ENTITYTYPE	The type of the entity, as defined in the NCIM entityType table.	Yes (for network events)
ExtraInfo_LocalPriObj	Provides a value for the LocalPriObj field in the alerts.status record. This field has the same value as the deprecated ExtraInfo_EventSnmpIndex field, except that it is prefixed by an identifier for the MIB entity being polled; for example ifEntry, bgpPeerEntry.	Yes (for network events)
ExtraInfo_EVENTTYPE	The type of the event raised by Network Manager. The values are as follows: • 1: Problem • 2: Resolution • 13: Information	Yes
ExtraInfo_FINDER	The finder responsible for a discovery finder (ItnmDiscoFinderStatus) event.	Yes (for ItnmDiscoFinderStatus events)
ExtraInfo_ifIndex	For events raised against an interface with an ifIndex value in the NCIM interface table, that value is given here. Applicable only to network events against interfaces.	No

Table 16. Network Manager fields that populate events (continued)

Network Manager field name	Field content	Always available?
ExtraInfo_IFALIAS	For events raised against interfaces, this field contains the ifAlias value, if known. Applicable only to network interface polls.	No
ExtraInfo_IFDESCR	For events raised against interfaces, this field contains the ifDescr value, if known. Applicable only to network interface polls.	No
ExtraInfo_IFNAME	For events raised against interfaces, this field contains the ifName value, if known. Applicable only to network interface polls.	No
ExtraInfo_IFTYPESTRING	For events raised against interfaces, this field contains the string representation of the ifType value. Applicable only to network interface polls.	No
ExtraInfo_MAINNODEADDRESS	The management interface of the main node containing the entity, as identified by the accessIPAddress field of the NCIM chassis table. Applicable only to network and ItnmEntityCreation events.	Yes (for network events)
ExtraInfo_MAINNODEENTITYID	The entityId field from the NCIM entityData table for the main node, as identified by the accessIPAddress field of the NCIM chassis table. Applicable only to network events.	Yes (for network events)
ExtraInfo_MAINNODEENTITYNAME	The entityName field from the NCIM entityData table for the main node, as identified in NCIM. Applicable only to network events.	Yes (for network events)
ExtraInfo_MONITOREDENTITYID	The entityId field from the NCIM entityData table for the entity against which the event is raised. Applicable only to network and ItnmEntityCreation events.	No
ExtraInfo_MONITOREDINSTID	A record in the ncpolldata.monitoredInstance table.	No
ExtraInfo_NEWPHASE	The discovery phase that has started. Applicable only to discovery phase (ItnmDiscoPhase) events.	Yes (for discovery phase events)
ExtraInfo_OLDPHASE	The discovery phase that has completed. Applicable only to discovery phase (ItnmDiscoPhase) events.	Yes (for discovery phase events)
ExtraInfo_POLICYNAME	The name of the polling policy that resulted in the event.	Yes (for network events)
ExtraInfo_PID	The process ID of the affected Network Manager service. Applicable only to ItnmServiceState events.	Yes (for service state events)
ExtraInfo_REMOTEDOMAIN	The name of the remote domain. Applicable only to ItnmFailoverConnection events.	Yes (for failover connection events)
ExtraInfo_sysContact	If available, the sysContact value is given for ItnmEntityCreation events only.	No
ExtraInfo_sysLocation	If available, the sysLocation value is given for ItnmEntityCreation events only	No

Table 16. Network Manager fields that populate events (continued)

Network Manager field name	Field content	Always available?
ExtraInfo_sysObjectId	If available, the sysObjectId value is given for ItnmEntityCreation events only	No
ExtraInfo_SERVICE	The name of the affected Network Manager service. Applicable only to ItnmServiceState events.	Yes (for service state events)
ExtraInfo_SNMPSTATUS	A numerical SNMP status code.	Yes (for NmosSnmpPollFail events)
ExtraInfo_SNMPSTATUSSTRING	A human-readable indication of the SNMP failure state.	Yes (for NmosSnmpPollFail events)
ExtraInfo_SOURCE	The name of the process from which the event originated.	Yes
ExtraInfo_STITCHER	The stitcher responsible for a discovery stitcher (ItnmDiscoStitcherStatus) event.	Yes (for ItnmDiscoStitcherStatus events)
Severity	The severity level of the event. The severity is a non-zero value.	Yes

Related reference:

"Network Manager network events" on page 162
The Polling engine, **ncp_poller**, generates events about the state of the network. These events can be used to identify network problems, and are configurable by using the Network Polling GUI (go to **Administration** > **Network** > **Network Polling**). These events are known as network events and have the alerts.status AlertGroup field value of `ITNM Monitor`.

"Network Manager status events" on page 163
Network Manager can generate events that show the status of various Network Manager processes. These events are known as Network Manager status events and have the alerts.status AlertGroup field value of `ITNM Status`.

alerts.status fields used by Network Manager:

The alerts.status table in the ObjectServer contains status information about problems that have been detected by probes.

A subset of the standard alerts.status fields is populated with Network Manager event data. Additionally, a set of dedicated alerts.status fields are reserved to hold data that is specific to Network Manager. The dedicated alerts.status field names are identifiable by the prefix `Nmos`.

The following table describes the alerts.status fields that are populated by Network Manager fields. Some of these alerts.status fields are allocated default values from within the probe rules file. (Avoid modifying these default values.)

Table 17. alerts.status fields used by Network Manager

alerts.status field	Data type	Description	Network Manager field name/Default value in rules file
Agent	varchar(64)	The name of the process that generated the event. You can use this field to filter an AEL to display only events of a specific type; for example, only discovery events (with a value of ncp_disco).	ExtraInfo_SOURCE
AlertGroup	varchar(255)	Used to group events by type. Values supplied by default from Network Manager events are either `ITNM Monitor` for network events, or `ITNM Status` for status events.	ExtraInfo_ALERTGROUP
AlertKey	varchar(255)	A text string concatenating several elements relating to the event. Elements can include the event ID, domain, phase, and process name. Allows problem and resolution events to be matched.	This value is generated from the input to ensure appropriate matching of problem and resolution events within the ObjectServer.
Class	integer	The alert class asigned to the Probe for Tivoli Netcool/OMNIbus.	A value of `8000` is reserved for events generated by Network Manager.
EventId	varchar(255)	The type of event (for example, SNMPTRAP-linkDown). The Event Gateway uses this value to look up the event map, and to determine the precedence of events.	EventName
ExpireTime	integer	The expiry time of the event in the database. Not currently used by Network Manager.	
FirstOccurrence	time	A timestamp indicating when the event first occurred.	
Identifier	varchar(255)	A unique value for each type of event on a given entity (for example, a LinkDown event on a specific device interface). This identifier controls deduplication.	This value is generated from the input to ensure appropriate deduplication of events in the ObjectServer. In the rules file, the identifier is constructed as a concatenation of field values.
LastOccurrence	time	A timestamp indicating when the event last occurred.	
LocalNodeAlias	varchar(64)	The IP or DNS address of the device. This value usually refers to the chassis, but for pingFails only, can correspond to the interface.	For network events, this field is set to the same value as the Node field. No value is set for status events, to ensure that they are not fed back into Network Manager through the Event Gateway.

Table 17. alerts.status fields used by Network Manager (continued)

alerts.status field	Data type	Description	Network Manager field name/Default value in rules file
LocalPriObj	varchar(255)	The specific entity for which the event is generated; for example, the ifIndex, ifDescr, or ifPhysAddress field value.	ExtraInfo_AGENT or ExtraInfo_FINDER or ExtraInfo_ifIndex or ExtraInfo_NEWPHASE or ExtraInfo_SERVICE or ExtraInfo_STITCHER The ExtraInfo_ifIndex value is shown using the syntax `ifEntry.<ifIndex>`; for example, `ifEntry.12`.
LocalRootObj	varchar(255)	The container of the entity referenced in the LocalPriObj field. This need not be the chassis, but could, for example, be slot in a chassis. The chassis can still be identified using LocalNodeAlias.	
LocalSecObj	varchar(255)	The secondary object referenced by the event.	ExtraInfo_OLDPHASE
Manager	varchar(64)	A descriptive name that identifies the system that forwarded the events.	A value of `ITNM` is used for events generated by Network Manager V3.8, or later. A value of `Omnibus` is used in earlier versions.
NmosCauseType	integer	The event state. Populated by the NMOS gateway. The possible values are as follows: • 0: Unknown • 1: Root Cause • 2: Symptom	
NmosDomainName	varchar(64)	The name of the Network Manager network domain that raised the event. The name of the primary domain is used in failover mode. By default, this field is populated only for events that are generated by Network Manager. To populate this field for other event sources, such as those from other probes, you must modify the rules files for those probes. This field is populated by the Event Gateway if an event is matched to an entity in a domain.	Domain

Table 17. alerts.status fields used by Network Manager (continued)

alerts.status field	Data type	Description	Network Manager field name/Default value in rules file
NmosEntityId	integer	The unique Object ID that identifies the topology entity with which the event is associated. This field is similar to the NmosObjInst field but contains more detailed information. For example, this field can include the ID of an interface within a device. For events generated by the Polling engine, the NmosEntityId field is populated in the probe rules file. For all other events, this field is populated by the gateway when the entity is identified.	ExtraInfo_MONITOREDENTITYID
NmosEventMap	varchar(64)	The event map name and optional precedence for the event, which indicates how Network Manager should process the event; for example, PrecisionMonitorEvent.910. The optional precedence number can be concatenated to the end of the value, following a period (.). If the precedence is not supplied, it is set to 0. **Note:** This value can be overridden by an explicit insertion into the Event Gateway config.precedence table, which provides the same data.	
NmosManagedStatus	integer	The managed status of the network entity for which the event was raised. When a network entity is unmanaged, the Network Manager polls are suspended and events from other sources are tagged as unmanaged. This field allows you to filter out events from unmanaged entities. The possible values for this field are as follows: • 0: Managed • 1: Operator unmanaged • 2: System unmanaged • 3: Out of scope	
NmosObjInst	integer	The unique Object ID that identifies the containing topology chassis entity with which the event is associated. Populated by the NMOS gateway. **Tip:** This field can be used to detect whether the event has been passed for event enrichment.	
NmosSerial	integer	The serial number of the event that is suppressing the current event. Populated by the NMOS gateway.	

Table 17. alerts.status fields used by Network Manager (continued)

alerts.status field	Data type	Description	Network Manager field name/Default value in rules file
Node	varchar(64)	The device from which the event originated. If an event is raised against an entity with an accessible IP address, the IP address is used. Otherwise, the entityName value from NCIM is used. By default, Node has the same value as LocalNodeAlias.	ExtraInfo_ACCESSIPADDRESS or EntityName The EntityName value maps to the Node field only if the ExtraInfo_ACCESSIPADDRESS input field is empty.
NodeAlias	varchar(64)	The IP address of the main node, if available.	ExtraInfo_MAINNODEADDRESS
RemoteNodeAlias	varchar(64)	The network address of a remote node, where relevant. For example: • A blank value (where an interface has gone down) • A neighbouring address (where a connected interface has gone down) • The polling station (for a ping failure event)	
Serial	incr	A unique ID per event per ObjectServer instance. Where primary and backup ObjectServers are configured, the ObjectServers will have different serial numbers for the same event.	
ServerName	varchar(64)	The name of the originating ObjectServer.	
ServerSerial	integer	The Serial number of the event in the originating ObjectServer. Where primary and backup ObjectServers are configured, the ObjectServers will have different serial numbers for the same event. If the event originated in the current ObjectServer, the ServerSerial value is the same as the Serial value.	
Severity	integer	The severity level of the event stored in the ObjectServer. The default values are as follows: • 0: Clear (GREEN) • 1: Indeterminate (PURPLE) • 2: Warning (BLUE) • 3: Minor (YELLOW) • 4: Major (ORANGE) • 5: Critical (RED)	Severity
StateChange	time	A timestamp indicating when the event was last modified. This field can be used to determine whether a process is modifying an event after it has been added to the ObjectServer.	
Summary	varchar(255)	A textual description of the event.	Description

Table 17. alerts.status fields used by Network Manager (continued)

alerts.status field	Data type	Description	Network Manager field name/Default value in rules file
Tally	integer	A count of the number of times that an event has occurred. This value is displayed in the Count column in the event list or AEL, and in the Occurred column in the mojo.events table.	
Type	integer	The type of the alert. The values of particular relevance to Network Manager are • 1: Problem • 2: Resolution • 13: Information	ExtraInfo_EVENTTYPE

For more information about the alerts.status table, see the *IBM Tivoli Netcool/OMNIbus Administration Guide* in the Tivoli Netcool/OMNIbus information centre at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Related reference:

"Network Manager network events" on page 162
The Polling engine, **ncp_poller**, generates events about the state of the network. These events can be used to identify network problems, and are configurable by using the Network Polling GUI (go to **Administration** > **Network** > **Network Polling**). These events are known as network events and have the alerts.status AlertGroup field value of `ITNM Monitor`.

"Network Manager status events" on page 163
Network Manager can generate events that show the status of various Network Manager processes. These events are known as Network Manager status events and have the alerts.status AlertGroup field value of `ITNM Status`.

Tivoli Netcool/OMNIbus automations added by Network Manager:

Network Manager provides a number of Tivoli Netcool/OMNIbus automations. Each automation performs different tasks within the Network Manager installation.

To enable an automation, use the Tivoli Netcool/OMNIbus Administrator GUI.

The following table describes the Tivoli Netcool/OMNIbus automations installed by Network Manager.

Table 18. Tivoli Netcool/OMNIbus automations added by Network Manager

Automation	Description	Added during installation?	Default status
severity_from_ causetype	Sets the severity of events in the ObjectServer alerts.status table based on the value of NmosCauseType, an enumerated field that contains the results of the Network Manager root cause analysis (RCA) calculations. Possible values for the NmosCauseType field are: • 0 - Unknown • 1 - Root Cause • 2 - Symptom	Yes	Enabled
suppress_cross_ domain_connections	Suppresses events from connected devices where the connected device is in a different domain. This automation is triggered whenever an event is updated by the Event Gateway. **Restriction:** Network Manager only models connections across network domains in MPLS networks between provider-edge and customer edge devices and in BGP networks between BGP peers. In order for the automation to work, the two network devices must be connected at layer 3 on a /30 subnet, that is, a subnet with only two hosts. Each device must also be discovered in a different network domain and the existence of its companion device must have been inferred during discovery. This means that in each domain an inferred customer-edge device or an inferred BGP peer entity must have been created.	Yes	Disabled
update_service_ affecting_events	Generates service-affected events (SAEs) when it encounters network events on service-supporting entities. Following each discovery the SAE plugins to the Event Gateway analyse the updated topology and update the ObjectServer with the a list of entities that support services. This information enables the automation to generate service-affected events when it encounters network events on service-supporting entities.	No	Not applicable

Configuring integration with Netcool Configuration Manager

To add network configuration and policy management capabilities to your network management solution, set up Network Manager and Tivoli Netcool/OMNIbus to work with IBM Tivoli Netcool Configuration Manager.

You can configure integration between Network Manager, Tivoli Netcool/OMNIbus, and Netcool Configuration Manager. For more information, go to http://www-01.ibm.com/support/knowledgecenter/SS7UH9/welcome, select your Netcool Configuration Manager version, and see the *Integrating Netcool Configuration Manager with Network Manager and Tivoli Netcool/OMNIbus* topics. Alternatively, you can download the PDF version, titled *IBM Tivoli Netcool Configuration Manager Integration Guide*.

Exporting discovery data to CCMDB, TADDM, and TBSM

Configure and use the Discovery Library Adapter (DLA) to collect data on network resources and relationships from Network Manager for import into other systems.

The DLA collects data from Network Manager and creates XML Discovery Library books (also known as Identity Markup Language, or IdML books) that contain data on the discovered resources and their relationships known to the system. The books conform to the Tivoli Common Data Model (CDM) version 2.10.10. For more information on the Tivoli CDM, go to http://www.redbooks.ibm.com/abstracts/redp4389.html.

The Discovery Library books can be imported into other systems for which a Discovery Library Reader exists. The DLA supports both IPv4 and IPv6.

The DLA is installed by default with Network Manager on the GUI server. It is installed into the following directory: `$NCHOME/precision/adapters/ncp_dla`.

Prerequisites for use

Before you configure and use the Discovery Library Adapter (DLA), make sure the prerequisites are met.

- A successful Network Manager network discovery has been performed and the Network Connectivity and Inventory Model (NCIM) database has been populated.
- The DLA uses the GUI server connection pool by default. If you want to use a different NCIM database than the one provided during installation, then you must have the access credentials for that NCIM database.
- You must have a working knowledge of how the product you want to integrate with is deployed.
  - For more information about IBM Tivoli Application Dependency Discovery Manager, see the Information Center at the following Web address:

    http://www-01.ibm.com/support/knowledgecenter/SSPLFC_7.2.0/welcome_page/kc_welcome-444.html
  - For more information about IBM Tivoli Business Service Manager, see the Information Center at the following Web address:

    http://www-01.ibm.com/support/knowledgecenter/SS3HLM_7.1.1.16/com.ibm.tivoli.tpm.osd.doc_7.1.1.16/welcome/osdlanding.html
  - For more information about IBM Tivoli Change and Configuration Management Database, see the Information Center at the following Web address:

http://www-01.ibm.com/support/knowledgecenter/SSBH2C_7.2.2/com.ibm.isdm_7.2.2.doc/isdm_homepage.html

Configuring the DLA

The Discovery Library Adapter (DLA) requires a configuration properties file in order to determine the data source to connect to, the domain to query, the target directory for Discovery Library books and logging parameters.

You need to configure the DLA properties if you have a separate GUI server or if you want to use the DLA with a different NCIM instance than the default provided during installation.

A preconfigured `ncp_dla.properties` configuration file is provided in the DLA installation directory at `$NCHOME/precision/adapters/ncp_dla`. The presence of 'XXXXXX' or <'word'> in the configuration file indicates that the parameter should be specified by the user. The configuration file provides useful defaults for most options but make sure to replace them with values appropriate for your environment.

Windows Specify directories on Windows systems by using two path delimiters, for example `C:\\temp`.

Note: By default, the NCIM access parameters required to use the DLA are derived from the Network Manager GUI access pool. This setting is specified by the **`ncp.dla.datasource.autoConnect`** parameter, where the default value is "true". If you change this value to "false," you must specify values for the parameters listed in step 6 on page 183. Setting how to connect to the NCIM database manually is useful when the connection pool cannot be accessed or if you want to use a different NCIM instance than the default provided during installation.

1. Go to `$NCHOME/precision/adapters/ncp_dla` and copy the `ncp_dla.properties` file to a domain-specific version by appending the name of the file with the domain name, for example, `ncp_dla.properties.NCOMS`.
2. Specify the Network Manager domain name by assigning a value to the **`ncp.dla.precisionDomain`** property. The default domain name is "NCOMS."
3. Optional: You can set the path to a temporary directory the DLA should use while generating the output if you do not want it to use the operating system's default temporary directory. Use the **`ncp.dla.scratchDirectory`** parameter to set the full path to a writable temporary directory, for example **`ncp.dla.scratchDirectory=/opt/space/temp`**.
4. Optional: You can set what CDM objects you want to have data generated for. Use the **`ncp.dla.generationFilter`** parameter to specify the values in a comma-separated list. The possible values are as follows:
   - `ComputerSystem` - generates the following data for devices:
     - ComputerSystem
     - SnmpSystemGroup
     - OperatingSystem
     - IpInterface for IpDevice, devices with no SNMP access
     - Router
     - Bridge
   - Networking - generates the following data for networks:
     - L2Interface
     - IpInterface

- IpV4Address
- IpV6Address
- IpNetwork

- Physical - generates the following data for physical classes:
  - PowerSupply
  - Fan
  - Chassis
  - Sensor
  - PhysicalPackage
  - Card
  - Fix Pack 5 Daughter Card

For example, to generate system and network connectivity-related data, add the following values to the parameter:

```
ncp_dla.generationFilter=ComputerSystem,Networking
```

5. Optional: You can define the URL to use for the contextual launching into other systems. Set the **ncp.dla.contextualLaunchURL** parameter to the topology value you want to launch into, and specify the host name and port for the Topoviz topology server. The default is to launch into the Hop View. For example, to set up the contextual launch into the Structure Browser:

   ```
   ncp.dla.contextualLaunchURL=https://hostname:16316/ibm/console/
   ncp_structureview/Launch.do?entityId=
   ```

6. Optional: If you change the value of the **ncp.dla.datasource.autoConnect** to "false," specify the RDBMS access details by editing the following parameters that define the database that the DLA connects to for generating Discovery Library books:

   ncp.dla.datasource.type
   Specify the RDBMS type, the default is DB2:
   - DB2 `DB2`
   - MySQL `MySQL`
   - Oracle `Oracle`
   - IDS `Informix`

   ncp.dla.datasource.driver
   Specify the JDBC driver to use:
   - DB2 `com.ibm.db2.jcc.DB2Driver`
   - MySQL `com.mysql.jdbc.Driver`
   - Oracle `oracle.jdbc.driver.OracleDriver`
   - IDS `com.informix.jdbc.IfxDriver`

   ncp.dla.datasource.url
   Specify the JDBC URL for connecting to the NCIM database:
   - DB2 `jdbc:db2://host_name:port_number/database_name`
   - MySQL `jdbc:mysql://host_name:port_number/database_name`
   - Oracle `jdbc:oracle:thin:@host_name:port_number/database_name` where *database_name*is the Oracle System Identifier (SID) that refers to the Oracle database instance running on the server.

- IDS `jdbc:informix-sqli://host_name:port_number/database_name`

ncp.dla.datasource.schema
The database schema name, typically “ncim”

ncp.dla.datasource.username
The database username, typically “ncim”

ncp.dla.datasource.password
The database user password

ncp.dla.datasource.encrypted
Whether the database password is encrypted [true|false]

If set to true, you must specify a valid value for `ncp.dla.datasource.keyFile`, and you must use the encrypted password referenced in your `ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties` file.

ncp.dla.datasource.keyFile
Specify the full path and name of the cryptographic key file that is used in the `ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties` file.

ncp.dla.datasource.loginTimeout
The login timeout, default 5 seconds

7. Optional: You can limit the scope of data collection to one or more network views by setting the **`ncp.dla.network.view`** parameter to filter the data of selected network views only. Using standard SQL operators, define an SQL segment that is appended to the **`networkView.name`** field during the DLA query. The parameter must have a value starting with one of the following SQL operators:
   - =
   - <>
   - !=
   - IN
   - NOT IN
   - LIKE
   - NOT LIKE

   For example, the following defines the scope to use only the `BGP Networks` network view for the scope of the data collection:

   ```
   ncp.dla.network.view=='BGP Networks'
   ```

   Note: The DLA does not support double quotation marks. Everything after the initial equal sign in the previous example is part of the value defined, even the second equal (=) sign.

   Another example is the following where the scope for the data collection is defined as any network view containing the name `Cisco` (notice the standard SQL wildcard character % used):

   ```
   ncp.dla.network.view=LIKE 'Cisco%'
   ```

8. Specify how the Discovery Library books generated by the DLA should be transferred by specifying the following parameter:

   ncp.dla.datasink.type
   How Discovery Library books are transferred. Options are as follows:

FILE The Discovery Library books are locally copied to the target directory `/opt/IBM/tivoli/netcool/var/precision/ccmdb`. If you specify this option, skip step 9 and proceed to step 10.

FTP The Discovery Library books are transferred to a remote server by FTP. If you specify this option, you must complete step 9

ncp.dla.datasink.targetDirectory
The target directory for Discovery Library book files

Note: If you are running the DLA on a server other than the GUI server and want to place the generated books that server, you can specify the connection parameters in the `ncp_dla.properties` file by uncommenting and editing the parameters around **`ncp.dla.datasink.targetDirectory`**.

9. Optional: If you specified the option `FTP` for the **`ncp.dla.datasink.type`** property, specify the following additional parameters:

   ncp.dla.datasink.server
   The IP address or hostname of the remote FTP server.

   ncp.dla.datasink.port
   The TCP port to use, default 21

   ncp.dla.datasink.binary
   Whether binary FTP transfers should be used [true|false]

   ncp.dla.datasink.passive
   Whether passive FTP transfers should be made [true|false]

   ncp.dla.datasink.username
   The FTP username to use

   ncp.dla.datasink.password
   The FTP user password to use

   ncp.dla.datasink.encrypted
   Whether or not the FTP password is encrypted [true|false]

   ncp.dla.datasink.keyFile
   Specify the full path and name of the cryptographic key file that is used in the `$ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties` file.

10. Specify the debug level of the DLA by specifying a value for the **`log4j.rootLogger`** property. The following values are permitted; the default value is `FATAL`:
    - `DEBUG`
    - `INFO`
    - `WARN`
    - `ERROR`
    - `FATAL`
11. Specify the full path and name of the DLA log file by specifying a value for the **`log4j.appender.FILE.file`** property. The default is `dla.log`. The log file is written to the DLA installation directory.
12. Optional: The deprecated **`ncp.dla.validateComputerSystemFqdn`** property defines whether to validate the names of entities discovered by Network Manager as fully-qualified domain-names.

CAUTION:
Do not change value. This property has been deprecated and is no longer used in Network Manager versions 3.9 and later.
This property can take one of the following values:

True This is the default value. Entity names are validated. The DLA adds Fqdn attributes to ComputerSystem instances only if the device name is a valid fully-qualified domain-name.

False No validation takes place. The DLA adds Fqdn attributes to ComputerSystem instances irrespective of whether the device name is a valid fully-qualified domain-name.

13. Create a copy of the edited configuration file, giving the file a name of your choice.
14. Create a copy of the configuration for each Network Manager domain for which you want to create Discovery Library books.

    Remember: Create a configuration file for each Network Manager domain you want to generate Discovery Library books for, and append the name of the configuration file with the domain name (for example, `ncp_dla.properties.NCOMS`).

If you want to start the IBM Tivoli Application Dependency Discovery Manager GUIs from the Network Manager, complete the additional configuration tasks to add a menu option to the Network Manager GUIs, and add the Network Manager JSP inventory report to TADDM.

Related reference:

"Network Manager status events" on page 163
Network Manager can generate events that show the status of various Network Manager processes. These events are known as Network Manager status events and have the alerts.status AlertGroup field value of `ITNM Status`.

Creating a Discovery Library book

To create a Discovery Library book, run the Discovery Library Adapter (DLA) with the appropriate DLA properties file.

Before you can run the DLA, the DLA properties file must have been configured correctly

The DLA has two modes of operation:

Primary mode
Generates Discovery Library books by querying the Network Connectivity and Inventory Model (NCIM) database for the domain identified in the specified configuration file.

Import mode
Provides a means of importing IBM Tivoli Application Dependency Discovery Manager GUIDs back into the NCIM database, so that the TADDM UI can be opened from Network Manager.

1. Change to the DLA installation directory on the Network Manager GUI components server; the default is `$NCHOME/precision/adapters/ncp_dla`.
2. Run the Discovery Library Adapter (DLA) and reference the appropriate DLA properties file for your domain to create a Discovery Library book:
   - UNIX `./ncp_dla.sh ncp_dla.properties.`*`domain_name`*
   - Windows `ncp_dla.bat ncp_dla.properties.`*`domain_name`*

See “Example” for an example of running the command and the system response.

Example

The following example shows how to run the DLA, and the system response:

```
[root@sacramento test]# ./ncp_dla.sh ncp_dla.properties.NCOMS
ncp_DLA ( IBM Tivoli Network Manager IP Edition - Discovery Library Adapter )
Copyright (C) 1997 - 2011 By IBM Corporation.  All Rights Reserved.
See product license for details.

[IDML Generation Mode]
Initializing...
WARNING: user.install.root not defined, using /opt/IBM/tivoli/netcool
/precision/profiles/TIPProfile
Loading properties from /opt/IBM/tivoli/netcool/precision/profiles
/TIPProfile/etc/tnm/tnm.properties
ConnectionPool 'READ' Initialised
JDBC Driver: com.mysql.jdbc.Driver
JDBC URL   : jdbc:mysql://sacramento:3306/ncim?characterEncoding=UTF-8
Working on domain 'NCOMS'...
Processing 161 valid device(s)
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Writing IDML Book to
'/opt/dla/test/ITNMIP.sacramento.beach.tcr.com.2008-09-12T0192.168.34.909Z.
refresh.xml'
... Shutting down...
Finished.
```

Related tasks:

“Loading Discovery Library books and enabling bidirectional launch” on page 193
You need to load the Discovery Library (IdML) book into TADDM to make the book information available to TADDM. Importing the book also enables bidirectional contextual launch.

Fine-tuning the data export

To provide a more consumable set of resources and relationships to other systems from Network Manager, you can fine-tune the DLA data collection and export. Fine-tuning of the Network Manager data export allows TADDM and other Discovery Library (IdML) book consumers to import only the resources and relationships needed to build the appropriate linkage between commonly managed resources. Also, having only the required data can significantly expedite the export-import process.

To set up a more fine-tuned data collection and export, perform the following steps:

1. Discover the network using Network Manager, as described in Discovering the network.
2. Run the **itnmTagNetworkEdgeEntities.pl** tagging utility to identify network edge entities, as described in “Identifying network edge entities” on page 188.
3. Create a filtered network view that only displays the edge of the network, as described in “Creating a filtered network view for the edge of the network” on page 189.
4. Edit the DLA properties file `ncp_dla.properties.`*`domain_name`* to include the name of the filtered network view you created, and to ensure you have set the **ncp.dla.generationFilter** parameter as described in “Editing the DLA properties file for edge entities” on page 190.
5. Run the adaptor to create the Discovery Library book, as described in “Creating a Discovery Library book for network edge data” on page 191.

Identifying network edge entities:

Use the **itnmTagNetworkEdgeEntities.pl** utility to tag discovered entities such as ports and interfaces as being on the edge of the network. For most cases, you can run the utility to automatically tag entities considered to be on the network edge, which then identifies end-nodes such as hosts and servers that provide or consume services.

Ensure Network Manager has successfully discovered your network. End-nodes must be discovered before you can use the `-autoEndNodeTags` option with the **itnmTagNetworkEdgeEntities.pl** utility.

To run the utility to automatically tag the entities considered as being on the edge of the network in a domain:

1. Go to `NHCOME/precision/scripts/perl/scripts`.
2. Run **itnmTagNetworkEdgeEntities.pl** with the `-autoEndNodeTags` command-line option for the domain in which you want entities to be tagged. This automatically includes end-nodes and the routers and switches directly connected to end-nodes. For example, to automatically tag interfaces considered to be on the edge of the network in the domain called NCOMS, enter:
   - UNIX `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags`
   - Windows `%NCHOME%\precision\bin\ncp_perl.bat itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags`
3. Optional: You can use the `-includeNextHop` option with the `-autoEndNodeTags` option to go one hop further from the edge entities. Using the `-includeNextHop` option automatically includes the edge entities that are included when using only the `-autoEndNodeTags`, plus any routers or switches directly connected to the edge entities. For example, to automatically tag such interfaces, enter:
   - UNIX `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags -includeNextHop`
   - Windows `%NCHOME%\precision\bin\ncp_perl.bat itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags -includeNextHop`
4. Optional: You can also determine what devices you want the utility to consider as a network edge device based on the number of connections the device has. Use the `-autoDegreeTags` option to tag devices as being on the network edge if they have a certain number of connections. If you only use the `-autoDegreeTags` option on its own, the default is to consider all devices with one connection as being on the network edge.

   If you want to specify a larger connection number, use the `-autoDegreeTags` option and the `-degree` *n* option together, where *n* is the maximum number of connections. For example, running the following setting tags all devices with less than or equal to 2 connections:
   - UNIX `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoDegreeTags -degree 2`
   - Windows `%NCHOME%\precision\bin\ncp_perl.bat itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoDegreeTags -degree 2`

   Note: The `-autoDegreeTags` option cannot be used in conjunction with the `-autoEndNodeTags` option. The `-autoDegreeTags` option mode allows you to include devices as part of the edge of the network that are not considered

end-node devices by the `-autoEndNodeTags` option. It also provides the flexibility to filter out and identify devices that have up to a specific number of connections.

5. Optional: You can further refine the tagging by setting a number of options, such as excluding or including specific devices from being tagged or including devices that have no SNMP access but have Layer 2 connections. For further information on all the options available, view the utility help by typing:
   - UNIX `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -help`
   - Windows `%NCHOME%\precision\bin\ncp_perl.bat itnmTagNetworkEdgeEntities.pl -help`

The utility adds an ExtraInfo->m_NetworkEdge=1 attribute in the OQL master.entityByName database and registers an associated entityDetails record in the NCIM database.

Now, you can create a filtered network view that only displays the edge of your network.

Creating a filtered network view for the edge of the network:

Create a filtered network view that only displays the edge of the network in the domain based on the tagging performed by the **`itnmTagNetworkEdgeEntities.pl`** utility.

Tip: You can also use this filtered network view to visualize and monitor the edge of your network, and to see what data is exported using the DLA.

To create a filtered view of the edge of your network:

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View**  .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `Filtered`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse**  to browse for an icon.

Tree Icon
If you want a different icon than the default cloud icon to represent the view, click **Browse**  to browse for an icon.

Background Image
Click **Browse**  to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Set up the filter as follows:
   a. Click the **Filter** tab.
   b. From the **Domain** list, select the domain where you ran the tagging utility.
   c. In the **Table** column, select the entityDetails attribute
   d. In the **Filter** column, type `keyName = 'NetworkEdge' and keyValue = '1'`.
4. Set **End Nodes** to `Include`
5. Set **Connectivity** to `Layer 2`.
6. Click **Ok** and then **Save**.

You now need to include the name of this network view in the DLA properties file for the domain.

Editing the DLA properties file for edge entities:

Edit the `ncp_dla.properties` file for the domain to include the name of the filtered network view you created and to make sure you have set up the right data generation parameters.

To edit the file:

1. Go to the default `ncp_dla.properties` configuration file in the DLA installation directory at `$NCHOME/precision/adapters/ncp_dla`, or to where your DLA properties file for the domain is.
2. Open the `ncp_dla.properties.`*`domain_name`* file.
3. Locate the **`ncp.dla.network.view`** parameter and add the name of the filtered network view you created. For example, the filtered view called “Edge” would need to be added to this property as follows: `ncp.dla.network.view=='Edge'`

   Note: The use of the double equality sign (`==`) as relational operator is intentional.
4. Set the **`ncp.dla.generationFilter`** parameter to `ComputerSystem` and `Networking`. Specify the values in a comma-separated list as follows:

   ```
   ncp_dla.generationFilter=ComputerSystem,Networking
   ```

5. Save and close the file.

Now, you can run the DLA with the updated DLA properties file to export a subset of the Network Manager network data.

Related tasks:

"Configuring the DLA" on page 182
The Discovery Library Adapter (DLA) requires a configuration properties file in order to determine the data source to connect to, the domain to query, the target directory for Discovery Library books and logging parameters.

Creating a Discovery Library book for network edge data:

You can use the Discovery Library Adapter (DLA) to create the Discovery Library book containing only the data for your network edge entities.

Make sure you have edited the `ncp_dla.properties` file for the domain to include the name of the filtered network view containing the network edge entities.

To create a DLA book containing network edge data:

1. Change to the DLA installation directory on the Network Manager GUI components server; the default is `$NCHOME/precision/adapters/ncp_dla`.
2. Run the Discovery Library Adapter (DLA) to generate the book XML file with data on the tagged network edge entities:
   - UNIX `./ncp_dla.sh ncp_dla.properties.`*`domain_name`*
   - Windows `ncp_dla.bat ncp_dla.properties.`*`domain_name`*

   For example, to run the adaptor for the domain called NCOMS, enter the following: `./ncp_dla.sh ncp_dla.properties.NCOMS`

The following example shows the system response for running the adaptor for the NCOMS domain:

```
ncp_DLA ( IBM Tivoli Network Manager IP Edition - Discovery Library Adapter )
Copyright (C) 1997 - 2011 By IBM Corporation.  All Rights Reserved.  See product
license for details.

[IDML Generation Mode]
Initializing...
Will use the following Network View(s) filter : ='FILTER'
Working on ITNM domain 'NCOMS'...
Processing 1148 IP Network(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Processing 772 ComputerSystem(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Processing 1 Topology(s)...
Processing 2535 Connection(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Writing IDML Book to '/opt/netcool/itnm39017/netcool/var/precision/ccmdb
/ITNMIP39.9.180.209.195.2010-10-05T13.33.37.314Z.refresh.xml'...
Shutting down...
Finished.
```

The result is an XML file that contains the devices participating in the filtered network view previously created and specified in the `ncp_dla.properties` file for the domain. The content of the XML file depends on the configuration of the DLA properties file.

The XML file contains Common Data Model (CDM) Segments that describe how devices are connected from the perspective of a given Network Manager port or interface. The process removes duplicates and normalizes connection details. For more information on Segments, please refer to the Tivoli Common Data Model (CDM) documentation available at http://www.redbooks.ibm.com/abstracts/redp4389.html.

The following examples show parts of the XML file output. The interface chosen to be the segment identity is highlighted in bold, including each instance it is referenced.

- Example of a point-to-multipoint connection from the perspective of the interface chosen to be the starting point for a segment:

```
<cdm:net.Segment id="SegmentVia_359525_L2Interface" >
                <cdm:Name>Layer 2 Segment via 359525_L2Interface</cdm:Name>
                <cdm:ManagedSystemName>itnmSgmnt:359525_L2Interface
</cdm:ManagedSystemName>
 </cdm:net.Segment>
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="359525_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358156_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="404607_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358221_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358185_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="404595_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358107_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="357775_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358232_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="404589_L2Interface" />
            <cdm:networks source="SegmentVia_359525_L2Interface"
target="358300_L2Interface" />
```

- Example of a simple point-to-point connection:

```
<cdm:net.Segment id="SegmentVia_355664_L2Interface" >
                <cdm:Name>Layer 2 Segment via 355664_L2Interface</cdm:Name>
                <cdm:ManagedSystemName>itnmSgmnt:355664_L2Interface
</cdm:ManagedSystemName>
</cdm:net.Segment>
            <cdm:networks source="SegmentVia_355664_L2Interface"
target="355664_L2Interface" />
            <cdm:networks source="SegmentVia_355664_L2Interface"
target="357336_L2Interface" />
```

Loading Discovery Library books and enabling bidirectional launch

You need to load the Discovery Library (IdML) book into TADDM to make the book information available to TADDM. Importing the book also enables bidirectional contextual launch.

As well as being able to launch the IBM Tivoli Application Dependency Discovery Manager GUI from Network Manager, you can also configure TADDM to launch the Network Manager GUI.

To load Discovery Library books into TADDM and set up bidirectional contextual launch:

1. Create a Discovery Library book.
2. If required, transfer the Discovery Library book file to your TADDM server.
3. As the TADDM user, run the bulk load process to import the Discovery Library book. For example:

   ```
   user@host% cd $COLLATION_HOME/bin
   user@host% ./loadidml.sh -f full path to and full name of discovery library
   book file
   ```

   Attention: You must include the full path to the discovery library book file, together with the full file name only if the book is in a different directory.
4. Import the TADDM GUIDs into the NCIM database (see related tasks later in this section).

Related tasks:

"Creating a Discovery Library book" on page 186
To create a Discovery Library book, run the Discovery Library Adapter (DLA) with the appropriate DLA properties file.

"Importing IBM Tivoli Application Dependency Discovery Manager GUIDs into the NCIM database" on page 196
Optional: To enable users to open the IBM Tivoli Application Dependency Discovery Manager UI from Network Manager, import the TADDM GUIDs into the entityGUIDCache table of the Network Connectivity and Inventory Model (NCIM) database.

Configuring IBM Tivoli Application Dependency Discovery Manager to start Network Manager

Optional: To view a summary of the resources that Network Manager exports to IBM Tivoli Application Dependency Discovery Manager and, from there, open Network Manager, you must add a JSP report.

Important: If you are using an earlier version of TADDM than 7.2.1 Fix Pack 1, follow these instructions to install and configure the JSP report. However, if you are using version 7.2.1 Fix Pack 1 or later, ignore these steps. In version 7.2.1 Fix Pack 1 and later the report to show Network Manager inventory and provide the launch in context to Network Manager is installed (or updated if already exists) by the TADDM installation. For more information, see the TADDM documentation at http://www-01.ibm.com/support/knowledgecenter/SSPLFC_7.2.1/com.ibm.taddm.doc_721/welcome_page/kc_welcome-444.html.

The JSP report is provided; to use the report, the files must be copied to the correct location on your TADDM server.

1. Log in to the TADDM server.
2. Ensure the $COLLATION_HOME environment variable is set appropriately.

3. Copy the *dla_install_directory*/integration/itnm_inventory.jsp file from the Network Manager GUI components server to the $COLLATION_HOME/deploy-tomcat/reports/WEB-INF/view directory on the TADDM server.
4. Copy the two GIF files (tivoli.gif and ibm_logo.gif) in *dla_install_directory*/integration/itnm_images directory from the Network Manager GUI components server to the $COLLATION_HOME/deploy-tomcat/images directory on the TADDM server.
5. Stop your TADDM server.
6. Edit the $COLLATION_HOME/etc/cdm/xml/reports.xml file by adding the following section before the closing </beans> tag:

```
<bean class="com.collation.cdm.reports.viewer.JspReportViewer"
id="ITNMInventoryReport">

<property name="reportGroup">
  <value>Inventory Reports
</value>
 </property>

<property name="reportName">
  <value>ITNM IP Inventory Report
</value>
 </property>
 <!-- START NON-TRANSLATABLE -->
 <property name="jsp">
  <value>/WEB-INF/view/itnm_inventory.jsp</value>
 </property>
 <!-- END NON-TRANSLATABLE -->
</bean>
```

7. Restart your TADDM server.

The Network Manager Inventory Report is displayed in the TADDM Domain Manager console. The report has the following sections:

- Server Summary: Provides information about the installed instances of the Network Manager product, including the Network Manager versions installed, the host addresses of the servers where Network Manager is installed, and the URLs to access the Network Manager GUI.
- Resource Summary: Lists all Network Manager resources that have a relationship to a ComputerSystem, including information on their IP address, manufacturer, type of resource (for example, router), and unique identifier in the Network Manager database.

Configuring Network Manager to start IBM Tivoli Application Dependency Discovery Manager

Optional: To enable Network Operators to launch the IBM Tivoli Application Dependency Discovery Manager GUI from Network Manager, you must add the TADDM menu options to Network Manager.

The following steps assume that the Discovery Library Adapter (DLA) is installed on the same server as Tivoli Integrated Portal and the Network Manager GUI components. If the DLA is installed elsewhere, you must copy the DLA installation directory and its content to the server where the Tivoli Integrated Portal and the Network Manager GUI components are installed.

For more information about the relationship between IBM Tivoli Application Dependency Discovery Manager and IBM Tivoli Change and Configuration Management Database, see the Information Center at the following Web address

and search for "CCMDB overview": http://www-01.ibm.com/support/knowledgecenter/SSBH2C_7.2.2/com.ibm.isdm_7.2.2.doc/isdm_homepage.html

1. Configure the launch points from the menu to the TADDM installation:
   a. Change to the `ITNMHOME/profiles/TIPProfile/etc/tnm/tools/` directory.
   b. Edit the following files:
      - `ncp_wt_ccmdb_details.xml`
      - `ncp_wt_ccmdb_history.xml`
   c. Specify the following parameters:

      TADDM_HOST
      The IP address or host name of your TADDM server.

      TADDM_PORT
      The TCP port on which your TADDM server is listening. The default is 9430, and this value only needs to be changed if a different port number was provided when installing TADDM.

      TADDM_USER
      The user name to use to access your TADDM server.

      TADDM_PASSWORD
      The password associated with the **`TADDM_USER`** parameter.
   d. Optional: To configure TADDM to start in the same window as Network Manager, edit the `target` field of the `url` property in each tool definition file. By default, TADDM starts in a new window. For example, to display the CCMDB details in the same window, edit the property in the `ncp_wt_ccmdb_details.xml` file as follows:

      ```
      target="ccmdbDetails'"
      ```
2. Verify that the TADDM submenu was added to Network Manager:
   a. Log into Network Manager.
   b. Click **Network Availability** > **Network Views**
   c. Select a network view and right-click a device.

   In the context menu, the following TADDM menu items should be displayed under **Launch To...** > **TADDM/CCDMB**:

   View Details

   View History

   Note: It can take several minutes for the changes to take effect. If changes have not taken effect after 5 minutes, log off, restart your browser, and log in again.

You now need to import the TADDM GUIDs into the NCIM database.

Related tasks:

"Importing IBM Tivoli Application Dependency Discovery Manager GUIDs into the NCIM database" on page 196

Optional: To enable users to open the IBM Tivoli Application Dependency Discovery Manager UI from Network Manager, import the TADDM GUIDs into the entityGUIDCache table of the Network Connectivity and Inventory Model (NCIM) database.

Importing IBM Tivoli Application Dependency Discovery Manager GUIDs into the NCIM database

Optional: To enable users to open the IBM Tivoli Application Dependency Discovery Manager UI from Network Manager, import the TADDM GUIDs into the entityGUIDCache table of the Network Connectivity and Inventory Model (NCIM) database.

1. Run the DLA so that the Network Manager resources and relationships are imported into TADDM.
2. Log in to the server where your Network Manager GUI components are installed, and copy the DLA integration directory and content in `ITNMHOME/adapters/ncp_dla/integration` to your TADDM server (for example, `$COLLATION_HOME/sdk/dla/integration`). Ensure that permissions are set so that the TADDM user can access the files.
3. On the TADDM server, change to the directory where you copied the files to.
4. As the TADDM user, use the TADDM API to query the CCMDB for ComputerSystem data and pipe the results to an XML file called `itnm_guids.xml`. For example:

   ```
   user@host% $COLLATION_HOME/sdk/bin/api.sh -u user_name -p password find
   ComputerSystem > itnm_guids.xml
   ```

5. Make sure the `itnm_guids.xsl` and the `itnm_guids.xml` files exist in the current directory.
6. As the TADDM user, use the XLST processor to extract the entityId's and GUIDs, and pipe them to a CSV file called `itnm_guids.csv`. For example:

   ```
   user@host% $COLLATION_HOME/sdk/bin/xslt.sh -XSL ./itnm_guids.xsl >
   itnm_guids.csv
   ```

7. Copy the `itnm_guids.csv` file back to the Network Manager GUI server into the home directory or the `ITNMHOME/adapters/ncp_dla` directory.
8. Run the DLA in import mode to import the CSVs into the Network Manager NCIM database. See "Example" for an example of how to run in import mode, and the system response.

Example

The following example shows how to run the DLA in import mode, and how the system responds.

```
user@host% cd /opt/IBM/DiscoveryLibrary/ITNM
user@host% [./ncp_dla.sh | ncp_dla.bat ] -import
-file integration/itnm_guids.csv ncp_dla.properties.MYSQL
ncp_DLA ( IBM Tivoli Network Manager IP Edition - Discovery Library Adapter )
Copyright (C) 1997 - 2007 By IBM Corporation.  All Rights Reserved.
See product license for details.

[GUID Import Mode]
Initializing...
Importing GUIDs from 'integration/itnm_guids.csv'
Imported 15 GUID(s) into NCIM.
Shutting down...
Finished.
user@host%
```

Related tasks:

"Loading Discovery Library books and enabling bidirectional launch" on page 193
You need to load the Discovery Library (IdML) book into TADDM to make the book information available to TADDM. Importing the book also enables bidirectional contextual launch.

Integration with TBSM

Network Manager is integrated with IBM Tivoli Business Service Manager by default using the Probe for Tivoli Netcool/OMNIbus (nco_p_ncpmonitor). The probe provides IBM Tivoli Business Service Manager with BSM_Identity tokens for Network Manager.

You must have both IBM Tivoli Network Manager IP Edition and IBM Tivoli Business Service Manager installed and configured.

The BSM_Identity token is used by default by TBSM to associate events with resources. Using the Network Manager DLA, TBSM becomes aware of the Network Manager resources. Network Manager events will have the BSM_Identity field added based on the following setting in the `$NCHOME/probes/arch/nco_p_ncpmonitor.rules` file:

```
@BSM_Identity = "ITNMIP:" + $ExtraInfo_MONITOREDENTITYID + "&domain=" + $Domain
```

Related reference:

"Prerequisites for use" on page 181
Before you configure and use the Discovery Library Adapter (DLA), make sure the prerequisites are met.

Configuring the Tivoli Integrated Portal

After installation, you might need to configure Tivoli Integrated Portal security or single sign-on.

Configuring central user registries

As a post-installation task you can configure a central user registry for user management and authentication. You can configure an LDAP server or Tivoli Netcool/OMNIbus ObjectServer registry (or both).

Note: When you add a new user, you should check that the user ID you specify does not already exist in any of the user repositories to avoid difficulties when the new user attempts to log in.

In a network environment that includes a user registry on an LDAP server or Tivoli Netcool/OMNIbus ObjectServer, you can configure Network Manager to use either or both types.

Before configuring a central user registry, be sure that the user registry or registries that you plan to identify are started and can be accessed from the computer where you have installed the Network Manager.

Attention: When Network Manager is configured with multiple central user repositories, you cannot login if one remote user repository becomes inaccessible from Network Manager, even if your user ID exists in one of the other repositories. If you need access is this situation, you have to run WebSphere Application Server commands to allow access when all repositories are available, or the federated repositories will not function properly. For more information, refer to the following links:

- http://www-01.ibm.com/support/docview.wss?uid=swg1PK78677
- http://www-01.ibm.com/support/knowledgecenter/SSAW57_7.0.0/com.ibm.websphere.web20fep.multiplatform.doc/info/ae/ae/rxml_atidmgrrealmconfig.html

Adding an external LDAP repository:

After installation, you can add an IBM Tivoli Directory Server or Active Directory Microsoft Active Directory Server as an LDAP repository for Network Manager.

To add a new LDAP repository:

1. Log in to the Network Manager.
2. In the navigation pane, click **Settings** > **Websphere Admin Console** and click **Launch Websphere Admin Console**.
3. In the WebSphere Application Server administrative console, select **Settings** > **Global security**.
4. From the **Available realm definitions** list, select **Federated repositories** and click **Configure**.
5. In the Related Items area, click the **Manage repositories** link and then click **Add** to add a new LDAP repository.
6. In the **Repository identifier** field, provide a unique identifier for the repository. The identifier uniquely identifies the repository within the cell, for example, `LDAP1`.
7. From the **Directory type** list, select the type of LDAP server. The type of LDAP server determines the default filters that are used by WebSphere Application Server.

   Note: IBM Tivoli Directory Server users can choose either IBM Tivoli Directory Server or SecureWay as the directory type. For better performance, use the IBM Tivoli Directory Server directory type.
8. In the **Primary host name** field, enter the fully qualified host name of the primary LDAP server. The primary host name and the distinguished name must contain no spaces. You can enter either the IP address or the domain name system (DNS) name.
9. In the **Port** field, enter the server port of the LDAP directory.

   The host name and the port number represent the realm for this LDAP server in a mixed version nodes cell. If servers in different cells are communicating with each other using Lightweight Third Party Authentication (LTPA) tokens, these realms must match exactly in all the cells.

   Note:

   The default port value is `389`, which is not a Secure Sockets Layer (SSL) connection port. Use port `636` for a Secure Sockets Layer (SSL) connection. For some LDAP servers, you can specify a different port. If you do not know the port to use, contact your LDAP server administrator.
10. Optional: In the **Bind distinguished name** and **Bind password** fields, enter the bind distinguished name (DN) (for example, `cn=root`) and password.

    Note: The bind DN is required for write operations or to obtain user and group information if anonymous binds are not possible on the LDAP server. In most cases, a bind DN and bind password are needed, except when an anonymous bind can satisfy all of the required functions. Therefore, if the LDAP server is set up to use anonymous binds, leave these fields blank.
11. Optional: In the **Login properties** field, enter the property names used to log into the WebSphere Application Server. This field takes multiple login properties, delimited by a semicolon (`;`). For example, `cn`.

12. Optional: From the **Certificate mapping** list, select your preferred certificate map mode. You can use the X.590 certificates for user authentication when LDAP is selected as the repository.

    Note: The **Certificate mapping** field is used to indicate whether to map the X.509 certificates into an LDAP directory user by `EXACT_DN` or `CERTIFICATE_FILTER`. If you select `EXACT_DN`, the DN in the certificate must match the user entry in the LDAP server, including case and spaces.
13. Click **OK**.
14. In the Messages area at the top of the Global security page, click the **Save** link and log out of the WebSphere Application Server console.

Configure the Tivoli Integrated Portal Server to communicate with an external LDAP repository.

Configuring an external LDAP repository:

You can configure the Tivoli Integrated Portal Server to communicate with an external LDAP repository.

To configure an application server to communicate with an external LDAP repository:

1. Log in to the Network Manager.
2. In the navigation pane, click **Settings** > **Websphere Admin Console** and click **Launch Websphere Admin Console**.
3. In the WebSphere Application Server administrative console, select **Settings** > **Global security**.
4. From the **Available realm definitions** list, select **Federated repositories** and click **Configure**.
5. To add an entry to the base realm:
   a. Click **Add Base entry to Realm**.
   b. Enter the distinguished name (DN) of a base entry that uniquely identifies this set of entries in the realm. This base entry must uniquely identify the external repository in the realm.

      Note: If multiple repositories are included in the realm, use the DN field to define an additional distinguished name that uniquely identifies this set of entries within the realm. For example, repositories LDAP1 and LDAP2 might both use `o=ibm,c=us` as the base entry in the repository. So `o=ibm,c=us` is used for LDAP1 and `o=ibm2,c=us` for LDAP2. The specified DN in this field maps to the LDAP DN of the base entry within the repository (such as `o=ibm,c=us b`). The base entry indicates the starting point for searches in this LDAP directory server (such as `o=ibm,c=us c`).
   c. Click **OK**.
   d. In the Messages area at the top of the Global security page, click the **Save** link and log out of the WebSphere Application Server console.
6. In the WebSphere Application Server administrative console, select **Settings** > **Global security**.
7. From the **Available realm definitions** list, select **Federated repositories** and click **Set as current** to mark the federated repository as the current realm.
8. 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`

9. Verify that the federated repository is correctly configured:
   a. In the portal navigation pane, click **Users and Groups** > **Manage Users**.
   b. Select **User ID** from the **Search by** list.
   c. Click **Search** to search for users in the federated repository.
   d. Confirm that the list includes users from both the LDAP repository and the local file registry.

   On the Tivoli Integrated Portal Server, LDAP users are queried only by the `userid` attribute. When users are imported into LDAP using an LDAP Data Interchange Format (LDIF) file, an auxiliary class of type `eperson` and an `uid` attribute is added to the LDAP user ID. Note that this is to be done only if you want to search the LDAP repository using VMM from the server.

To be able to create or manage users in the portal that are defined in your LDAP repository, in the WebSphere Application Server administrative console, you must specify the supported entity types.

Managing LDAP users in the console:

To create or manage users in the portal that are defined in your LDAP repository, in the WebSphere Application Server administrative console specify the supported entity types.

To create or manage LDAP users in the portal:

1. Log in to the Network Manager.
2. In the navigation pane, click **Settings** > **Websphere Admin Console** and click **Launch Websphere Admin Console**.
3. In the WebSphere Application Server administrative console, select **Settings** > **Global security**.
4. From the **Available realm definitions** list, select **Federated repositories** and click **Configure**.
5. In the Additional Properties area, click **Supported entity types**.
6. In the Entity type column, click the **Group** link to display its properties page.
7. In the **Base entry for the default parent** field, provide a base entry relevant to your LDAP configuration, for example, `o=ibm,c=us`.
8. In the **Relative Distinguished Name properties** field, provide the same value that you did for the **Base entry for the default parent** field, for example, `o=ibm,c=us`.
9. Click **OK** to return to the Supported entity types page.

10. Edit the **OrgContainer** and the **PersonAccount** entities with the same values that you provided for the **Group** entity (for example, `o=ibm,c=us`).
11. In the Messages area at the top of the Global security page, click the **Save** link and log out of the WebSphere Application Server console.
12. For the changes to take effect, stop, and restart the Tivoli Integrated Portal Server.
13. 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`

You can now manage your LDAP repository users in the portal through the **Users and Groups** > **Manage Users** menu items.

Note: When you add a new user, you should check that the user ID you specify does not already exist in any of the user repositories to avoid difficulties when the new user attempts to log in.

Restriction: You cannot currently update user IDs through the **Users and Groups** > **Manage Users** portlet that have been created in Microsoft Active Directory repositories.

Configuring an SSL connection to an LDAP server:

If your implementation of Network Manager uses an external LDAP-based user repository, such as Microsoft Active Directory, you can configure it to communicate over a secure SSL channel.

This task assumes that you have already an existing connection to an LDAP server set up.

Your LDAP server (for example, an IBM Tivoli Directory Server Version 6 or an Microsoft Active Directory server), must be configured to accept SSL connections and be running on secured port number (636). Refer to your LDAP server documentation if you need to create a signer certificate, which as part of this task, must be imported from your LDAP server into the trust store of the Tivoli Integrated Portal Server.

Follow these instructions to configure the Tivoli Integrated Portal Server to communicate over a secure (SSL) channel with an external LDAP repository. All application server instances must be configured for the LDAP server.

1. Log in to the portal.
2. Follow these steps to import your LDAP server's signer certificate into the application server trust store.

a. In the navigation pane, click **Security** > **SSL certificate and key management**.
b. In the Related Items area, click the **Key stores and certificates** link and in the table click the **NodeDefaultTrustStore** link.
c. In the Additional Properties area, click the **Signer certificates** link and click the**Retrieve from port** button.
d. In the relevant fields, provide hostname, port (normally 636 for SSL connections), SSL configuration details, as well as the alias of the certificate for your LDAP server and click the **Retrieve signer information** button and then click **OK**.

3. Follow these steps to enable SSL communications to your LDAP server:
   a. In the navigation pane, click **Security** > **Secure administration, applications, and infrastructure**.
   b. Select **Federated repositories** from the **Available realm definitions** drop down list and click **Configure**.
   c. Select your LDAP server from the **Repository** drop down list.
   d. Enable the **Require SSL communications** check box and the select the **Centrally managed** option.
   e. Click **OK**.
4. For the changes to take effect, save, stop, and restart all Tivoli Integrated Portal Server instances.

If you intend to enable single sign-on (SSO) so that users can log in once and then traverse to other applications without having to re-authenticate, configure SSO.

Configuring an SSL connection to the ObjectServer:

For environments that include a Tivoli Netcool/OMNIbus ObjectServer user registry, you need to set up encrypted communications on the Tivoli Integrated Portal Server.

Follow these steps to establish a secure channel for communications between the Tivoli Integrated Portal Server and the ObjectServer.

1. Retrieve the ObjectServer certificate information, as follows:
   a. In the Tivoli Integrated Portal navigation pane, click **Security** > **SSL certificate and key management**.
   b. On the SSL certificate and key management page, click **Key stores and certificates** and on the page that is displayed, click **NodeDefaultTrustStore**.
   c. On the NodeDefaultTrustStore page, click **Signer certificates** and on the page that is displayed, click **Retrieve from port**.
   d. In the relevant fields, enter **Host**, **Port**, and **Alias** values for the ObjectServer and click **Retrieve signer information**.

      The signer information is retrieved and stored. For your reference, when the signer information has been retrieved, the following details are displayed:

      Serial number
      Specifies the certificate serial number that is generated by the issuer of the certificate.

      Issued to
      Specifies the distinguished name of the entity to which the certificate was issued.

Issued by
Specifies the distinguished name of the entity that issued the certificate. This name is the same as the issued-to distinguished name when the signer certificate is self-signed.

Fingerprint (SHA digest)
Specifies the Secure Hash Algorithm (SHA hash) of the certificate, which can be used to verify the certificate's hash at another location, such as the client side of a connection.

Validity period
Specifies the expiration date of the retrieved signer certificate for validation purposes.

2. Open *tip_home_dir*/profiles/TIPProfile/etc/com.sybase.jdbc3.SybDriver.props in a text editor and change these parameters:
   a. Enable SSL for ObjectServer primary host: `USESSLPRIMARY=TRUE`
   b. Enable SSL for ObjectServer backup host: `USESSLBACKUP=TRUE`
3. 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`

Single sign-on

The single sign-on (SSO) capability in Tivoli products means that you can log on to one Tivoli application and then launch to other Tivoli Web-based or Web-enabled applications without having to re-enter your user credentials.

The repository for the user IDs can be the Tivoli Netcool/OMNIbus ObjectServer or a Lightweight Directory Access Protocol (LDAP) registry. A user logs on to one of the participating applications, at which time their credentials are authenticated at a central repository. With the credentials authenticated to a central location, the user can then launch from one application to another to view related data or perform actions. Single sign-on can be achieved between applications deployed to Tivoli Integrated Portal servers on multiple machines.

Single sign-on capabilities require that the participating products use Lightweight Third Party Authentication (LTPA) as the authentication mechanism. When SSO is enabled, a cookie is created containing the LTPA token and inserted into the HTTP response. When the user accesses other Web resources (portlets) in any other application server process in the same Domain Name Service (DNS) domain, the cookie is sent with the request. The LTPA token is then extracted from the cookie and validated. If the request is between different cells of application servers, you must share the LTPA keys and the user registry between the cells for SSO to work. The realm names on each system in the SSO domain are case sensitive and must match exactly. See Managing LTPA keys from multiple WebSphere Application

Server cells on the WebSphere Application Server Information Center.

Configuring single sign-on:

Use these instructions to establish single sign-on support and configure a federated repository.

Configuring SSO is a prerequisite to integrating products that are deployed on multiple servers. All Tivoli Integrated Portal Server instances must point to the central user registry (such as a Lightweight Directory Access Protocol server).

Attention: ITM single sign on (SSO) support is only available with ITM Version 6.2 Fix Pack 1 or higher.

To configure the WebSphere federated repositories functionality for LDAP:

1. Log in to the administrative console.
2. In the **Authentication** area, expand **Web security** and click **Single sign-on**.
3. Click the **Enabled** option if SSO is disabled.
4. Click **Requires SSL** if all of the requests are expected to use HTTPS.
5. Enter the fully-qualified domain names in the Domain name field where SSO is effective. If the domain name is not fully qualified, the Tivoli Integrated Portal Server does not set a domain name value for the **LtpaToken** cookie and SSO is valid only for the server that created the cookie. For SSO to work across Tivoli applications, their application servers must be installed in same domain (use the same domain name).
6. Optional: Enable the **Interoperability Mode** option if you want to support SSO connections in WebSphere Application Server version 5.1.1 or later to interoperate with previous versions of the application server.
7. Optional: Enable the **Web inbound security attribute propagation** option if you want information added during the login at a specific Tivoli Enterprise Portal Server to propagate to other application server instances.
8. After clicking **OK** to save your changes, stop and restart all the Tivoli Integrated Portal Server instances.

Note: When you launch Network Manager, you must use a URL in the format protocol://host.domain:port /*. If you do not use a fully-qualified domain name, Network Manager cannot use SSO between Tivoli products.

Protecting the vault key file

To keep the encryption key for the administrator password secure, establish strict read-only access to the vault key file.

The Tivoli Integrated Portal administrator ID (default is **tipadmin**) that was created during the installation needs access to the vault key file for Tivoli Integrated Portal applications to work properly.

The vault key is an encryption key that is used to encrypt the administrator password that was provided during installation and is stored locally for Tivoli Integrated Portal applications. Use these steps to restrict access to the file.

1. On the computer where the application server is installed, open the *tip_home_dir*/_uninst/TIPInstall21 directory.
2. Use the method provided by your operating system to ensure that the .vault.key file has read-only access.

On Windows, for example, the attributes for the TIPInstall21 directory are already set to read-only; those for the `.vault.key` file are set to read-only and hidden.

Configuring access for HTTP and HTTPS

By default, the application server requires HTTPS (Hypertext Transfer Protocol Secure) access. If you want some users to be able to log in and use the console with no encryption of transferred data, including user ID and password, configure the environment to support both HTTP and HTTPS modes.

After installing Network Manager and before beginning this procedure, log in to the portal to ensure that it has connectivity and can start successfully.

Configuring for HTTP and HTTPS console access involves editing the `web.xml` file of Web components. Use this procedure to identify and edit the appropriate Web XML files.

1. Change to the following directory: *tip_home_dir*`/profiles/TIPProfile/config/cells/TIPCell/applications`.
2. From this location, locate the `web.xml` files in the following directories:
   - For the Integrated Solutions Console Web application archive: `isclite.ear/deployments/isclite/isclite.war/WEB-INF`
   - For the Tivoli Common Reporting: `tcr.ear/deployments/tcr/rptviewer_v1.2.0.war/WEB-INF`
   - For the Tivoli Common Reporting Web application archive: `isclite.ear/deployments/isclite/rptwebui_v1.2.0.war/WEB-INF`
   - For the Tivoli Integrated Portal Charts Web application archive: `isclite.ear/deployments/isclite/TIPChartPortlet.war/WEB-INF`
   - For the Tivoli Integrated Portal Change Password Web application archive: `isclite.ear/deployments/isclite/TIPChangePasswd.war/WEB-INF`
3. Open one of the `web.xml` files using a text editor.
4. Find the `<transport-guarantee>` element. The initial value of all `<transport-guarantee>` elements is `CONFIDENTIAL`, meaning that secure access is always required.
5. Change the setting to `NONE` to enable both HTTP and HTTPS requests. The element now reads: `<transport-guarantee>NONE</transport-guarantee>`.
6. Save the file, and then repeat these steps for the other `web.xml` deployment files.
7. Stop and restart the application server.

The following example is a section of the `web.xml` file for `TIPChangePasswd` where the transport-guarantee parameter is set to `NONE`:

```
<security-constraint>
 <display-name>
 ChangePasswdControllerServletConstraint</display-name>
 <web-resource-collection>
  <web-resource-name>ChangePasswdControllerServlet</web-resource-name>
  <url-pattern>/*</url-pattern>
 </web-resource-collection>
 <auth-constraint>
     <description>Roles</description>
  <role-name>administrator</role-name>
           <role-name>operator</role-name>
           <role-name>configurator</role-name>
           <role-name>monitor</role-name>
           <role-name>iscadmins</role-name>
 </auth-constraint>
```

```
  <user-data-constraint>
   <transport-guarantee>NONE</transport-guarantee>
  </user-data-constraint>
 </security-constraint>
```

Users must now specify a different port, depending on the mode of access. The default port numbers are as follows:

http://<*host_name*>:16310/ibm/console
Use the HTTP port for logging in to the Tivoli Integrated Portal on the HTTP port .

https://<*host_name*>:16311/ibm/console
Use the HTTPS secure port for logging in to the Tivoli Integrated Portal.

Note: If you want to use single sign-on (SSO) then you must use the fully qualified domain name of the Tivoli Integrated Portal host.

Enabling FIPS

You can configure the Tivoli Integrated Portal Server to use Federal Information Processing Standard Java Secure Socket Extension files.

Follow these steps to enable FIPS 140–2 for the Tivoli Integrated Portal Server.

1. Configure the application server to use FIPS.
   a. In the portal, click **Security > SSL certificate and key management**.
   b. Select the **Use the United States Federal Information Processing Standard (FIPS) algorithms** option and click **Apply**. This option makes IBMJSSE2 and IBMJCEFIPS the active providers.
2. Configure the application server to use FIPS algorithms for Java clients that must access enterprise beans:
   a. Open the *install_dir*/profiles/TIPProfile/properties/ssl.client.props file in a text editor.
   b. Change the com.ibm.security.useFIPS property value from false to true.
3. Configure the application server to use FIPS algorithms for SOAP-based administrative clients that must access enterprise beans:
   a. Open the *install_dir*/profiles/TIPProfile/properties/soap.client.props file in a text editor.
   b. Add this line:com.ibm.ssl.contextProvider=IBMJSSEFIPS.
4. Configure java.security to enable IBMJCEFIPS:
   a. Open the *install_dir*/java/jre/lib/security/java.security file in a text editor.
   b. Insert the IBMJCEFIPS provider (com.ibm.crypto.fips.provider.IBMJCEFIPS) before the IBMJCE provider, and also renumber the other providers in the provider list. The IBMJCEFIPS provider must be in the java.security file provider list. See the example at the end of this topic.
5. Enable your browser to use Transport Layer Security (TLS) 1.0:
   a. Microsoft Internet Explorer: Open the Internet Explorer and click **Tools > Internet Options**. On the **Advanced** tab, select the **Use TLS 1.0** option.
   b. Firefox: TLS 1.0 is enabled by default.
6. Export Lightweight Third Party Authentication keys so applications that use these LTPA keys can be reconfigured.
   a. In the navigation pane, click **Settings** > **Websphere Admin Console** and click **Launch Websphere Admin Console**.

b. In the WebSphere Application Server administrative console, select **Settings** > **Global security**.
c. In the Global security page, from the Authentication area, click the **LTPA** link.
d. Under **Cross-cell single sign-on**, specify a key file and provide a filename and password for the file that will contain the exported LTPA keys.
e. Click **Export keys**.

7. Reconfigure any applications that use Tivoli Integrated Portal Server LTPA keys: To reconfigure the Tivoli SSO service with the updated LTPA keys, run this script: *tip_home_dir*/profiles/TIPProfile/bin/setAuthnSvcLTPAKeys.jacl.
   a. Change directory to *tip_home_dir*/profiles/TIPProfile/bin/
   b. Start the Tivoli Integrated Portal Server:
      - Windows `startServer.bat server1`
      - UNIX Linux `startServer.sh server1`
   c. Run the following command:

      ```
      wsadmin -username tipadmin -password tipadmin_password -f
      setAuthnSvcLTPAKeys.jacl exported_key_path key_password
      ```

      Where:

      exported_key_path is name and full path to the key file that was exported.

      key_password is the password that was used to export the key.
8. For SSO, enable FIPS for any other application servers, then import the updated LTPA keys from the first server into these servers:
   a. Copy the LTPA key file from step 4 above to another application server computer.
   b. In the navigation pane, click **Settings** > **Websphere Admin Console** and click **Launch Websphere Admin Console**.
   c. In the WebSphere Application Server administrative console, select **Settings** > **Global security**.
   d. In the Global security page, from the Authentication area, click the **LTPA** link.
   e. Under **Cross-cell single sign-on**, provide the filename and password from above for the file that contains the exported LTPA keys.
   f. Click **Import keys**.
9. Run the ConfigureCLI command:

   Windows `tip_home_dir\bin\tipcli.bat ConfigureCLI --useFIPS true`

   Linux UNIX `tip_home_dir/bin/tipcli.sh ConfigureCLI --useFIPS true`

The IBM SDK *tip_home_dir*/java/jre/lib/security/java.security file looks like this when IBMJCEFIPS is enabled.

```
security.provider.1=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.2=com.ibm.crypto.provider.IBMJCE
security.provider.3=com.ibm.jsse.IBMJSSEProvider
security.provider.4=com.ibm.jsse2.IBMJSSEProvider2
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath
security.provider.7=com.ibm.crypto.pkcs11.provider.IBMPKCS11
security.provider.8=com.ibm.security.cmskeystore.CMSProvider
security.provider.9=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
```

Configuring the LPTA token timeout value

You can configure the Lightweight Third Party Authentication (LTPA) token timeout value for Tivoli Integrated Portal in the WebSphere Application Server console.

Tivoli Integrated Portal is enabled for single sign-on.

The default timeout for an LTPA token is 120 minutes. An LTPA timeout causes you to be logged out from Tivoli Integrated Portal and can also cause an authentication popup message, if the first request after the timeout is an AJAX request from a portlet. To configure the LTPA token timeout:

1. In the Tivoli Integrated Portal navigation pane, click **Settings** > **WebSphere Admin Console**.
2. Click **Launch WebSphere Admin Console** to start the WebSphere Application Server console.
3. In the WebSphere Application Server console navigation pane, click **Security** > **Global security**.
4. In the Authentication area of the Global security page, click the **LTPA** link.
5. In the LTPA timeout area of the LTPA page, edit the value for the LTPA timeout and click **OK**.
6. In the Messages area at the top of the Global security page, click the **Save** link and log out of the WebSphere Application Server console.

In a load balanced environment, you must set the LTPA token timeout value on each of the Tivoli Integrated Portal Server instances.

Configuring VMM for the ObjectServer

If you installed Tivoli Netcool/OMNIbus using the Network Manager installer and selected to use the ObjectServer for user authentication, the installer configures the Virtual Member Manager (VMM) adapter for the ObjectServer. Otherwise, you must configure VMM manually if you want to use the ObjectServer for user authentication.

Have the following ObjectServer information at hand: administrator name and password, IP address, and port number. If you have a second ObjectServer for failover support, you need the IP address and port number. The ObjectServer must be running at the time of installing Network Manager, as the installation process attempts to connect to the ObjectServer.

The script assumes that the `tip` installation directory is the parent directory and that the profile and cell names are TIPProfile and TIPCell. Run the VMM configuration script on every computer where the application server is installed.

1. Change to the *`tip_home_dir`*`/bin` directory. The directory contains a script to run:
   - Windows `confvmm4ncos.bat`
   - Linux `confvmm4ncos.sh`
   - UNIX `confvmm4ncos.sh`
2. Enter the following command at the command line: `confvmm4ncos user password address port [address2 port2]`where
   a. `user` is the ID of a user with administrative privileges for this ObjectServer
   b. `password` is the password for the user ID
   c. `address` is the IP address of the ObjectServer

d. `port` is the port number used by the ObjectServer
e. Optional: `address2` and `port2`, if there is a failover server, is the IP address and port number of the failover ObjectServer

The VMM adapter is configured for the ObjectServer. Thereafter, whenever the user registry needs to be accessed, the VMM adapter is called for this information.

Changing the default security registry

The default security registry can be set at install time. Use this procedure to change the default registry after installation.

These steps require that your user ID has the Administrator role and that you know the base entry value of your repository. For LDAP or Microsoft Active Directory, this is usually a string like `ou=company,dc=country,dc=region`. For the ObjectServer, the base entry is `o=netcoolObjectServerRepository`.

If you did not select a default user registry during installation or you would like to change the default to a different registry, complete these steps.

1. If you are not already logged in to the administrative console, log in now. Your ID must have the Administrator role.
2. Click **Security** > **Secure administration, applications, and infrastructure**.
3. In the User account repositories area, select **Federated repositories** from the Available realm definitions, then click **Configure**.
4. Click **Supported entity types** under **Additional Properties**.
5. Click the entity type, then edit the **Base entry for the default parent** and **Relative Distinguished Name properties**.
6. After you click **OK** to save your changes, repeat the previous step to configure the other entity types. For Microsoft Active Directory, the entity types (PersonAccount, Group, and OrgContainer) must be configured with a base DN and the RDN for PersonAccount should be `cn` instead of `uid`.
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`

Integrating with IBM Tivoli Monitoring

You can install IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition to monitor the health of your Network Manager installation. IBM Tivoli Monitoring is included in the Network Manager package.

You must have installed Network Manager before installing IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.

Restriction: UNIX The launchpad opens xterm windows to run the shell scripts for migration and installation of IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition. If you want to paste non-ASCII characters between the xterm windows started by the installer and other windows, you must set your locale to one that ends with UTF-8 before running the launchpad. Use a command similar to this example: `export LANG=fr_FR.UTF-8`.

To install IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, perform the following tasks:

1. On the server where Network Manager core components are installed, run the IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition installation script.
   - To run the installation script using the launchpad, start the launchpad using the **`launchpad.sh`** script on UNIX or the **`launchpad.exe`** executable on Windows, and click **Postinstallation** > **Install the Monitoring Agent** > **Start ITM Agent Installation**.
   - To run the installation script using the command line, run the `ITMagent\WINDOWS\setup.exe` script on Windows or the `ITMagent/install.sh` script on UNIX from the `scripts` directory of the installation media.
2. For more installation steps, refer to the *IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition User's Guide*.

Configuring integration with IBM Systems Director

You can set up Network Manager to work with IBM Systems Director. After setting up the integration, you can launch IBM Systems Director from the Network Manager GUI and perform various tasks on the selected device in IBM Systems Director.

Overview of integration with IBM Systems Director

IBM Systems Director provides consolidated views of your managed systems and a set of tasks for system management including discovery, inventory, configuration, system health, monitoring, updates, event notification and automation across managed systems. After setting up the integration, you can open IBM Systems Director tasks from the Network Manager GUI using the right-click menu.

You can launch IBM Systems Director to manage resources in your network by right-clicking a device in any Network Manager topology view and selecting the **Launch to** > **Director** menu option, followed by selecting the task you want to open in IBM Systems Director.

The IBM Systems Director features you can launch for a device from within Network Manager depend on the information shared about the discovered device in both products. The following list identifies all IBM Systems Director tasks available when launching from Network Manager:

- Active Status

- Configure Access
- Current Configuration
- Create Group
- Compliance Issues
- Configuration Manager
- Configuration Plans
- Compliance Policy
- Configuration Templates
- Distributed Command
- Deployment History
- Event Log
- File Management
- Network Diagnostics
- Navigate Resource: Basic Topology
- Navigate Resources: Virtualization Topology
- Performance Summary
- Request Access
- Remote Command Line
- Verify Connection
- View and Collect Inventory
- Navigate Resources: Properties View

Note: The list of features available to launch from the Network Manager right-click menu will vary and might be a subset of the previous list.

For more information about the features opened in IBM Systems Director and assistance using them, click the help button on the opened IBM Systems Director page.

Alternatively, go to the IBM Systems Director information center at http://www-01.ibm.com/support/knowledgecenter/SSAV7B_621/com.ibm.director.main.helps.doc/fqm0_main.html?cp=SSAV7B_621%2F2 and search for the name you clicked on in the right-click menu option (for example, search for "Configure Access").

Integration architecture

The integration between Network Manager and IBM Systems Director requires a Java adapter process to run based on settings defined in the `itnmSystemsDirector.properties` configuration file.

The configuration file is installed by default with Network Manager on the GUI server, and it can be found in the `NCHOME/precision/adapters/itnm_systemsDirectorLiC` directory.

The Java adapter process communicates with the IBM Systems Director server using HTTPS to associate IBM Systems Director resources and launch-points with devices discovered by Network Manager for the domain defined in the properties file. The adapter determines the set of IBM Systems Director launch points related to a Network Manager device, and stores them in the LiCmapping NCIM table.

The LiCmapping table describes the IBM Systems Director resource, launch-point URL, and menu name for each task you can run against a Network Manager device.

Restriction: For the integration to be successful, both Network Manager and IBM Systems Director must discover and manage the same resources.

Downloading and installing the IBM Systems Director

You must have an IBM Systems Director installation running before configuring integration with Network Manager.

To obtain IBM Systems Director, perform the following steps:

1. Go to http://www.ibm.com/systems/management/director/downloads/
2. Go to the **Management servers** tab and download IBM Systems Director version 6.2 or later.
3. Go to the IBM Systems Director information center at http://www-01.ibm.com/support/knowledgecenter/SSAV7B_621/com.ibm.director.main.helps.doc/fqm0_main.html?cp=SSAV7B_621%2F2, expand "IBM Systems Director V6.2.1", and then go to the "Planning" and "Installing" topic collections.
4. Follow the instructions provided to plan the installation and complete the installation of IBM Systems Director.

Setting up integration with the IBM Systems Director

Perform the following tasks to set up the integration between Network Manager and IBM Systems Director.

Preparing the properties file:

To set up the integration, you must create a copy of the `itnmSystemsDirector.properties` file for each Network Manager domain you want to run IBM Systems Director tasks against.

Create a copy of the properties file for the domain against which you intend to run the adapter:

1. Go to the `NCHOME/precision/adapters/itnm_systemsDirectorLiC` directory. The configuration file is installed by default with Network Manager on the GUI server.
2. Make a copy of the `itnmSystemsDirector.properties` file and append the file name with the name of the domain you want to set up integration for.

   For example, to create a copy of the properties file for the domain NCOMS, enter the following command on UNIX operating systems:

   ```
   cp itnmSystemsDirector.properties itnmSystemsDirector.properties.NCOMS
   ```

   This creates a copy of the properties file and adds NCOMS to the end of the file.
3. Use the copy of the file to set up the integration as described in the following tasks.

Exporting and importing the SSL certificate:

The Java adapter process that communicates between Network Manager and IBM Systems Director requires the setup of a secure connection. You must import the SSL certificate from the IBM Systems Director server into the trust store used by the Network Manager Java process running the adapter.

To obtain the certificate, you must export it from IBM Systems Director and then import it into Network Manager:

1. Log into the IBM Systems Director server.
2. Export the certificate using the **keytool -export** command:

   ```
   /opt/ibm/director/jre/bin/keytool -export -alias lwiks -keystore
   /opt/ibm/director/lwi/security/keystore/ibmjsse2.jks -file
   directorcert.arm
   ```
3. Copy the `directorcert.arm` file to the Network Manager server where the adapter will run. For example, `/tmp/directorcert.arm`.
4. Import the `directorcert.arm` file into the local trust store using the **keytool -import** command:

   ```
   keytool -import -alias directorcert -file /path to file/directorcert.arm
   -keystore TIPHOME/java/jre/lib/security/cacerts
   ```

   Note: The default password is `changeit`.

   The following shows an example of importing the certificate:

   ```
   /opt/IBM/tivoli/tip/java/bin/keytool -import -alias directorcert -file
   /tmp/directorcert.arm -keystore /opt/IBM/tivoli/tip/java/jre/lib/
   security/cacerts
   ```

Configuring connection properties:

Edit the copy of the `itnmSystemsDirector.properties` file to specify the connection properties for the adapter linking Network Manager and IBM Systems Director.

Make sure you have created a copy of the `itnmSystemsDirector.properties` file and appended the file name with the name of the domain for which you want to set up the integration with IBM Systems Director; for example `itnmSystemsDirector.properties.NCOMS`.

To configure the connection properties:

1. Open the properties file `itnmSystemsDirector.properties.`*`name of domain`*.
2. Edit the following values to set up the connection:
   a. Set the **itnm.integration.ibm.SystemsDirector.cryptographicKeyFile** parameter to reference the Network Manager cryptographic key file or a key file you generated using the **./itnm_systemsDirectorLiC.sh** `-generate -keyfile` *file name* option.

      For example, set the path as follows to use the default key file:

      ```
      itnm.integration.ibm.SystemsDirector.cryptographicKeyFile=/opt/IBM/
      tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/
      encryption/keys/crypt.key
      ```
   b. Set the **itnm.integration.ibm.SystemsDirector.server** parameter to reference the IP address or host name of the IBM Systems Director server. For example:

      ```
      itnm.integration.ibm.SystemsDirector.server=192.0.2.24
      ```

c. Set the **itnm.integration.ibm.SystemsDirector.port** parameter to the port number on which the IBM Systems Director server is listening on. For example:

```
itnm.integration.ibm.SystemsDirector.port=4495
```

Note: The default port is 8422.

d. Set the **itnm.integration.ibm.SystemsDirector.userName** parameter to reference the IBM Systems Director user name. For example:

```
itnm.integration.ibm.SystemsDirector.userName=root
```

3. Encrypt and set the password for the IBM Systems Director user:
   a. Go to the NCHOME/precision/adapters/itnm_systemsDirectorLiC directory.
   b. Run the following command using the password for the IBM Systems Director user set in the **itnm.integration.ibm.SystemsDirector.userName** parameter: `./itnm_systemsDirectorLiC.sh -encrypt` *password* `-keyfile` */full path to cryptographic key file/cryptographic key file name*`.key`. This will create an encrypted text string for the password.

      For example, to encrypt the password Network1 using the default key file, enter:

      ```
      ./itnm_systemsDirectorLiC.sh -encrypt Network1 -keyfile
      /opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/
      encryption/keys/crypt.key
      ```

      An example output of the encryption process is jR/CjUmgRaYRF64Dsf37FGJvxDxqmxcE3XybALZ7THo=.

   c. Set the **itnm.integration.ibm.SystemsDirector.password** parameter to reference the encrypted password of the user.

      For example, to use the encrypted password from the previous step, enter:

      ```
      itnm.integration.ibm.SystemsDirector.password=
      jR/CjUmgRaYRF64Dsf37FGJvxDxqmxcE3XybALZ7THo=
      ```

4. Set the **itnm.integration.ibm.SystemsDirector.jreKeyStoreFile** parameter to reference the location of the Network Manager keystore you imported the SSL certificate into. For example:

   ```
   itnm.integration.ibm.SystemsDirector.jreKeyStoreFile=/opt/IBM/tivoli/tip/
   java/jre/lib/security/cacerts
   ```

5. Encrypt and set the password for the keystore file:
   a. Go to the NCHOME/precision/adapters/itnm_systemsDirectorLiC directory.
   b. Run the following command using the password for the keystore file: `./itnm_systemsDirectorLiC.sh -encrypt` *password* `-keyfile` */full path to cryptographic key file/cryptographic key file name*`.key`. This will create an encrypted text string for the password.

      For example, to encrypt the password Crypto1 using the default key file, enter:

      ```
      ./itnm_systemsDirectorLiC.sh -encrypt Crypto1 -keyfile
      /opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/
      encryption/keys/crypt.key
      ```

      An example output of the encryption process is i/y7aYCV5looIK3eRoYEPWJvxDxqmxcE3XybALZ7THo=.

   c. Set the **itnm.integration.ibm.SystemsDirector.jreKeyStorePassword** parameter to reference the encrypted password for the keystore file.

      For example, to use the encrypted password from the previous step, enter:

      ```
      itnm.integration.ibm.SystemsDirector.jreKeyStorePassword=
      i/y7aYCV5looIK3eRoYEPWJvxDxqmxcE3XybALZ7THo=
      ```

6. Save the properties file.

You can specify additional optional settings in the `itnmSystemsDirector.properties` file for the adapter.

Related tasks:

"Additional adapter settings" on page 216
Apart from setting the connection properties, you can modify the default parameters that control additional behavior and logging characteristics of the adapter. Edit the copy of the `itnmSystemsDirector.properties` file for the adapter linking the Network Manager domain and IBM Systems Director.

Configuring connection to NCIM:

You can configure the connection settings to the NCIM database where the adapter populates the LiCmapping table with data from IBM Systems Director. If the **itnm.integration.ibm.SystemsDirector.itnmDatabaseUseConnectionPool** is set to `true`, then the default settings to NCIM are used, and you do not need to configure the database properties.

The only mandatory parameter is **itnmDomain** which must be specified (see first step).

To set the connection properties for the NCIM database:

1. In the **itnm.integration.ibm.SystemsDirector.itnmDomain** property, specify the Network Manager domain against which the adapter runs. For example:
   `itnm.integration.ibm.SystemsDirector.itnmDomain=NCOMS`
2. Optional: If you do not want to use the default settings and have **itnm.integration.ibm.SystemsDirector.itnmDatabaseUseConnectionPool** set to `false`, you can specify alternative database properties for the adapter to use:
   a. Remove the hash from the beginning of the line and set the **itnm.integration.ibm.SystemsDirector.itnmDatabaseType** property to the database type you want to use. The supported values are `DB2`, `Oracle`, `MySQL`, and `Informix`.
   b. Remove the hash from the beginning of the line and set the **itnm.integration.ibm.SystemsDirector.itnmDatabaseDriver** property to the JDBC driver URL that specifies the type of JDBC driver to use. Use one of the following values based on your selected database:
      - For DB2: `com.ibm.db2.jcc.DB2Driver`
      - For Oracle: `oracle.jdbc.driver.OracleDriver`
      - For MySQL: `com.mysql.jdbc.Driver`
      - For Informix: `com.informix.jdbc.IfxDriver`
   c. Remove the hash from the beginning of the line and set the **itnm.integration.ibm.SystemsDirector.itnmDatabaseURL** property to the JDBC URL for connecting to the NCIM database. Use one of the following syntax based on your selected database:
      - For DB2: `jdbc:db2://`*`host_name`*`:`*`port_number`*`/`*`database_name`*
      - For Oracle: `jdbc:oracle:thin:@`*`host_name`*`:`*`port_number`*`:`*`database_name`*
      - For MySQL: `jdbc:mysql://`*`host_name`*`:`*`port_number`*`/`*`database_name`*
      - For Informix: `jdbc:informix-sqli://`*`host_name`*`:`*`port_number`*`/`*`database_name`*`:INFORMIXSERVER=`*`server_name`*

Tip: This setting depends on the database you use. Refer to ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties for information about the database used and help with completing the platform-specific URL.

The following example shows the settings for an Informix database:

```
# itnm.integration.ibm.SystemsDirector.itnmDatabaseType=Informix
# itnm.integration.ibm.SystemsDirector.itnmDatabaseDriver=
com.informix.jdbc.IfxDriver
# itnm.integration.ibm.SystemsDirector.itnmDatabaseURL=
jdbc:informix-sqli://abc123.ibm.com:9995/ncimdb:INFORMIXSERVER=inst1
```

3. Optional: Set the **itnm.integration.ibm.SystemsDirector.itnmDatabaseUserName** property to reference the NCIM database user name. For example:

   ```
   itnm.integration.ibm.SystemsDirector.itnmDatabaseUserName=root
   ```

4. Optional: Encrypt and set the password for the NCIM user:
   a. Go to the NCHOME/precision/adapters/itnm_systemsDirectorLiC directory.
   b. Run the following command using the password for the NCIM user set in the **itnm.integration.ibm.SystemsDirector.itnmDatabaseUserName** property: `./itnm_systemsDirectorLiC.sh -encrypt` *password* `-keyfile` */full path to cryptographic key file/cryptographic key file name*`.key`. This will create an encrypted text string for the password.

      For example, to encrypt the password Database1 using the default key file, enter:

      ```
      ./itnm_systemsDirectorLiC.sh -encrypt Database1 -keyfile
      /opt/IBM/tivoli/netcool/precision/profiles/TIPProfile/etc/tnm/
      encryption/keys/crypt.key
      ```

      An example output of the encryption process is DvDlWqoRzRHAD9WpYzkI0mJvxDxqmxcE3XybALZ7THo=.

   c. Set the **itnm.integration.ibm.SystemsDirector.itnmDatabasePassword** property to reference the encrypted password. For example:

      ```
      itnm.integration.ibm.SystemsDirector.itnmDatabasePassword=
      DvDlWqoRzRHAD9WpYzkI0mJvxDxqmxcE3XybALZ7THo=
      ```

5. Save the properties file.

Additional adapter settings:

Apart from setting the connection properties, you can modify the default parameters that control additional behavior and logging characteristics of the adapter. Edit the copy of the itnmSystemsDirector.properties file for the adapter linking the Network Manager domain and IBM Systems Director.

Make sure you edit the copy of the itnmSystemsDirector.properties file for the domain you set up the integration for.

The configuration file is installed by default with Network Manager on the GUI server, and it can be found in the NCHOME/precision/adapters/itnm_systemsDirectorLiC directory.

To modify additional characteristics of the adapter:

1. Open the properties file itnmSystemsDirector.properties.*name of domain*.
2. Edit the following values:
   a. Set the **itnm.integration.ibm.SystemsDirector.connectTimeout** parameter to the amount of time during which the adapter attempts to connect to the

IBM Systems Director server. If the adapter cannot connect after the specified time elapses, it produces an error. The value is in milliseconds and the default is 60000 (60 seconds).

b. Set the **itnm.integration.ibm.SystemsDirector.readTimeout** parameter to the amount of time the adapter waits to read data from the IBM Systems Director server after connecting to it. If the adapter cannot read any data after the specified time elapses, it produces an error. The value is in milliseconds and the default is 60000 (60 seconds).

c. Use the **itnm.integration.ibm.SystemsDirector.verifySSLHostNames** parameter to set whether or not the adapter verifies the name of the IBM Systems Director server stored in the certificate. Verification is performed if set to `true`, while no verification is performed if set to `false`.

d. Use the **itnm.integration.ibm.SystemsDirector.usePasswordAuthentication** parameter to set whether or not password authentication is used. Password authentication turned on if set to `true`, while authentication is turned off if set to `false`.

e. Use the **itnm.integration.ibm.SystemsDirector.ignoreIPAddress.n** parameter to instruct the adapter to ignore specific IP addresses in IBM Systems Director. Specify more than one IP address by repeating this parameter and incrementing *n* by 1 each time.

   For example, to set adapter to ignore IP addresses 192.0.2.12 and 192.0.2.24, add the following lines:

   ```
   itnm.integration.ibm.SystemsDirector.ignoreIPAddress.1=192.0.2.12
   itnm.integration.ibm.SystemsDirector.ignoreIPAddress.2=192.0.2.24
   ```

f. Use the **itnm.integration.ibm.SystemsDirector.ignoreHostName.n** parameter to instruct the adapter to ignore specific host names. Specify more than one host name by repeating this parameter and incrementing *n* by 1 each time.

   For example, to set adapter to ignore host names mymachine and ball.company.com, add the following lines:

   ```
   itnm.integration.ibm.SystemsDirector.ignoreHostName.1=mymachine
   itnm.integration.ibm.SystemsDirector.ignoreHostName.2=ball.company.com
   ```

g. The adapter creates a table in NCIM associating IBM Systems Director resources with devices discovered by Network Manager for the domain defined in the properties file. You can override the individual IBM Systems Director resource to Network Manager device mapping by manually specifying which IBM Systems Director OID corresponds to what Network Manager main node IP address or host name. Use the **itnm.integration.ibm.SystemsDirector.mapOIDtoITNMIPAddressOrHostName.n** parameter to instruct the adapter to override the automatic resource association. Specify more than one resource by repeating this parameter and incrementing *n* by 1 each time. The format is `mapOIDtoITNMIPAddressOrHostName.`*`n=oid:ipaddress`* or `mapOIDtoITNMIPAddressOrHostName.`*`n+1=oid:hostname`*.

   For example, to set adapter to take the OID 2292 and associate it with IP address 192.0.2.12, and take OID 2286 and associate it with host name mymachine, add the following lines:

   ```
   itnm.integration.ibm.SystemsDirector.mapOIDtoITNMIPAddressOrHostName.1=
   2292:192.0.2.12
   itnm.integration.ibm.SystemsDirector.mapOIDtoITNMIPAddressOrHostName.1=
   2286:mymachine
   ```

h. You can set the adapter to ignore specific IBM Systems Director tasks. Use the **itnm.integration.ibm.SystemsDirector.ignoreTask.n** parameter to set

tasks that are ignored by the adapter and are not available to run on a device. Specify more than one task by repeating this parameter and incrementing *n* by 1 each time.

For example, to set adapter to ignore the Network Diagnostics task, add the following line:

```
itnm.integration.ibm.SystemsDirector.ignoreTask.1=Network Diagnostics
```

3. Save the properties file.

You can also set the logging properties for the adapter process.

Related tasks:

"Setting logging properties for adapter"
You can specify logging properties for the adapter used to link IBM Systems Director and Network Manager.

Setting logging properties for adapter:

You can specify logging properties for the adapter used to link IBM Systems Director and Network Manager.

Make sure you edit the copy of the `itnmSystemsDirector.properties` file for the domain you set up the integration for.

To set the logging properties for the adapter:

1. Open the properties file `itnmSystemsDirector.properties.`*`name of domain`*.
2. Edit the following values:
   a. Set the overall logging level using the **`.level`** parameter. The default is `WARNING` and the following levels can be set:
      - `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.
      - `FINER`:

        Medium level of tracing that provides more detailed debug messages.
      - `FINEST`:

        Maximum level of tracing that produces very detailed technical information.

   b. Set the logging level for the file handler using the **`java.util.logging.FileHandler.level`** parameter. The possible levels are the same as for the **`.level`** parameter.
   c. If used, set the logging level for the console handler using the **`java.util.logging.ConsoleHandler.level`** parameter. The possible levels are the same as for the **`.level`** parameter.

d. Modify where the log file is saved to using the **java.util.logging.FileHandler.pattern** parameter.

3. Save the properties file.

Logging for the adapter process uses the same logic as other logging in Network Manager. Check the log files to pinpoint any potential issues.

Running the adapter to populate NCIM

After setting the adapter properties, you can run the adapter to populate the NCIM database with information on the resources that can be managed in IBM Systems Director for the Network Manager domain defined in the properties file.

Make sure you have set all the required parameters in the adapter properties file for the domain.

To run the adapter:

1. Change to the `NCHOME/precision/adapters/itnm_systemsDirectorLiC` directory.
2. Run the adapter using the **./itnm_systemsDirectorLiC.sh** command and reference the properties file for the domain you set up the adapter for.

   For example, to run the adapter for the NCOMS domain, enter the following command:

   ```
   ./itnm_systemsDirectorLiC.sh itnmSystemsDirector.properties.NCOMS
   ```

   Based on the settings in the properties file, the adapter populates the LiCmapping table in the NCIM database with launch-point information from IBM Systems Director.
3. Right-click devices in any Network Manager topology view after running the adapter. A set of IBM Systems Director tasks are available to be launched from Network Manager for the device if the device is managed by both products. The following list identifies all IBM Systems Director tasks available when launching from Network Manager:
   - Active Status
   - Configure Access
   - Current Configuration
   - Create Group
   - Compliance Issues
   - Configuration Manager
   - Configuration Plans
   - Compliance Policy
   - Configuration Templates
   - Distributed Command
   - Deployment History
   - Event Log
   - File Management
   - Network Diagnostics
   - Navigate Resource: Basic Topology
   - Navigate Resources: Virtualization Topology
   - Performance Summary
   - Request Access
   - Remote Command Line

- Verify Connection
- View and Collect Inventory
- Navigate Resources: Properties View

Note: The list of features available to launch from the Network Manager right-click menu will vary and might be a subset of the previous list.

Troubleshooting the integration with IBM Systems Director

If the launch in context from Network Manager to IBM Systems Director does not work, you might need to check your IBM Systems Director integration settings.

If the integration with IBM Systems Director does not work, it is likely that the adapter did not run and populate the launch-point data in the LiCmapping table.

To check the integration settings:

1. The first step when an error occurs is to check all of the configuration settings and check that both Network Manager and IBM Systems Director are managing the same set of resources.
2. Check the following items:

Option	Description
The SSL certificate was not imported from IBM Systems Director into Network Manager.	Export the certificate and then import it into Network Manager as described in "Exporting and importing the SSL certificate" on page 213.
The IBM Systems Director configuration is not correct.	Make sure you set the connection properties to the IBM Systems Director properly, as described in "Configuring connection properties" on page 213.
The Network Manager NCIM database configuration is not correct.	Check the NCIM settings as described in "Configuring connection to NCIM" on page 215.
There is a firewall blocking access to the IBM Systems Director API.	Check your firewall settings and allow access to the IBM Systems Director host.
The specified Network Manager domain does not have devices managed by IBM Systems Director.	Make sure that the same devices are discovered by both products.
The IBM Systems Director server is not running.	Make sure the IBM Systems Director server is running and you can log on. For more information about IBM Systems Director, see the information center at http://www-01.ibm.com/support/knowledgecenter/SSAV7B/welcome and search for "Management server and agent commands."
The Network Manager NCIM database is not running.	Make sure all processes are running in Network Manager, as described in .
The specified passwords have been encrypted using a different cryptographic key file to the one specified in the properties file.	Make sure you encrypt the passwords with the file you reference in the adapter properties file, as described in "Configuring connection properties" on page 213.

3. If the error requires more detailed information to understand its cause, set the logging level to FINEST and examine the log file for error messages.

Related tasks:

"Setting logging properties for adapter" on page 218
You can specify logging properties for the adapter used to link IBM Systems Director and Network Manager.

Configuring Network Manager for UNIX operating systems

On UNIX-based operating systems, such as Solaris and AIX, you might need to perform extra configuration tasks before using the product.

Configuring root/non-root permissions

On UNIX, if you installed Network Manager as a non-root user, you must perform additional configuration.

Certain components of Network Manager require root permissions to run. You must perform different actions depending on whether you want to run Network Manager as a root user or a non-root user.

Root and non-root installation

On UNIX Network Manager can be installed as either the root user or a non-root user.

If you have installed any other IBM Tivoli products into the same installation directory, you must install Network Manager as the same user that installed the other products.

The Network Manager web applications must always be run as the user who installed the product.

After installation, you can configure the Network Manager core components to be run as a different user. For example, if you installed as the root user, you can configure the core components to be run as a non-root user.

Restriction: When Network Manager is installed and run as root, scripts are installed that restart Network Manager and Tivoli Netcool/OMNIbus processes when the server is rebooted. When Network Manager is installed and run as a non-root user, Network Manager and Tivoli Netcool/OMNIbus processes are not restarted automatically when the server is rebooted.

Restriction: AIX If you install the Network Manager core components as a non-root user on AIX, and you are using DB2 as the NCIM topology database, you must perform some additional configuration, and you must ensure that only one DB2 client library is active on the DB2 server. Having multiple DB2 clients active on the server might cause issues and is not supported.

Restriction: IBM Tivoli Business Service Manager must run as non-root. When installing Network Manager and IBM Tivoli Business Service Manager on the same server, make sure you install and run both as a non-root user.

Due to these restrictions, you cannot run the Network Manager core components and IBM Tivoli Business Service Manager on the same AIX server if you are using DB2 for the NCIM topology database.

Configuring the core components to run as root

On UNIX, if you installed Network Manager as a non-root user, you must perform additional configuration to run the core components as the root user.

The Network Manager Web applications must always be run as the user who installed the product.

You must run a script that updates file permissions to ensure that the root user has access to all necessary files.

If you installed Network Manager as the root user, you do not need to perform any configuration in order to run the core components as the root user.

1. Log in to the server where the Network Manager core components are installed. Log in as the root user.
2. Run the script either from the installer launchpad or the command line:

Option	Description
From the launchpad	1. Go to the directory where you extracted the Network Manager installation package. 2. Start the launchpad as root using the **./launchpad.sh** command. 3. Select the **Postinstallation** menu. 4. Expand **Non-root postinstallation tasks (UNIX only)** and click **Run IBM Tivoli Network Manager IP Edition 3.9 as root**.
From the command line	1. Go to the NCHOME/precision/scripts directory. 2. Run the setup_run_as_root.sh script.

Configuring the core components to run as non-root

On UNIX, if you installed Network Manager as a non-root user, and you want to allow that user permissions to run the core components, you must log in as root and perform additional configuration.

Attention: Only install and run as a non-root user on servers where trusted users are the only users who can log in.

The Network Manager Web applications must always be run as the user who installed the product.

To give a non-root user these permissions, you must run a script. It is not possible to install and run Network Manager without ever logging in as the root user. At a minimum you must log in as root temporarily to run this script.

Important: On Linux operating systems for s390 and s390x, you must install the GSKit software before running the setuid script.

Complete the following configuration steps in order to run the core components as a non-root user:

1. Log in as the root user.
2. Run the script either from the installer launchpad or the command line:

Option	Description
From the launchpad	1. Go to the directory where you extracted the Network Manager installation package. 2. Start the launchpad as root using the **./launchpad.sh** command. 3. Select the **Postinstallation** menu. 4. Expand **Non-root postinstallation tasks (UNIX only)** and click **Run IBM Tivoli Network Manager IP Edition 3.9 as installing user**.
From the command line	1. Go to the NCHOME/precision/scripts directory. 2. Run the following script: setup_run_as_setuid_root.sh.

3. Optional: If you want to run the mttrapd probe (also known as the SNMP probe) as non-root, perform additional configuration:
   - Configure the probe to run as a non-root user using the instructions on *Running the mttrapd probe as suid root* in the *IBM Tivoli Netcool/OMNIbus Probe for SNMP Reference Guide*.
   - AIX On AIX, you must also follow the instructions provided at this URL: http://www.ibm.com/support/docview.wss?uid=swg21296292

     Important: Note that because these instructions involve copying Sybase libraries to the /usr/lib directory, this might impact the operation of any installation of Sybase that is on the same server as the mttrapd probe.

After this script has completed, the user who performed the Network Manager installation can log in and run the Network Manager core components.

Installing GSKit on AIX:

Before you configure the core components to run as non-root on AIX, you must install the IBM Global Secure ToolKit (GSKit).

Make sure you have version 8.0.13.3 or later of the GSKit, an IBM cryptography software that enables Secure Socket Layer (SSL) communication. The GSKit is provided with the Network Manager installation package.

Before running the setup_run_as_setuid_root.sh script, you must install GSKit into the /usr/lib directory. Processes running as setuid do not use the LIBPATH environment variable, and so cannot use the GSKit if it is installed into a sub-directory of $NCHOME.

To install GSKit on AIX into /usr/lib using the **installp** command, complete the following tasks.

1. Log on as the root user.
2. Change to the directory where you extracted the Network Manager installation package or go to the root location on the installation media.
3. Open a command prompt and enter the following commands.

```
installp -acgXd . GSKit8.gskcrypt32.ppc.rte
installp -acgXd . GSKit8.gskssl32.ppc.rte
```

Where `-a` stands for apply, `-c` stands for commit, `-g` automatically installs or commits any requisite software product, `-X` expands the filesystem if necessary, and `-d` specifies the location of the installation media.

Note: The two GSKit packages are provided in the Network Manager installation package, and are available at the top level after you extract the package. In the previous example, the command is run from that top level directory.

Installing and configuring Informix after a non-root installation

Informix can only be installed by the root user. If you installed Network Manager as non-root and want to use Informix as your topology database, you must log in as root after the installation has completed and install Informix on the system using the values provided during the Network Manager installation.

Make sure the Network Manager installation has completed successfully. Check the installation log files for information on the post-installation work required for the database installation.

To set up Informix after a non-root installation:

1. Log in as root.
2. You can use the GUI (launchpad) or the command line interface:

Option	Description
Configuring Informix using the GUI (launchpad)	1. Go to the directory where you extracted the Network Manager installation package. 2. Start the launchpad as root using the **`./launchpad.sh`** command. 3. Select the **Postinstallation** menu. 4. Expand **Non-root postinstallation tasks (UNIX only)** and click **Finish installing Informix as topology database**. 5. Provide the location where you installed Network Manager (the $NCHOME environment variable value), and wait for the command window to complete. This might take a few minutes.
Configuring Informix using the command line interface	1. Go to `NCHOME/precision/install/scripts` 2. Run the **`install_ids_root.ksh`** command as follows: `./install_ids_root.ksh -f ../data/ids.properties` 3. Wait for the script to complete.

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://www-01.ibm.com/support/knowledgecenter/SSGU8G_11.70.0/com.ibm.welcome.doc/welcome.htm and search for *Administrator's Reference*.

Related tasks:

"Viewing the installation logs" on page 109
Viewing the installation logs can be useful for troubleshooting purposes.

Configuring remote Informix for reporting

If you have a non-root installation and are installing Informix on a different server than where the GUI components are installed, you must install the Informix IConnect software as root on the GUI components server to use Cognos reports.

To install Informix IConnect:

1. Log in to the server as root where you installed the GUI components (such as the Tivoli Integrated Portal server).
2. Install IConnect using the GUI (launchpad) or the command line interface:

Option	Description
Install Informix IConnect using the GUI (launchpad)	1. Go to the directory where you extracted the Network Manager installation package. 2. Start the launchpad as root using the **./launchpad.sh** command. 3. Select the **Postinstallation** menu. 4. Expand **Non-root postinstallation tasks (UNIX only)** and click **Install Informix IConnect**. 5. Provide the location where you installed Network Manager (the $NCHOME environment variable value), and wait for the command window to complete. This might take a few minutes.
Install Informix IConnect using the command line interface	1. Create the `informix` user and group. Refer to the platform-specific instructions for *Creating the Group informix and User informix* at the Informix information centre at the following URL:http://www-01.ibm.com/support/knowledgecenter/SSGU8G_11.50.0/com.ibm.start.doc/welcome.htm 2. Go to the directory where you extracted the Network Manager installation package. 3. Change to the following location: `scripts` 4. Run the installation command as follows: `./installConnect` 5. Follow the prompts for a typical installation into `NCHOME/platform/$ARCH/informix`.

Configuring permissions for WebTools on Solaris 10

On Solaris 10 you must set the net_rawaccess permission to enusre that all WebTools run correctly.

These library path and permissions settings primarily affect the ability of a non-root user to execute the Advanced Traceroute webtool.

1. As the root user, issue the `ppriv` command to display permissions. Here is an example of the output where the net_rawaccess permission is not set.

```
flags = <none>
E: all
I: basic
P: all
L: all
```

2. Issue the usermod command to set the net_rawaccess permission. For example, the following command sets the net_rawaccess permission for the itnmuser user.

```
usermod -K defaultpriv=basic,net_rawaccess itnmuser
```

Configuring GUIs

You can change the appearance and functionality of the Hop Views; update MIB information; and configure the presentation of events from unmanaged devices.

Administering the TopoViz client

You can customize the operations of the TopoViz client. This includes the display settings, for example device icons, the frequency of topology updates, and alert settings.

Changing Tivoli Integrated Portal timeouts

When you are working in the Tivoli Integrated Portal, your GUI session is subject to timeouts. You can change the timeout settings.

The Tivoli Integrated Portal provides the following default timeout settings:

Invalidation timeout
: If a user is logged into Network Manager using Tivoli Integrated Portal and closes the Tivoli Integrated Portal window, then the user session automatically times out after 30 minutes.

Lightweight Third Party Authentication (LTPA) timeout
: After a user is logged in for 24 hours, the Tivoli Integrated Portal login session is automatically closed down and the user is forced to log in again.

Changing the invalidation timeout setting:

If a user is logged into Network Manager using Tivoli Integrated Portal and closes the Tivoli Integrated Portal window, then, by default, the user session automatically times out after 30 minutes. This is known as the invalidation timeout. You can modify the invalidation timeout setting.

To change the invalidation timeout setting:

1. Log in to the server where the Network Manager GUI components are installed and edit the following file:

- UNIX `$TIPHOME/profiles/TIPProfile/config/cells/TIPCell/applications/isclite.ear/deployments/isclite/deployment.xml`
- Windows `%TIPHOME%\profiles\TIPProfile\config\cells\TIPCell\applications\isclite.ear\deployments\isclite\deployment.xml`

2. Within this file find the `invalidationTimeout` value. By default, this value is set to 30 minutes.
3. Set the `invalidationTimeout` to the required value in minutes.
4. Save the `deployment.xml` file.

Changing the Lightweight Third Party Authentication (LTPA) timeout setting:

After a user is logged in for a certain amount of time, by default 24 hours, the Tivoli Integrated Portal login session is automatically closed down and the user is forced to log in again. This is known as the Lightweight Third Party Authentication (LTPA) timeout. You can modify the LTPA timeout setting.

To change the LTPA timeout setting:

1. Click **Security** > **Secure administration, applications, and infrastructure**.
2. In the Secure administration, applications, and infrastructure window, click **Authentication mechanisms and expiration**.
3. Set the **Timeout value for forwarded credentials between servers** value as required. The default value is 1440 minutes (24 hours).
4. Click **OK**.

Features of the TopoViz client

Use this information to understand the features of the TopoViz client that can be customized.

TopoViz icons:

In a topology map, icons represent types of device or network elements. You can customize these icons.

The following icons can be customized:

- Device icons
- Tree and map icons

The following figure shows a representation of the tree and map icons:

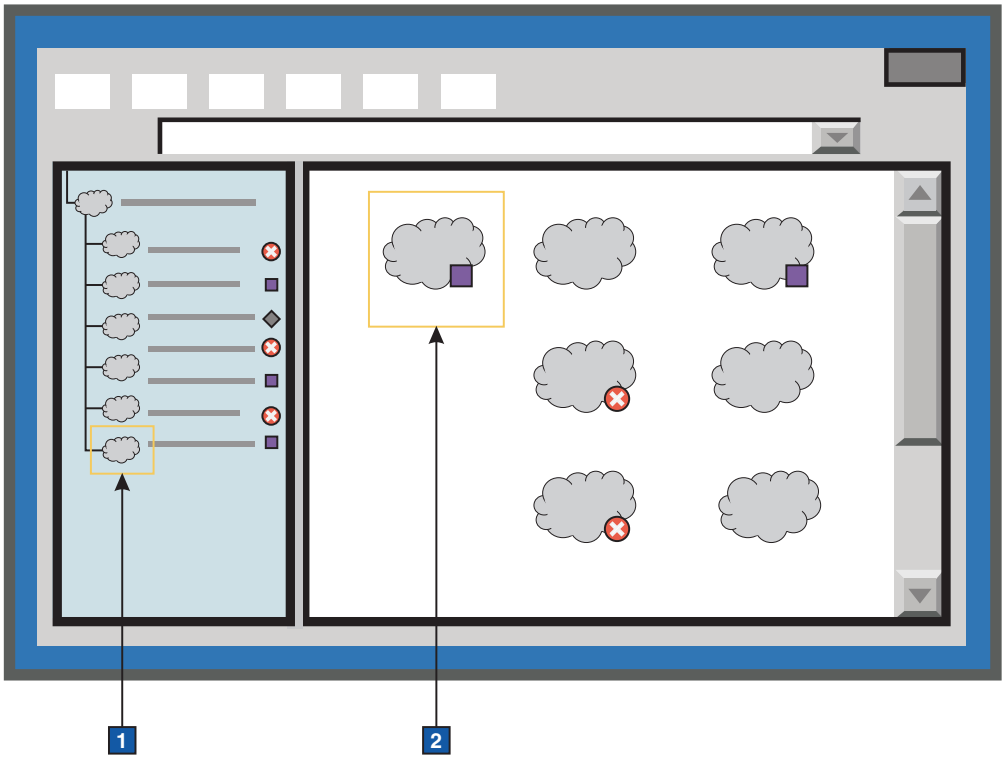

Figure 10. Tree and map icons

1 Tree icon
Used to represent views in the Navigation Panel. The default tree and map icons take the form of a cloud. Network operators can customize these icons when defining a new network view in the Network Views GUI. To do this, they choose from a list of predefined icons.

2 Map icons
Used to represent views in the Topology Display Panel.

Related tasks:

"Adding icons" on page 230
Make extra, custom icons available for network operators to choose from if they want to change the icons that they use in the Network Views and Network Hop View GUIs.

Related reference:

"Configuring the display of extra information associated with a device" on page 233
Information such as alert status and maintenance state of a device is displayed in a colored border around the device. You can configure the colors, icons, and positioning of the elements used to display this information.

Device class types:

All device class are automatically categorized by *class type*. In topology maps, each class type is represented by a different icon, whereas each device class is not.

Class types are stored in the NCIM topology database, in the classType field of the entityType table.

The following class types apply:

- Core
- End Node
- Network Device
- Router
- Switch

All the class types consist of device classes. For example, the Network Device class type contains the Alcatel and Cisco device classes.

Device ToolTips:

Device ToolTips appear when you roll your mouse over devices in topology maps.

Device ToolTips are defined by HTML entries in the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` configuration file on the server where the Network Manager GUI components are installed. You can specify the content of ToolTips associated with devices, subnets and links.

The `topoviz.properties` file is monitored every 60 seconds for changes, so that any changes are automatically detected by Topoviz.

Entries in the topoviz.properties file that control device ToolTips

The default settings for controlling device ToolTips are as follows:

`topoviz.tooltip.`*`map_item.entityType=HTML_statement`*

Where:

map_item
Takes one of the following values:
- `device`: For a chassis (main node device) or subnet ToolTip
- `link`: for a link ToolTip

entityType
Is the entityType number for a device, subnet, or link. It takes one of the following values:
- `1`: For a chassis (main node device) ToolTip
- `15`: For a subnet ToolTip
- `2`: For a link ToolTip

HTML_statement
Is any valid HTML code that is used to define the content and format of the ToolTip.

To insert the value from an NCIM topology database field use the following syntax: {*`table.field`*}

Example

The following example statement defines a ToolTip:

```
topoviz.tooltip.device.1=<b>{entity.displayLabel}</b><br><b>sysDescr</b> 
{chassis.sysDescr}<br><b>sysContact</b> {chassis.sysContact}
```

Changing icons in the Network Views and Network Hop View GUIs

You can change the icons that represent device classes, class types, trees, and maps to make them more recognizable to users when users view topology maps within the Network Views and the Network Hop View.

Adding icons:

Make extra, custom icons available for network operators to choose from if they want to change the icons that they use in the Network Views and Network Hop View GUIs.

To make custom tree and map icons available to network operators:

1. Create your icon. For best results, use the following formats:
   - For the tree icon: 16 by 16 pixel PNG, GIF, or JPG image
   - For the map icon: PNG, GIF, JPG, or SVG image of any size

   You need only supply one image, because Topoviz scales the icon as appropriate.
2. Copy your icon to the `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/` directory on the server where the Web Applications are installed.

Related concepts:

"TopoViz icons" on page 227
In a topology map, icons represent types of device or network elements. You can customize these icons.

Assigning icons to devices:

You can change the icons for devices and other entities used in topology maps displayed within the Network Views and Network Hop View GUIs..

Assigning icons to device classes:

To represent different device classes with different icons, assign each device class its own icon. This helps operators distinguish between device classes in topology maps, for example between Cisco and Alcatel devices.

Make custom icons available by adding icons as described in the related link.

To assign a custom icon to a device class:

1. Assign the icon prepared earlier to a class type by modifying the line that describes the icon to the `topoviz.properties` file, as follows:
   a. Edit the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` file.
   b. Find the section that specifies icon names for device types.
   c. Modify the relevant line of code as follows:

      ```
      topoviz.deviceicon.classname=iconname.extension
      ```

      Where

- *classname* is the name of the device class. This must correspond to the `active object` parameter within the AOC file that defines the class. AOC files are contained in the `$NCHOME/precision/aoc/` directory.
- *iconname* is the name of your icon.
- *extension* is the file extension.

2. Save the `topoviz.properties` file.

Related tasks:

"Adding icons" on page 230
Make extra, custom icons available for network operators to choose from if they want to change the icons that they use in the Network Views and Network Hop View GUIs.

Assigning icons to entity types:

Some network entities that display in the GUI are not devices and therefore do not have an associated class name. In order to be able to display an icon for these entities in the GUI, you can associate an icon to the related entity type to an icon.

Make custom icons available by adding icons as described in the related link.

To assign a custom icon to an entity type:

1. Assign the icon prepared earlier to a class type by adding a line that describes the icon to the `topoviz.properties` file, as follows:
   a. Edit the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` file.
   b. Find the section that specifies icon names for device types.
   c. Add the relevant line of code as follows:

      `topoviz.image.`*`entitytype=iconname.extension`*

      Where
      - *entitytype* is the entity type. This must exactly match the entity type name as listed in the NCIM `entityType` table. For more information on the `entityType` table, see the *IBM Tivoli Network Manager IP Edition Topology Database Reference*.
      - *iconname* is the name of your icon.
      - *extension* is the file extension.

2. Save the `topoviz.properties` file.

Related tasks:

"Adding icons" on page 230
Make extra, custom icons available for network operators to choose from if they want to change the icons that they use in the Network Views and Network Hop View GUIs.

Assigning icons to class types:

Change the icons that are used to represent class types to make it easier for network operators to identify the class types in topology maps. Class types group together more than one class. For example, you might want a single icon that represents the class type CiscoSwitch, where the CiscoSwitch class type groups together multiple Cisco switch class icons.

Make custom icons available by adding icons as described in the related link.

To assign a custom icon to a class type:

1. Identify the classes that make up your class type. For example, if you want a single icon for all Cisco switches (the Cisco switch class type), then identify each of the AOC files that represent individual Cisco switch classes.
2. Go to the directory that contains the active object class (AOC) files. AOC files define the device classes.

   ```
   cd $NCHOME/precision/aoc/
   ```
3. For each AOC file in your class type, modify the `visual_icon` parameter as follows:

   ```
   visual_icon = classtype;
   ```

   For example, in each Cisco switch AOC file, modify the `visual_icon` parameter as follows:

   ```
   visual_icon = CiscoSwitch;
   ```

   Restart the **ncp_class** process after changing AOC files. After **ncp_class** is restarted and running, restart the **ncp_model** process.
4. Assign the icon prepared earlier to a class type. For example, if you want to use a single icon for all Cisco switches (the Cisco switch class type), then edit the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` file, find the section that specifies icon names for device types and modify the relevant line of code as follows:

   ```
   topoviz.image.CiscoSwitch=my_icon.svg
   ```

   Where *my_icon* is the name of your custom icon file for the Cisco switch class type.
5. Save the `topoviz.properties` file.

Related tasks:

"Adding icons" on page 230
Make extra, custom icons available for network operators to choose from if they want to change the icons that they use in the Network Views and Network Hop View GUIs.

Configuring topology map updates and appearance

You can change the way devices and alert status are displayed in the topology maps. You can also modify frequency of updates to topology and alert status.

Appearance of nodes and lines in topology maps:

By default nodes, representing, for example, devices, and other network entities, always appear before the lines showing connections between the nodes. You can change this default setting, but this can make it difficult to view and interact with the nodes.

By default nodes overlay lines in a topology map. The setting that controls this option can be found in the following file: `$ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`. To locate this settings, search for the relevant section that begins with the comment `# Specifies whether nodes are drawn before edges`.

```
# Specifies whether nodes are drawn before edges
#    true => Edges overlay nodes
#    false => Nodes overlay edges
topoviz.graph.nodesBeforeEdges=false
```

By default the setting `topoviz.graph.nodesBeforeEdges` is set to false, which means that nodes always overlay lines in a topology map.

Changing the frequency of topology update checks:

TopoViz checks at regular intervals whether the topology shown in a network view has been updated. To change this frequency, change the topoviz.topologyupdateperiod value of the `topoviz.properties` file.

Any new nodes appear automatically in the topology maps; the new nodes are highlighted using handles.

The default frequency is 3600 seconds (60 minutes). You can change this to any value in seconds. If you set the topoviz.topologyupdateperiod value to `0`, Topoviz stops checking for updates to the topology.

To change the check frequency:

1. Open the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` configuration file and identify the following line:

   ```
   topoviz.topologyupdateperiod=3600
   ```

2. Change the frequency to the required value in seconds. Save and close the `topoviz.properties` file.

Configuring the display of extra information associated with a device:

Information such as alert status and maintenance state of a device is displayed in a colored border around the device. You can configure the colors, icons, and positioning of the elements used to display this information.

You control the display of extra information associated with a device using the settings in the following files:

- `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`
- `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties`

The settings that you can configure using these files include the following:

Managed status of device
: Icons that displays unmanaged and partially unmanaged status, position, and size of the icons.

Manually added device indication
Icon to indicate that this is a manually added device, position, and size of the icon.

Alert status of device
Whether to display an alert status icon, and if displayed, position of the alert status icon.

Frame around the device
Roundness of the corners of the frame around the device, height and width of the frame.

Device label text
Typeface, font size and font style of the device label text.

Example

The following figure shows a representation of a device display, showing a manually added device in unmanaged mode.

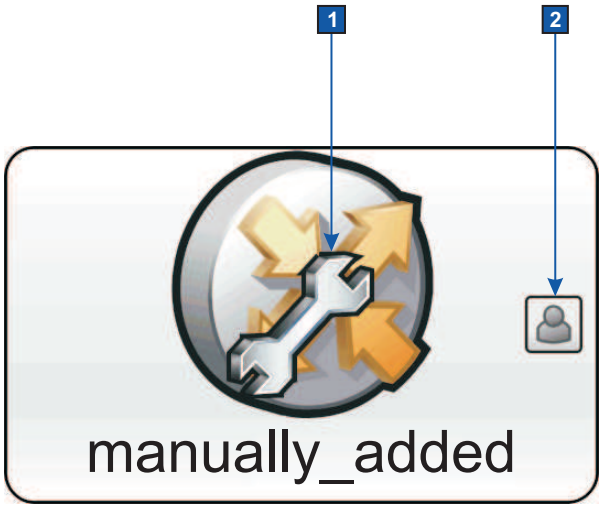

Figure 11. Representation of a device display, showing a manually added device in unmanaged mode

Configure the settings for the unmanaged status and manually added device icons as follows:

1 Unmanaged status icon, position, and size
The settings are specified in the `topoviz.properties` file. To locate these settings, search for the relevant section that begins with the comment `# Overlay definitions.`.

```
1]    # Overlay definitions.
2]    topoviz.overlay.image.UNMANAGED=unmanaged.svg
3]    topoviz.overlay.position.UNMANAGED=C
4]    topoviz.overlay.size.UNMANAGED=25
5]    topoviz.overlay.image.PARTIALMANAGED=partial_managed.svg
6]    topoviz.overlay.position.PARTIALMANAGED=C
7]    topoviz.overlay.size.PARTIALMANAGED=25
```

Table 19. Description of settings for the unmanaged status icons

Line	Description
2	Specifies the icon to use to indicate unmanaged status.
3	Specifies the position of the unmanaged status icon. The letter C means centered.
4	Specifies the size of the unmanaged status icon. The number is a relative value.
5	Specifies the icon to use to indicate partially unmanaged status.
6	Specifies the position of the partially unmanaged status icon. The letter C indicated centered.
7	Specifies the size of the partially unmanaged status icon. The number is a relative value.

2 Manually added device icon, position, and size

The settings are specified in the `topoviz.properties` file. To locate these settings, search for the relevant section that begins with the comment `# Overlay definitions.`.

```
1]    # Overlay definitions - Manual device
2]    topoviz.overlay.image.MANUAL=manualoverlay.svg
3]    topoviz.overlay.position.MANUAL=E
4]    topoviz.overlay.size.MANUAL=10
5]    topoviz.overlay.xoffset.MANUAL=-2
```

Table 20. Description of settings for the manually added device status icon

Line	Description
2	Specifies the icon to use to indicate a manually added device.
3	Specifies the position of the manually added device icon. The letter E means east of center.
4	Specifies the size of the manually added device icon. The number is a relative value.
5	Specifies x-axis offset of the icon. The East of center positioning in line 2 would place the icon so that it is touching the frame surrounding the device. The -2 offset value moves the icon slightly to the left, so that it is positioned just inside the frame.

Example

The following figure shows a representation of a device display, showing an associated critical alert.

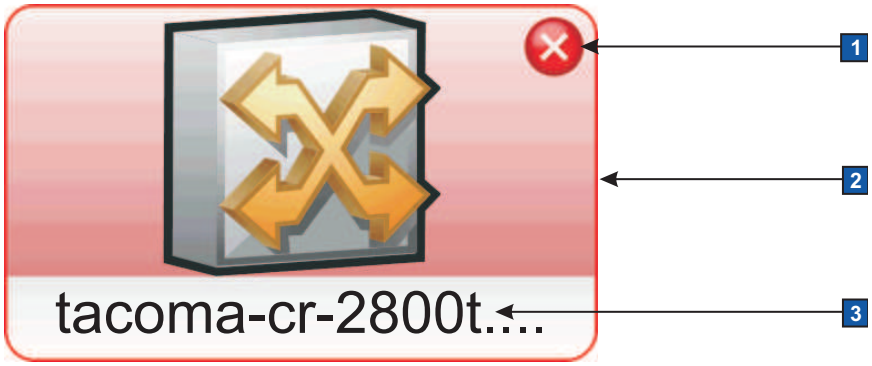

Figure 12. Representation of a device display, showing an associated critical alert

Configure the settings for the alert status icon, the device frame, and device label text as follows:

1 Alert status icon

The settings that control whether and where to display alert status icons in topology maps are as follows. Some settings are in the `topoviz.properties` file and others are in the `status.properties` file.

Whether to display alert status icons in the topology maps

The setting in the `status.properties` file that instructs the system to display alert status is `status.enabled=true`.

Position

The setting in the `topoviz.properties` file that specifies the position of the alert status icon.is `topoviz.status.position=NE`. This instructs the system to place the alert status icon in the north east (top right) corner of the frame containing the device.

2 Device frame

The settings are specified in the `topoviz.properties` file. To locate these settings, search for the sections that begins with the comment `# Node dimensions` and `# Corner arc`.

```
1]    # Node dimensions (not used in legacy mode).
2]    topoviz.node.height=60
3]    topoviz.node.width=100
4]
5]    # Node resizability
6]    # Options: LOCKED (Fixed height and width)
7]    #   TIGHT_HEIGHT (Fixed height, variable width)
8]    topoviz.node.resizeability=TIGHT_HEIGHT
9]
10]   # Corner arc (not used in legacy mode).
11]   topoviz.node.arc=10
```

Table 21. Description of settings for the device frame

Line	Description
2	Specifies the height of the frame.
3	Specifies the width of the frame. **Note:** There is no wrapping of text for the device label, so if you want to show all of the device label text you must either increase this width value or decrease the text font size using the **topoviz.node.fontsize** setting.
8	Specifies how the **topoviz.node.height** and **topoviz.node.width** settings are handled. The default is `TIGHT_HEIGHT`. Using `LOCKED` means the values set in the **topoviz.node.height** and **topoviz.node.width** parameters are used for the device frame. Using `TIGHT_HEIGHT` maintains the **topoviz.node.height** setting, but does not maintain the **topoviz.node.width** setting, which means the device frame is automatically widened as necessary to accommodate the device label while keeping the width to the minimum.
11	Specifies the roundness of the corners of the frame. The higher the value, the more rounded the corners.

3 Device label

The settings are specified in the `topoviz.properties` file. To locate these settings, search for the relevant section that begins with the comment `# Font settings`.

```
1]    # Font settings
2]    topoviz.node.font=Arial,Helvetica
3]    topoviz.node.fontsize=10
4]    topoviz.node.fontstyle=0
```

Table 22. Description of settings for the device label text

Line	Description
2	Specifies the typeface to use for the device label text.
3	Specifies the font size to use for the device label text.
4	Specifies the font style to use for the device label text.

Related concepts:

"TopoViz icons" on page 227
In a topology map, icons represent types of device or network elements. You can customize these icons.

Related tasks:

"Changing alert settings" on page 238
If required, you can change the settings for alerts. You can change the frequency of updates to alert severity information, replace the default icons that represent alert severity, configure how alert status is retrieved, and configure other alert settings.

Configuring position of nodes in Network Views after rediscovery:

You can configure how newly discovered and existing nodes are positioned in the network views after a rediscovery of the network.

By default, the TopoViz client changes the layout of a network view map as newly discovered nodes are added to the map. The position of existing nodes is not guaranteed when the map layout is updated because the layout is governed by factors such as connectivity information obtained during the discovery.

To change the default behavior and configure Network Manager to maintain the position of existing nodes and visually separate new nodes from nodes already present in the network views, edit the following parameters.

Note: This behavior works best with the **Symmetric Layout**. Other layout options take other factors into account which can affect the position of existing nodes. For example, the **Circular Layout** places greater emphasis on presenting nodes in a circular layout than maintaining node positions, while the **Hierarchical** and **Orthogonal** layouts place greater emphasis on routing the connections between nodes using orthogonal lines than maintaining exact node positions.

1. Go to `NCHOME/precision/profiles/TIPProfile/etc/tnm` and open the `topoviz.properties` file.
2. Locate the **`topoviz.node.freezeold`** parameter and change the value to `true` (the default value is `false`).

   The `true` setting maintains the position of existing nodes, while new nodes are placed in a row at the top of the map, clearly separating the new nodes from nodes not added during the last rediscovery. The new nodes are placed in one or more rows at the top of the map with a horizontal and vertical spacing of 20 pixels by default.
3. Log out of the Network Manager GUI and restart the browser. This is required for the `true` setting to take effect.

4. Optional: You can further adjust the positioning of new nodes using the following parameters in the `topoviz.properties`:
   - You can set whether the new nodes are placed at the top or bottom of the map using the **`topoviz.node.new.placement`** parameter. The default setting is `top`, change it to `bottom` to have the new nodes placed at the bottom of the network view map.
   - You can set the horizontal spacing between new nodes in pixels using the **`topoviz.node.new.spacing.horizontal`** parameter. The default setting is `20` pixels, change it to a different pixel count to position each new node closer to each other or further apart horizontally.
   - You can set the vertical spacing between new nodes in pixels using the **`topoviz.node.new.spacing.vertical`** parameter. The default setting is `20` pixels, change it to a different pixel count to position each new node closer to each other or further apart vertically.

   Note: All additional settings discussed in this step only take effect if the **`topoviz.node.freezeold`** is set to `true`.

Changing alert settings:

If required, you can change the settings for alerts. You can change the frequency of updates to alert severity information, replace the default icons that represent alert severity, configure how alert status is retrieved, and configure other alert settings.

Related reference:

"Configuring the display of extra information associated with a device" on page 233

Information such as alert status and maintenance state of a device is displayed in a colored border around the device. You can configure the colors, icons, and positioning of the elements used to display this information.

Changing the frequency of alert severity updates:

If required, change how often the alert severity information is updated from the Tivoli Netcool/OMNIbus Web GUI.

To change the frequency with which the alert severity is updated:

1. On the server where the Web Applications are installed, open the `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties` file.
2. Make the following changes:
   - To change the frequency of alert severity updates in the network view tree, change the value of the `status.tree.updateperiod` property. The value is in seconds. For example:

     ```
     status.tree.updateperiod=60
     ```
   - To change the frequency of alert severity updates in the topology map, change the value of the `status.map.updateperiod` property. The value is in seconds. For example:

     ```
     status.map.updateperiod=60
     ```
3. Save and close the file.

Changing the icons for alert severity levels:

You can change the alert status icons used to represent alert severity levels in the network view tree, topology map, and the topology tabular layout.

Changing icons for alert severity levels in the network view tree and topology map:

If you want different alert status icons to represent alert severity levels in the network view tree and topology map, replace the default icons.

The required formats for replacement icons are as follows:

- For the network view tree: GIF or PNG files.
- For the topology map: GIF, PNG, or SVG files.

GIF or SVG files.

To replace a default icon:

1. Create the image for the security icon that you want to replace and copy the image to `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/`.
2. Open the `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties` file and make the following changes.
   a. In the `Tree status images` section of the files, point the property for the required severity to the new image. For example, to replace the default `critical.gif` file for severity level 5 with your own new image:
      `status.tree.image.5=status/<filename for new critical icon>.gif`
   b. In the `Map status images` section of the files, point the property for the required severity to the new image. For example, to replace the default `critical.gif` file for severity level 5 with your own new image:
      `status.map.image.5=status/<filename for new critical icon>.gif`
3. Repeat the steps for each default icon that you want to replace.
4. Save and close the file.

Changing icons for alert severity levels in topology map tabular layout:

If you want different alert status icons to represent alert severity levels in the topology map tabular layout option, replace the default icons.

The required formats for replacement icons for the topology map table view are GIF or PNG files.

To replace a default icon:

1. Create the image for the security icon that you want to replace and copy the image to `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/`.
2. Open the `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties` file and in the `Net View Table status images` section of the files, point the property for the required severity to the new image. For example, to replace the default `ac16_critical04_24.gif` file for severity level 5 with your own new image:
   `status.table.image.5=status/<filename for new critical icon>.gif`
3. Repeat the steps for each default icon that you want to replace.
4. Save and close the file.

Configuring on-demand AEL filters for the Network View tree:

When you click on an alert status icon in the Network View tree, a filtered AEL is displayed. You can configure the Network View tree to define these filters on demand, which uses less memory.

Configuring AEL filters to be defined for all Network Views in the Network View Tree uses a large amount of heap memory, especially with deep, highly structured navigation trees with a large number of parent views, and might cause performance issues.

You can configure the Network View tree to define AEL filters for only the Network View that is currently displayed. Defining filters on demand uses less memory. By default, on-demand filtering is disabled and filters are created for all views when the Network View tree is displayed.

Filters are always created for the leaf nodes in the Network View Tree. Leaf nodes are Network Views (not containers) that do not themselves contain other Network Views. Aggregated alert status is shown for all nodes in the Network View tree regardless of whether on-demand AEL filters are enabled or not.

To configure on-demand AEL filters in the Network View tree, complete the following steps:

1. On the server where the Web Applications are installed, back up and edit the `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties` file.
2. Make the following changes:
   - To enable on-demand AEL filters in the Network View tree, change the value of the status.tree.filterael property to false. AEL filters are created only when you open a Network View. When you open an AEL from a parent Network View in the Network View tree that has not been opened in the topology display pane, the AEL shows events for all devices. If you click on the Network View, and then launch an AEL from that view, the AEL is filtered to show events on only those devices in that view.
   - To disable on-demand AEL filters in the Network View tree, change the value of the status.tree.filterael property to true. AEL filters are created for every view in advance. When you open an AEL from any Network View, the AEL is filtered to show events on only those devices in that view.
3. Save and close the file.

Alert status settings:

The alert status settings control whether and how devices are displayed in topology maps, and the frequency with which the settings are updated.

The alert status settings are in the `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties` file. The following table describes the properties. Where multiple properties exist that control a setting for each possible alert severity, a single property is given with an asterisk (*). For example, **`status.color.background.*`** refers to the **`status.color.background.unknown`**, **`status.color.background.nonw`**, and **`status.color.background.0`** to **`status.color.background.5`** properties.

Table 23. Alert status settings

Setting	Description
status.color.background.*	Specifies background status color for each severity .
status.color.foreground.*	Specifies the color of the device label text for each severity .
status.enabled	Specifies whether the device status is displayed in topology maps.

status.globalfilter	Filters certain alerts from the status display of devices in the topology maps. This property filters on the `alerts.status` table of the ObjectServer.
	
	The following example prevents ping fail events from affecting the displayed status of devices in the topology:
	`status.globalfilter=EventId<>' NmosPingFail'`
	
	The following example displays the status of only those devices in the topology views that have associated events with `EventId ='NmosPingFail'`:
	`viewsstatus.globalfilter=EventId= 'NmosPingFail'`
	
	The following example displays status of devices in the topology views that have associated events with `Severity` of `Minor`, `Major` or `Critical`:
	`status.globalfilter=Severity>2`

status.hopview.linestyle	Indicates whether to display the alert status on links between nodes in the Hop View.
status.map.updateperiod	Specifies how often the system updates the alerts status settings in the topology maps.
status.map.maxnodes	Indicates the maximum number of nodes for which alert status can be displayed in a single topology map.
status.map.image.*	Specifies which icons represent device alert status in the topology map. To change these icons, create a `.gif` or `.svg` file with the relevant name and save it to `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/`.
status.map.image.size.*	Specifies the size of the icons that represent device alert status in topology maps.
status.map.image.xoffset.* **status.map.image.yoffset.***	Specifies the x-axis and y-axis offset of the icon. The NE (northeast) positioning that is specified in the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` file puts the icon so that it is touching the frame that surrounds the device. The offset values move the icon down and to the left so that it is positioned inside the frame.

Table 23. Alert status settings (continued)

Setting	Description
status.map.topcolor.saturation.* **status.map.bottomcolor.saturation.*** **status.map.topcolor.brightness.*** **status.map.bottomcolor.brightness.***	Specifies the saturation and brightness adjustment controls that control the gradient of the background status color for each alert severity level.
status.netview.linestyle	Indicates whether to display the alert status on links between nodes in the Network Views.
status.none.enabled	Indicates whether the None status for a device is represented in the same way as the clear status. **Tip:** The None status means that no events were received for the device. The clear status means that earlier events of severity 1 or greater are cleared on the device.
status.pathview.linestyle	Indicates whether to display the alert status on links between nodes in the Hop View. Also applies to MPLS TE and IP Paths.
status.registration.devicealert	Set this property to `true` to include alerts from devices in the alert status of views that are based on device components. For example, if you have an MPLS view that includes only interfaces, you might want to exclude alerts from the chassis of the devices containing those interfaces. To exclude alerts from the main nodes, set this property to `false`.
status.table.image.*	Specifies which icons represent device alert status in the topology map tabular layout. To change these icons, create a `.gif`or `.svg` file with the relevant name and save it to `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/`.
status.table.image.sortUp **status.table.image.sortDown**	Specify how to sort alert severity icons in the topology map tabular layout.
status.tree.filterael	To enable on-demand Active Event List (AEL) filters in the Network View tree, change the value of the **status.tree.filterael** property to `false`. When you open an AEL from a parent Network View in the Network View tree that was not opened in the topology display pane, the AEL shows events for all devices. If you click the Network View, and then launch an AEL from that view, the AEL is filtered to show events on only those devices in that view. Enabling on-demand filters uses less heap memory. To disable on-demand AEL filters in the Network View tree, change the value of the **status.tree.filterael** property to `true`. When you open an AEL from any Network View, the AEL is filtered to show events on only those devices in that view.

Table 23. Alert status settings (continued)

Setting	Description
status.tree.updateperiod	Specifies how often the system updates the alerts status settings in the Network Views and Structure Browser navigation pane.
status.tree.image.*	Specifies which icons represent device alert status in the network view tree. To change these icons, create a `.gif` or `.svg` file with the relevant name and save it to `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/`.

Configuring visual differentiation between manually added and discovered devices:

You can configure the topology views to highlight manually added devices in the topology map using an overlay icon.

To configure the system to highlight manually added devices:

1. Edit the following file: `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`.
2. Within this file check the `topoviz.topologymanagement.differentiate_manual` value.
   - `topoviz.topologymanagement.differentiate_manual=true`: configures manually added devices and connections to be differentiated from discovered devices and connections.
   - `topoviz.topologymanagement.differentiate_manual=false`: manually added devices and connections are not differentiated from discovered devices and connections.

   By default, this value is set to `true`.
3. If the setting is `topoviz.topologymanagement.differentiate_manual=true`, then check the overlay image configuration for differentiation of manually added nodes.

   ```
   # Overlay definitions - Manual device
   topoviz.overlay.image.MANUAL=manualoverlay.svg
   topoviz.overlay.position.MANUAL=E
   topoviz.overlay.size.MANUAL=10
   topoviz.overlay.xoffset.MANUAL=-2
   ```

   This configuration snippet contains the following settings:
   - The overlay image used for is called `manualoverlay.svg`. This file is located at `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/`. You can change the overlay image used by copying a different .svg icon to `ITNMHOME/profiles/TIPProfile/etc/tnm/resource/manualoverlay.svg`.
   - By default, the icon appears to the right (E stands for east) of the manually added device. Other options are N, S, W, NE, NW, SW, SEand C, where C means centred on the device.
4. Save the `topoviz.properties` file.

Switching to V3.8 visualization mode:

Topology icons and the way they are presented have changed in V3.9 from previous versions. Use this information if you want to switch back to the V3.8 mode of topology presentation.

To switch back to the V3.8 mode of topology presentation you must edit the following configuration files:

- `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`
- `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties`

1. Open the file `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties`.
2. Search for the text `legacy`.
3. Each time the text `legacy` is found, follow the instructions in the comments.
4. Save the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` file.
5. Open the file `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties`.
6. Search for the text `legacy`.
7. Each time the text `legacy` is found, follow the instructions in the comments.
8. Save the `ITNMHOME/profiles/TIPProfile/etc/tnm/status.properties` file.

Loading updated MIB information

To ensure that the MIB browser reflects the most up-to-date MIB information, load updated MIB information by running the **ncp_mib** command-line application.

You need to run the ncp_mib command-line application only when new MIBs are added to the `NCHOME/precision/mibs` directory. It is run once during installation, so if you do not add new MIBs, you do not need run it again.

Important: You must run ncp_mib if you are migrating data to a new version of Network Manager and have copied over custom MIBs as part of this data migration. If you do not do this then processes such as the SNMP helper, ncp_dh_snmp, will not start up when you start Network Manager.

Important: All MIBs must be valid in order to be parsed correctly. The ncp_mib command is case-sensitive and expects a suffix of .mib (not .MIB). The prefix can be a combination of upper or lower case.

When run, **ncp_mib** populates the ncmib schema in the NCIM database to provide a central store of all MIB information that Network Manager can query. The ncmib schema within the NCIM database is defined in `NCHOME/etc/precision/MibDbLogin.cfg`; the default value is `MIB`.

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.

In a distributed installation, ncp_mib is installed on the Tivoli Integrated Portal server, that is, on the same server as the Network Manager Web applications.

If your MIB database gets corrupted or if you want to import a new MIB that conflicts with one that was imported previously, note the various command-line options by running **ncp_mib -help**. For more information on the ncp_mib command-line option, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Tip: If you are uncertain what the result will be of running **ncp_mib**, run it with the **-dryrun** option. You can see the results, but the database will not be altered.

To update the MIB information, complete the following steps on the server where the Tivoli Integrated Portal is installed.

1. Copy any new MIB files to the NCHOME/precision/mibss directory.
2. Ensure that the database login credentials are correct.

   The only configuration parameters required for the ncp_mib command-line application are the database login credentials for the ncim database. These are stored in a configuration file, NCHOME/etc/precision/MibDbLogin.cfg. Note that because **ncp_mib** is domain-independent, this file does not have domain-specific variants as other configuration files do.
3. Start the **ncp_mib** process by issuing the **ncp_mib** command.

To verify that a MIB has successfully loaded, query the database table ncmib.mib_modules by entering the following command from the NCIM database prompt (this example assumes that NCIM 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.

Tip: For information on using the SNMP MIB Browser and graphing MIB variables, see the *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*.

Configuring the presentation of events from unmanaged devices

You can configure the way events from unmanaged devices (devices that are not polled by Network Manager) are presented to network operators.

You can configure Network Manager to present unmanaged events in the **AEL** in the following ways:

- Filtering out the unmanaged events so that they do not appear at all in the **AEL**, or tagging these events in the **AEL** so that you know that they come from unmanaged devices.
- Tagging these events in the **AEL** so that the network operator knows that they come from unmanaged devices. In this case, the NmosManagedStatus field associated with an unmanaged event in the **AEL** displays the value 1 (Operator unmanaged) or 2 (System unmanaged).

Tivoli Netcool/OMNIbus probes and event sources from other network management systems can generate events on devices or interfaces that have been marked as Unmanaged in Network Manager. An unmanaged device is usually marked Unmanaged because it is undergoing maintenance and may therefore

generate unnecessary network events. The following topics describe how to manage network events from an unmanaged device.

Remember: Unmanaged devices are shown in the network map with an overlaid double-ended wrench icon. Partially unmanaged devices (devices in which only certain interfaces are unmanaged) are shown in the network map using an overlaid single-ended wrench icon.

Filtering out events from unmanaged devices

You can filter events from unmanaged devices so that they do not appear in the **AEL**.

1. In the **AEL**, select the **Filter Builder**.
2. Create a new filter or edit the existing filter to filter out all events where the NmosManagedStatus field is equal to 1 (Operator unmanaged) or 2 (System unmanaged).

Once you have completed this operation and applied the filter to the **AEL**, events from unmanaged devices no longer appear in the **AEL**.

Tagging events from unmanaged devices

You can tag events in the **AEL** so that you know that these events come from unmanaged devices.

1. In the **AEL**, select the **View Builder**.
2. Create a new view or edit the existing view to display the NmosManagedStatus field associated with an event. This field displays the managed status of the device or interface the event was raised for. For unmanaged devices, this field displays the value 1 (Operator unmanaged) or 2 (System unmanaged).

Once you have completed this operation and applied the view to the **AEL**, each event in the **AEL** will display the managed status of the associated network device or interface.

Configuring Tivoli Common Reporting

Network Manager uses Tivoli Common Reporting as a reporting tool. Perform the following tasks to configure Tivoli Common Reporting to run Network Manager reports.

Restriction: You can choose to configure Tivoli Common Reporting 2.x on the local machine, but be aware that Tivoli Common Reporting 2.x does not support Internet Explorer versions 10 or 11. Consequently, you cannot use the reporting feature if you are using Internet Explorer 10 or 11 for the Network Manager GUI. Alternatively, you can install Tivoli Common Reporting 3.1 remotely; Tivoli Common Reporting 3.1 provides full browser coverage.

Restriction: Tivoli Common Reporting 3.1 is available for Netcool Operations Insight users only.

Configuring Tivoli Common Reporting 2.x

Perform these tasks to configure Tivoli Common Reporting 2.x. Note that Tivoli Common Reporting 2.x does not support Internet Explorer versions 10 or 11. Consequently, you cannot use the reporting feature if you are using Internet Explorer 10 or 11 for the Network Manager GUI.

Configuring reports for existing installations

You can configure the network management reports provided by Network Manager to use with Tivoli Common Reporting.

To enable network management reports, you must have Tivoli Common Reporting installed. If you installed Network Manager GUI components on a machine where Tivoli Common Reporting was already present, then you do not need to complete these steps.

To configure network management reports:

1. Log into the machine where you have Network Manager GUI components and Tivoli Common Reporting installed.
2. Run the script to configure network management reports either from the installer launchpad or the command line:

Option	Description
From the launchpad	1. Go to the directory where you extracted the Network Manager installation package. 2. Start the launchpad as the user that installed Network Manager by entering the **./launchpad.sh** command. 3. Select the **Postinstallation** menu. 4. Expand **Install Network Manager reports to use with TCR** and click **Install Network Manager reports**.
From the command line	1. Go to the `NCHOME/precision/products/tnm/bin` directory. 2. Run the `configTCR.sh -d` *`NCIM_database_password`* `-p` *`TIP_administrator_password`* `-i install` script. 3. Oracle When using an Oracle RAC setup, or when using a service name to connect to the database, also add the `-s` *`Oracle_service_name`* option to define the JDBC URL for accessing the database. The `-s` option is required to configure the BIRT data source to be able to access the database using the service name. **Note:** You must use the command line in such cases. The launchpad does not provide the option to use the `-s` value.

Configuring data sources for BIRT

Fix Pack 5

If you use reports based on the BIRT data model, you must configure data sources. 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 the datasources `NCIM`, `PARAMETERS` and `NCPOLLDATA` to point to the NCIM database.

If you are using Tivoli Data Warehouse, configure the datasources `NCIM` and `PARAMETERS` to point to the NCIM database, and `NCPOLLDATA` to point to the Tivoli Data Warehouse database. Obtain the database and connection details from the database administrator before starting this task.

Tip: The reference documentation for each report shows you whether a particular report uses the BIRT or Cognos data model.

To configure the data sources for all reports based on the BIRT data model, complete the following steps.

1. If Tivoli Common Reporting is installed on the same server as Network Manager, configure the datasources `NCIM`, `PARAMETERS` and `NCPOLLDATA` to point to the NCIM database. Run the `configTCR.sh` script with a command similar to the following command: UNIX

   ```
   $NCHOME/precision/products/tnm/bin/configTCR.sh -d NCIM_database_password
    -p TIP_administrator_password
   ```

   The following table describes the command line options:

Table 24. configTCR command-line options

Command-line option	Description
`-d`	The password for the NCIM database user name. This could be on the local machine or on a remote host.
`-p`	The password for the Tivoli Integrated Portal administrator.
`-i` *install*	Specifies that the network management reports are installed. You must use the **`install`** parameter in all cases after option `-i`.
Oracle `-s` *Oracle_service_name*	When using an Oracle RAC setup, or when using a service name to connect to the database, use this option followed by the *Oracle_service_name* to define the JDBC URL for accessing the database. The `-s` option is required to configure the BIRT data source to be able to access the database using the service name.
`-t` *path_to_TIPHOME*	If you do not have TIPHOME set or you have not run the env.sh script, then you can define where your Tivoli Integrated Portal instance is installed.

Table 24. configTCR command-line options (continued)

Command-line option	Description
`-r` *path_to_reports_package*	If your Network Manager installation has the reports package in a non-default location, you can define where the package is using this option.
`-u` *NCPOLLDATA_user_name*	On some databases, such as Oracle, you might have different user names for the NCIM and the NCPOLLDATA database. You must specify both user names if you have separate ones. Use this option to provide the NCPOLLDATA user name.
`-v` *NCPOLLDATA_password*	If you set the NCPOLLDATA user name, you must set its password using this option.
`-e` *NCIM_user_name*	On some databases, such as Oracle, you might have different user names for the NCIM and the NCPOLLDATA database. You must specify both user names if you have separate ones. Use this option to provide the NCIM user name. The `-d` defines the password for this user.

2. If Tivoli Common Reporting is installed on a different server to Network Manager, configure the datasources `NCIM`, `PARAMETERS` and `NCPOLLDATA` to point to the NCIM database. Run the `configRemoteTCR.sh` script with a command similar to the following command: UNIX

```
$NCHOME/precision/products/tnm/bin/configRemoteTCR.sh -b database_name
-d NCIM_password -e NCIM_username -h
database_hostname  [-i install] -j tip_admin_username
 -n database_port -p tip_admin_password
[-r PackagesDirectory] [-s Oracle_service_name]
 -t $TIP_HOME -z database_type
```

Restriction: The `configRemoteTCR.sh` script is available in versions of Network Manager starting from V3.9 Fixpack 5.

The following table describes the command line options for the **`configRemoteTCR`** script.

Table 25. configRemoteTCR command-line options

Command-line option	Description
`-b` *database_name*	The NCIM DB2 database name or NCIM Oracle service name.
`-d` *NCIM_password*	The password for the NCIM database user name. The NCIM database can be on the local server or on a remote host.
`-e` *NCIM_user_name*	On some databases, such as Oracle, you might have different user names for the NCIM and the NCPOLLDATA database. You must specify both user names if you have separate ones. Use this option to provide the NCIM user name. The `-d` defines the password for this user.
`-h` *database_hostname*	The host name of the NCIM database.

Table 25. configRemoteTCR command-line options (continued)

Command-line option	Description
`-i` *install*	Specifies that the network management reports are installed. You must use the **`install`** parameter in all cases after option `-i`.
`-j` *Jazz_SM_admin_username*	The user name of the Jazz for Service Management administrative user.
`-n` *database_port*	The port of the NCIM database.
`-p` *Jazz_SM_admin_password*	The password for the Tivoli Integrated Portal administrator.
`-r` *path_to_reports_package*	If your Network Manager installation has the reports package in a non-default location, you can define where the package is using this option.
Oracle `-s` *Oracle_service_name*	When you use an Oracle RAC setup, or a service name to connect to the database, use this option followed by the *Oracle_service_name* to define the JDBC URL for accessing the database. The `-s` option is required to configure the BIRT data source to be able to access the database by using the service name.
`-t` *JazzSM_HOME*	The location where Jazz for Service Management is installed.
`-z` *database_type*	The database server type. Can be `db2`, `informix`, or `oracle`.

3. If you are using Tivoli Data Warehouse, configure the datasources `NCPOLLDATA` to point to the Tivoli Data Warehouse database.
   a. Change to the following directory (the following path is the default location):`/opt/IBM/tivoli/tipv2Components/TCRComponent/bin`.
   b. 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. Use NCPOLLDATA to configure the connection to Tivoli Data Warehouse. Other allowed values are:
     – NCIM for reports using topology information.

– PARAMETERS for reports using the NCPOLLDATA database or the NCPOLLDATA schema for report parameters.

- *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=Y;IFX_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 the NCPOLLDATA data source to Tivoli Data Warehouse

DB2 example command

The following command configure the NCPOLLDATA data source for historical reporting to use Tivoli Data Warehouse running 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
```

Oracle example command

The following command configure the NCPOLLDATA data source for historical reporting to use Tivoli Data Warehouse running on Oracle.`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
```

Related tasks:

"Migrating 3.8 reports" on page 145
If you have modified or created reports in Network Manager 3.8, you must migrate those reports manually.

Migrating the Cognos content store from Derby to DB2 or Oracle

The default content store database that is used by Cognos is suitable for demonstration purposes, but it is not to be used as the content store database in a production environment. If you use network management reports with Tivoli Common Reporting, you have the option of migrating the content store database from the default Derby database to DB2 or Oracle. Network Manager uses the database set up in Tivoli Common Reporting for the Cognos content store. If you have already changed your Tivoli Common Reporting setup to use another database other than the default Derby database, you might not need to perform this task.

For more information about the default Derby database and the alternative content store databases for Tivoli Common Reporting, see the following technote: http://www-01.ibm.com/support/docview.wss?uid=swg21609287.

You need to perform the following steps to switch to DB2 or Oracle for the Cognos content store regardless of whether you are installing Network Manager on a server with an existing Tivoli Common Reporting installation, or you are installing Tivoli Common Reporting on a server with existing Network Manager GUI and Tivoli Integrated Portal components already installed. This is because any installation of Tivoli Common Reporting uses Derby by default, and you need to change to DB2 or Oracle manually.

To migrate the Cognos content store from the default Derby database to DB2 or Oracle, complete the following steps. Ensure that you follow each step unless the step is highlighted to be specific to a database, in which case only follow the steps for the database of your choice.

1. Log in to the Network Manager GUI as the itnmadmin user and export the content store data as described in http://www.ibm.com/support/knowledgecenter/SSEP7J_8.4.0/com.ibm.swg.im.cognos.inst_cr_winux.8.4.1.doc/inst_cr_winux_id3024c8bi_CreateAnExportDeploymentSpecif.html.

   Note: When clicking **Select the entire content store** to export the entire content store, ensure you select to include user account information.

2. Create the database for your Cognos content store. Follow the appropriate steps depending on your database type:

Option	Description
To use DB2 for your Cognos content store:	DB2 1. Log in as the user that created the Network Manager database. In this example 'db2inst1': `su - db2inst1` 2. Source the DB2 environment variables: `. sqllib/db2profile` 3. Create the Cognos database using the following Network Manager script, calling out the database user, in this case 'ncim': a. Go to `$NCHOME/precision/scripts/sql/db2`. b. Type `./create_db2_cognos_database.sh` *`database_name user_name`*, where *database_name* is the required name of the Cognos content store database, and *user_name* is the DB2 user that is used to connect to the database. For example, to create a database called ITNMCM for the DB2 user ncim, type `./create_db2_cognos_database.sh ITNMCM ncim`. **Note:** If your DB2 database is on a different server to Network Manager, then copy the script to the server where your database is located and run the script there.
To use Oracle for your Cognos content store:	Oracle Create a new Oracle database for Cognos reports with character set AL32UTF8 or AL32UTF16 as described in the Cognos page "Guidelines for Creating the Content Store". **Note:** You only need to create the database at this stage. The database schema is then created when you start Cognos later.

The Cognos page "Guidelines for Creating the Content Store" can be found at the following location: http://www.ibm.com/support/knowledgecenter/SSEP7J_10.1.0/com.ibm.swg.im.cognos.inst_cr_winux.10.1.0.doc/inst_cr_winux_id2792CreatetheContentStore.html

3. As the user who installed Network Manager, configure the content store data source access using the following Network Manager script:
   a. Source the environment variables:
      `. /opt/IBM/tivoli/netcool/env.sh`
   b. Go to `$NCHOME/precision/products/tnm/bin`.
   c. Type `./modify_cognos_cm -filename` *`full path to file`* `-dbname` *`DB2_database_name or Oracle_SID_instance or Oracle_service_name`*

(Oracle RAC only) -dbport *port_number* -dbhost *host_name* -dbtype db2 -username *user_name* -password *password* .

DB2 For example, use a command line similar to the following for DB2: UNIX

```
$NCHOME/precision/products/tnm/bin/modify_cognos_cm -filename
TCR_installation_directory/cognos/configuration/cogstartup.xml
 -dbname ITNMCM -dbport 50000 -dbhost abc
 -dbtype db2 -username db2inst1 -password password
```

Oracle For example, use a command line similar to the following for Oracle: UNIX

```
$NCHOME/precision/products/tnm/bin/modify_cognos_cm -filename
TCR_installation_directory/cognos/configuration/cogstartup.xml
 -dbname ITNM411 -dbport 1521 -dbhost abc
 -dbtype oracle -username oracleadmin -password password
```

d. Oracle When using an Oracle RAC setup, or when using a service name to connect to the database, use the **./tcr_cogconfig.sh** script in $NCHOME/../tipv2Components/TCRComponent/cognos/bin to create an advanced Oracle database data source. Use a connection string similar to the following:
(description=(address=(host=myhost)(protocol=tcp)(port=1521)
(connect_data=(service_name=(orcl)))))

For more information about data source configuration, see http://www.ibm.com/support/knowledgecenter/SSEP7J_8.4.0/com.ibm.swg.im.cognos.inst_cr_winux.8.4.0.doc/inst_cr_winux_id7376UninstallCognosContentDatabase.html.

4. Oracle When using Oracle as the content manager, edit the following file. This is required to solve a known issue with ojdbc6.jar not being loaded by cognos.
   a. Open $NCHOME/../tipv2Components/TCRComponent/cognos/bin64/cogconfig.sh for editing.
   b. Locate the following string: CLASSPATH=.:../bin/cclcfgmcf_mcf.jar:cogconfig.jar
   c. Add the following to the end: :../webapps/p2pd/WEB-INF/lib/ojdbc6.jar

   The following example shows the CLASSPATH string with the addition at the end:

```
CLASSPATH=.:../bin/cclcfgmcf_mcf.jar:cogconfig.jar:../bin/
cogconfigi.jar:../bin/dom4j.jar:../bin/xercesImpl.jar:../bin/xml-
apis.jar:../bin/cclcfgmcf.jar:../bin/cclcfgapi.jar:../bin/
jcam_crypto.jar:../bin/i18nj.jar:../bin/icu4j.jar:../bin/commons-
httpclient.jar:../bin/commons-logging.jar:../bin/CognosIPF.jar:../bin/
log4j-1.2.8.jar:../bin/jcam_jni.jar:../bin/jaxp.jar:../bin/
jdxslt.jar:../bin/ant.jar:../bin/jcam_config_test.jar:../bin/
cclcoreutil.jar:../bin/CognosCCL4J.jar:../webapps/p2pd/WEB-INF/lib/
ojdbc6.jar
```

5. As the user who installed Network Manager, restart the Tivoli Integrated Portal server: go to $NCHOME/precision/bin and issue **itnm_stop tip** and then **itnm_start tip**.

   Note: If your environment variables are set, you can run the stop and start commands from any directory.

6. Import the content store as described in http://www.ibm.com/support/knowledgecenter/SSEP7J_8.4.0/com.ibm.swg.im.cognos.ug_cra.8.4.1.doc/ug_cra_i_ImportData.html

   Note the following for the import procedure:

   a. In the **Deployment archive** box, select the archive you previously created during the export procedure.
   b. When selecting the options you want, ensure you select **Reports should be upgraded** for your conflict resolution choice.

7. After migrating the Cognos content store, uninstall the Derby content database as described in the *Uninstall Cognos Content Database* topic in the IBM Cognos 8 Business Intelligence Installation and Configuration Guide 8.4.0 on the IBM Cognos information center:
   http://www.ibm.com/support/knowledgecenter/SSEP7J_8.4.0/com.ibm.swg.im.cognos.inst_cr_winux.8.4.0.doc/inst_cr_winux_id7376UninstallCognosContentDatabase.html

   Important: Note the following for the Derby uninstall procedure, when using Tivoli Common Reporting the command is **`tcr_cogconfig.sh`** (instead of **`cogconfig.sh`**).

Configuring NCIM for Tivoli Common Reporting

If you want to use Informix, MySQL, or Oracle as the NCIM database, you must configure the databases before you can use Tivoli Common Reporting reports.

Configure Informix, MySQL, or Oracle databases after installing Network Manager. If you want to use DB2 as the NCIM database, you must configure DB2 before installing Network Manager.

Related tasks:

"Setting up a topology database" on page 56
Apart from the default Informix database, you can use a DB2, MySQL, or Oracle database to store your topology. Unless you are installing the default Informix database bundled with Network Manager, you must configure an existing database or install and configure a new one before installing Network Manager.

Configuring the Informix database for Tivoli Common Reporting on Windows:

If you are using Informix on Windows, you must perform some configuration tasks before you can use Tivoli Common Reporting reports.

Install Network Manager and the Informix database.

To configure Informix for Tivoli Common Reporting, complete the following steps.

1. Open the file `C:\Program Files (x86)\IBM\Informix\Client-SDK\bin\setnet32.exe`. A configuration panel for the Informix database opens.
2. Click the **Environment** tab.
3. Select the variable **DELIMIDENT** and set it to `Y`.
4. Select the variable **DBDATE** and set it to `Y4MD-`.
5. Click the **Server Information** tab.
6. Select the server **ITNM**.

Configuring the Informix database for Tivoli Common Reporting on Unix:

If you are using Informix on Unix, you must perform some configuration tasks before you can use Tivoli Common Reporting reports.

Install Network Manager and the Informix database.

To configure Informix for Tivoli Common Reporting, complete the following steps.

1. Create the file `odbcinst.ini` in the directory `%NCHOME%/etc/`.
2. Edit the file to include the configuration information for the Informix database. The following example is for the Informix Linux version of `odbcinst.ini`.

```
[ODBC Drivers]
IBM INFORMIX ODBC DRIVER=Installed
[IBM INFORMIX ODBC DRIVER]
Driver=/opt/IBM/tivoli/netcool/platform/linux2x86/informix/lib/cli/
iclit09b.so
Setup=/opt/IBM/tivoli/netcool/platform/linux2x86/informix/lib/cli/
iclit09b.so
smProcessPerConnect = Y
FileUsage           = 0
SQLLevel            = 1
```

Configuring the MySQL database for Tivoli Common Reporting on Unix:

If you are using MySQL as the topology database on Unix platforms, you must configure the database before you can use Tivoli Common Reporting reports.

Install Network Manager and the MySQL database.

To configure MySQL for Tivoli Common Reporting, complete the following steps.

1. Create the file `odbcinst.ini` in the directory `$NCHOME/etc/`.
2. Edit the file to include the configuration information for the MySQL database. The following example is for the MySQL Solaris version of `odbcinst.ini`.

```
[ODBC Drivers]
MySQL=Installed
[MySQL]
Description      = ODBC for MySQL
Driver           = /opt/IBM/tivoli/netcool/platform/solaris2/mysql-connector
-odbc-5.1.6/lib/libmyodbc5-5.1.6.so
FileUsage        = 1
UsageCount       = 2
```

Configuring the Oracle database for Tivoli Common Reporting:

If you are using Oracle as the topology database, you must configure the database before you can use Tivoli Common Reporting reports.

Install Network Manager and the Oracle database.

To configure Oracle for Tivoli Common Reporting, complete the following steps.

1. Create or edit the file `tnsnames.ora` located in the following directory: `NCHOME/platform/linux2x86/oracleInstantClient11.1/network/admin`.
2. Edit the file to include the configuration information for the Oracle database. Specify the correct host, port, and service name.

   For Oracle database access, configure the file with an insert similar to the following. Note that the insert must be all on one line:

```
orcl = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)
(HOST = p6tpm06n)(PORT = 1521))) (CONNECT_DATA =
(SID = orcl.london.company.com) )
```

Note: Fix Pack 5 If your Oracle SID value is not the same as your SERVICE_NAME value, or when accessing Oracle RAC with a single client access name, you must use the SERVICE_NAME value in the insert instead of the SID, for example:

```
orcl = (DESCRIPTION = (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)
(HOST = p6tpm06n)(PORT = 1521))) (CONNECT_DATA =
(SERVICE_NAME = orcl.london.company.com) )
```

Important: The SERVICE_NAME must be the fully resolved name.

Configuring Tivoli Common Reporting 3.1 on a remote server

In order to run reports using Tivoli Common Reporting 3.1, you must install Tivoli Common Reporting 3.1 on a separate server and configure a loosely coupled integration between the Network Manager server and the Tivoli Common Reporting server.

Restriction: Tivoli Common Reporting 3.1 is available for Netcool Operations Insight users only.

Tivoli Common Reporting 3.1 to Network Manager integration architecture

Use this information to understand how to integrate Tivoli Common Reporting 3.1 on a separate server to the Network Manager server.

The following figure shows the Tivoli Common Reporting 3.1 to Network Manager integration architecture.

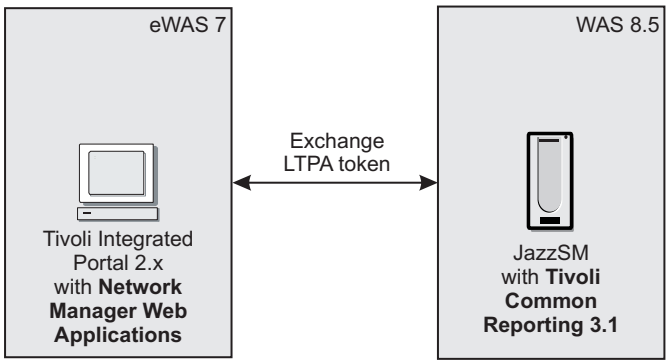

Figure 13. Tivoli Common Reporting 3.1 to Network Manager integration architecture

Requirements for the Tivoli Common Reporting 3.1 server

You must download and install the following software on the Tivoli Common Reporting 3.1 server machine:

- JazzSM
- WAS 8.5
- Tivoli Common Reporting 3.1.

Preparing the Tivoli Common Reporting 3.1 server

Prepare the Tivoli Common Reporting 3.1 server by deploying reports to the server, and configuring databases and data sources.

Deploying reports: Fix Pack 5

You must copy reports from the Network Manager server and deploy the reports on the Tivoli Common Reporting 3.1 server.

In order to configure Tivoli Common Reporting you must run the Tivoli Common Reporting `trcmd.sh` command. You must perform the following set-up procedures before running this command:

- Technote: OutOfMemoryError exception occurs when issuing trcmd command
- SMC blog entry: TCR Birt Engine throws java.lang.StackOverflowError : There is a slight modification to step 6 of this procedure. In that step, add the following property to the file:

  ```
  osgi.nl=en_US
  ```

- Edit the script `/opt/IBM/JazzSM/reporting/bin/trcmd.sh` and change the following line:

  ```
  # Store the location of the BIRT lib directory
  BIRT_LIB=${TCR_ADDONS_DIR}/birt/birt-runtime-2_2_2/ReportEngine/lib
  ```

  Change the value for `BIRT_LIB` to:

  ```
  BIRT_LIB=$TCR_HOME/lib/birt-runtime-2_2_2/ReportEngine/lib
  ```

Proceed as follows:

1. Copy the following files to a convenient target directory on the Tivoli Common Reporting 3.1 server. Make a note of the location of the target directory.
   - `$ITNMHOME/products/tnm /itnmreports.zip`
   - `$ITNMHOME/products/tnm /itnmcognos.zip`
   - `configRemoteTCR.sh`
2. DB2 For DB2 only, copy the following files:
   - `/opt/IBM/JazzSM/lib/db2/db2jcc.jar` to `/opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers`
   - `/opt/IBM/JazzSM/lib/db2/db2jcc_license_cu.jar` to `/opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers`
   - `/opt/IBM/JazzSM/lib/db2/db2jcc.jar` to `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `/opt/IBM/JazzSM/lib/db2/db2jcc_license_cu.jar` to `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
3. Oracle For Oracle only, copy the following files:
   - `$NCHOME/precision/products/tnm/lib/ojdbc6.jar` to `/opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers`
   - `$NCHOME/precision/products/tnm/lib/ojdbc6.jar` to `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
4. Oracle For Oracle only, ensure that the `ncpolldata` user can access the `NCPOLLDATA` schema.

5. Informix For Informix only, copy the following files:
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxjdbc.jar` to `/opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxlang.jar` to `/opt/IBM/JazzSM/reporting/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxjdbc.jar` to `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxlang.jar` to `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxjdbcx.jar` to `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxlsupp.jar` to `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxsqlj.jar` to `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
   - `$NCHOME/platform/<platform>/informix/jdbc/lib/ifxtools.jar` to `/opt/IBM/JazzSM/reporting/cognos/webapps/p2pd/WEB-INF/lib/`
6. DB2 On the Tivoli Common Reporting 3.1 server, locate and run the `configRemoteTCR.sh` script. Supply the full path to the reports package by using the `-r` option. Run the script once for the `itnmcognos10.zip` package and once for the `itnmreports.zip` package.

   Use a command similar to the following example: UNIX

   ```
   $NCHOME/precision/products/tnm/bin/configRemoteTCR.sh -d database_name -e
   NCIM_username -h database_hostname  [-i install] -j
   Jazz_SM_admin_username -n database_port -p
   Jazz_SM_admin_password [-r PackagesDirectory]
   [-s Oracle_service_name] -t $JazzSM_HOME -z
   database_type
   ```

   The options are different for DB2, Oracle 11, and Oracle 12. The options for the `configRemoteTCR` script are described in the following table:

Table 26. configRemoteTCR command-line options

Command-line option	Description
`-d` *database_name* or *service_name*	The NCIM DB2 database name or NCIM Oracle service name.
`-e` *NCIM_user_name*	On some databases, such as Oracle, you might have different user names for the NCIM and the NCPOLLDATA database. You must specify both user names if you have separate ones. Use this option to provide the NCIM user name. The `-d` defines the password for this user.
`-h` *database_hostname*	The host name of the NCIM database.
`-i` *install*	Specifies that the network management reports are installed. You must use the **`install`** parameter in all cases after option `-i`.
`-j` *Jazz_SM_admin_username*	The user name of the Jazz for Service Management administrative user.

Table 26. configRemoteTCR command-line options (continued)

Command-line option	Description
`-n` *database_port*	The port of the NCIM database.
`-p` *Jazz_SM_admin_password*	The password for the Tivoli Integrated Portal administrator.
`-r` *path_to_reports_package*	If your Network Manager installation has the reports package in a non-default location, you can define where the package is using this option.
Oracle `-s` *<Oracle_SID*	Defines the NCIM Oracle System ID (SID).
`-t` *JazzSM_HOME*	The location where Jazz for Service Management is installed.
`-u`	Optional. If a particular user requires access to the NCPOLLDATA schema, specify the username by using this option. The default username is `ncpolldata`.
`-z` *database_type*	The database server type. Can be `db2`, `informix`, or `oracle`.

7. Restart the Jazz for Service Management server using the `stopServer.sh` and `startServer.sh` scripts. By default, these scripts are in the `/opt/IBM/JazzSM/profile/bin/` directory.

Configuring DB2 data sources:

To configure DB2 data sources on the Tivoli Common Reporting 3.1 server, follow these configuration steps.

Adding DB2 support:

To add DB2 support on the Tivoli Common Reporting 3.1 server, follow these configuration steps.

Complete the following tasks to add DB2 support.

1. Install the DB2 client on the Tivoli Common Reporting 3.1 server.
2. Run the following commands to catalog the database used by the reports.

   ```
   db2 CATALOG TCPIP NODE ITNMNODE REMOTE HOSTNAME SERVER PORT
   db2 CATALOG DATABASE DBNAME AT NODE ITNMNODE
   db2 TERMINATE
   ```

   Where:

   - *HOSTNAME* is the hostname of the remote Network Manager NCIM topology database server, or the hostname of the Network Manager server, if the NCIM topology database is installed there.
   - *PORT* is the communication port of the remote Network Manager NCIM topology database server, or the hostname of the Network Manager server, if the NCIM topology database is installed there
   - *DBNAME* is the name of the database.
3. Set the `LD_LIBRARY_PATH` environment variable to enable Cognos to access to the DB2 32-bit libraries.

   ```
   Export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$DB2HOME/sqllib/lib32
   ```
4. Copy the following DB2 JAR files to the specified location: JAR files:

- db2jcc.jar
- db2jcc_license_cu.jar

Location: `$TCRHOME/lib/birt-runtime-2_2_2/ReportEngine /plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/ drivers`

Configuring DB2 data sources for Cognos:

Configure DB2 data sources for reports based on the Cognos data model. DB2 data sources for reports based on the BIRT data model must be configured separately.

To configure DB2 data sources for Cognos, run the following command for each database, substituting the appropriate parameters for each database:

```
$TCRHOME/bin/trcmd.sh -dataSource -add data_source_name -dbType DB2 -dbname db_name
-openSessionSql "SET CURRENT SCHEMA=data_source_name" -dbLogin db_user
-dbPassword db_password -username user_name -password password -force
```

Where the following definitions apply to this command and to the commands in the following steps :

- *data_source_name* is the name of the data source that you are adding. In the following commands you will add the following data sources:
  - NCIM
  - NCPOLLDATA
  - PARAMETERS
  - NCPGUI
  - NCMONITOR
- *db_name* is the name of the database corresponding to the data source that you are configuring.
- *db_user* is the user name for that database.
- *db_password* is the password for that database.
- *user_name* is the user name for the WebSphere Application Server administrator user; by default, this is smadmin.
- *password* is the password for the WebSphere Application Server administrator user.

1. Run the following command to configure the NCIM data source:

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add NCIM -dbType DB2
    -dbname db_name -openSessionSql "SET CURRENT SCHEMA=NCIM"
   -dbLogin db_user -dbPassword db_password -username
   user_name -password password -force
   ```

2. Run the following command to configure the NCPOLLDATA data source:

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add NCPOLLDATA -dbType DB2 -dbname db_name
   -openSessionSql "SET CURRENT SCHEMA=NCPOLLDATA" -dbLogin db_user
   -dbPassword db_password -username user_name -password password -force
   ```

3. Run the following command to configure the PARAMETERS data source:

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add PARAMETERS -dbType DB2 -dbname db_name
   -openSessionSql "SET CURRENT SCHEMA=NCPOLLDATA" -dbLogin db_user
   -dbPassword db_password -username user_name -password password -force
   ```

4. Run the following command to configure the NCPGUI data source:

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add NCPGUI -dbType DB2 -dbname db_name
   -openSessionSql "SET CURRENT SCHEMA=NCPGUI" -dbLogin db_user
   -dbPassword db_password -username user_name -password password -force
   ```

5. Run the following command to configure the NCMONITOR data source:

```
$TCRHOME/bin/trcmd.sh -dataSource -add NCMONITOR -dbType DB2 -dbname db_name
-openSessionSql "SET CURRENT SCHEMA=NCMONITOR" -dbLogin db_user
-dbPassword db_password -username user_name -password password -force
```

If you are using Tivoli Data Warehouse, configure the datasource NCPOLLDATA to point to the Tivoli Data Warehouse database.

1. Change to the following directory (the following path is the default location):/opt/IBM/JazzSM/reporting/bin/.
2. Run the following command: UNIX

```
trcmd.sh -dataSource -add data_source_name -connectionString "^UserID:^?Password:;
LOCAL;D2;DSN=WAREHOUS;UID=%s;PWD=%s;@ASYNC=0@0/
0@COLSEQ=IBM_JD_CNX_STR:^UserID:^?Password:;
LOCAL;JD-D2;URL==JDBC_database_URL odaDriverClass=JDBC_driver_class odaUser=
database_user odaPassword=database_user_password;;DRIVER_NAME=com.ibm.db2.jcc.
DB2Driver" -openSessionSql "SET CURRENT SCHEMA =schema_name" -signonName
database_user  -dbLogin database_user -dbPassword database_user_password
-username jazz_username -password jazz_password -force
```

Windows

```
trcmd.bat -dataSource -add data_source_name -connectionString "^UserID:^?Password:;
LOCAL;D2;DSN=WAREHOUS;UID=%s;PWD=%s;@ASYNC=0@0/
0@COLSEQ=IBM_JD_CNX_STR:^UserID:^?Password:;
LOCAL;JD-D2;URL==JDBC_database_URL odaDriverClass=JDBC_driver_class odaUser=
database_user odaPassword=database_user_password;;DRIVER_NAME=com.ibm.db2.jcc.
DB2Driver" -openSessionSql "SET CURRENT SCHEMA =schema_name" -signonName
database_user  -dbLogin database_user  -dbPassword database_user_password
-username jazz_username -password jazz_password -force
```

Replace the variables in the command using the following definitions:

- *jazz_username* is the username of the administrative user for Jazz for Service Management, for example smadmin.
- *jazz_password* is the password for this user.
- *data_source_name* is the name of the data source you want to configure. Use NCPOLLDATA to configure the connection to Tivoli Data Warehouse.
- *schema_name* is the name of the database schema.
- *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

  "jdbc:db2://*hostname*:*port*/*database_name*:currentSchema=NCIM;"

  Using the following values:

  hostname
  The name of the host where the Tivoli Data Warehouse database is installed.

  port The port on which to connect to the Tivoli Data Warehouse database. The default for DB2 databases is 50000.

  database_name
  The default name of the Tivoli Data Warehouse database is WAREHOUS.

  server The name of the Informix server.

  The following example shows the JDBC connection URL for DB2.

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

  `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 command to set the NCPOLLDATA data source to Tivoli Data Warehouse

DB2 example command

The following command configures the NCPOLLDATA data source for historical reporting to use Tivoli Data Warehouse running on DB2.

```
./trcmd.sh -dataSource -add NCPOLLDATA -connectionString "^UserID:^?Password:;
LOCAL;D2;DSN=WAREHOUS;UID=%s;PWD=%s;@ASYNC=0@0/
0@COLSEQ=IBM_JD_CNX_STR:^User ID:^?Password:;
LOCAL;JD-D2;URL=jdbc:db2://sqa03.hursley.ibm.com:50000/
Warehous:currentSchema=ITMUSER;;
DRIVER_NAME=com.ibm.db2.jcc.DB2Driver" -
openSessionSql "SET CURRENT SCHEMA =ITMUSER"
-signonName ncpolldata -dbLogin itmuser -dbPassword itmuser -username
smadmin -password netcool -force
```

Configuring DB2 data sources for BIRT:

If you use reports based on the BIRT data model, you must configure data sources. 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 the datasources `NCIM`, `PARAMETERS` and `NCPOLLDATA` to point to the NCIM database.

If you are using Tivoli Data Warehouse, configure the datasources `NCIM` and `PARAMETERS` to point to the NCIM database, and `NCPOLLDATA` to point to the Tivoli Data Warehouse database. Obtain the database and connection details from the database administrator before starting this task.

Tip: The reference documentation for each report shows you whether a particular report uses the BIRT or Cognos data model.

To configure the data sources for all reports based on the BIRT data model, complete the following steps.

1. If Tivoli Common Reporting is installed on the same server as Network Manager, configure the datasources NCIM, PARAMETERS and NCPOLLDATA to point to the NCIM database. Run the configTCR.sh script with a command similar to the following command: UNIX

   ```
   $NCHOME/precision/products/tnm/bin/configTCR.sh -d NCIM_database_password
    -p TIP_administrator_password
   ```

2. If Tivoli Common Reporting is installed on a different server to Network Manager, configure the datasources NCIM, PARAMETERS and NCPOLLDATA to point to the NCIM database. Run the configRemoteTCR.sh script with a command similar to the following command: UNIX

   ```
   $NCHOME/precision/products/tnm/bin/configRemoteTCR.sh -d database_name -e
   NCIM_username -h database_hostname  [-i install] -j
   Jazz_SM_admin_username -n database_port -p
   Jazz_SM_admin_password [-r PackagesDirectory]
   [-s Oracle_service_name] -t $JazzSM_HOME -z
   database_type
   ```

   Restriction: The configRemoteTCR.sh script is available in versions of Network Manager starting from V3.9 Fixpack 5.

3. If you are using Tivoli Data Warehouse, configure the datasource NCPOLLDATA to point to the Tivoli Data Warehouse database.
   a. Change to the following directory (the following path is the default location):/opt/IBM/JazzSM/reporting/bin/.
   b. Run the following command: UNIX

      ```
      trcmd.sh -modify -dataSources -reports
      -reportName "/content/package[@name='NetworkManager']/
      folder[@name='Performance Reports']/report
      [@name='Historical SNMP  Trend Quick View Report']"
      -username jazz_username -password jazz_password  -
      dataSourcename=data_source_name
      -setDatasource odaURL=JDBC_database_URL odaDriverClass=JDBC_driver_class
      odaUser=warehousdb_username odaPassword=warehousdb_password
      ```

      Windows

      ```
      trcmd.sh -modify -dataSources -reports
      -reportName "/content/package[@name='NetworkManager']/
      folder[@name='Performance Reports']/report
      [@name='Historical SNMP  Trend Quick View Report']"
      -username jazz_username -password jazz_password  -
      dataSourcename=data_source_name
      -setDatasource odaURL=JDBC_database_URL odaDriverClass=JDBC_driver_class
      odaUser=warehousdb_username odaPassword=warehousdb_password
      ```

      Replace the variables in the command using the following definitions:

      - *jazz_username* is the username of the administrative user for Jazz for Service Management, for example smadmin.
      - *jazz_password* is the password for this user.
      - *data_source_name* is the name of the data source you want to configure. Use NCPOLLDATA to configure the connection to Tivoli Data Warehouse. Other allowed values are:
        - NCIM for reports using topology information.
        - PARAMETERS for reports using the NCPOLLDATA database or the NCPOLLDATA schema for report parameters.
      - *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**

  `"jdbc:db2://hostname:port/database_name:currentSchema=NCIM;"`

  Using the following values:

  hostname
  The name of the host where the Tivoli Data Warehouse database is installed.

  port The port on which to connect to the Tivoli Data Warehouse database. The default for DB2 databases is 50000.

  database_name
  The default name of the Tivoli Data Warehouse database is WAREHOUS.

  server The name of the Informix server.

  The following example shows the JDBC connection URL for DB2.

  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**
  `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 command to set the NCPOLLDATA data source to Tivoli Data Warehouse

DB2 example command

The following command configure the NCPOLLDATA data source for historical reporting to use Tivoli Data Warehouse running on DB2.

```
trcmd.sh -modify -dataSources -reports -reportName "/content/package
[@name='Network Manager']/folder[@name='Performance Reports']/report
[@name='Historical SNMP Trend Quick View Report']" -username
jazz_username
-password jazz_password -dataSource name=data_source_name
-setDatasource odaURL=JDBC_database_URL
odaDriverClass=JDBC_driver_class
odaUser=warehousdb_username odaPassword=warehousdb_password
```

Configuring Oracle data sources:

To configure Oracle data sources on the Tivoli Common Reporting 3.1 server, follow these configuration steps.

Adding Oracle support:

To add Oracle support on the Tivoli Common Reporting 3.1 server, follow these configuration steps.

Make sure that you install the Oracle database client on the computer where Tivoli Common Reporting 3.1 is installed.

Complete the following tasks to add Oracle support.

1. Copy the Oracle client 32-bit libraries from the following location on the Network Manager server to the to the Tivoli Common Reporting 3.1 machine.

   `$NCHOME/platform/linux2x86/oracleInstantClient11.1`

2. Set the `LD_LIBRARY_PATH` environment variable to enable Cognos to access to the Oracle 32-bit libraries.

   ```
   Export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:$NCHOME/platform/linux2x86/
   oracleInstantClient11.1
   ```

3. Create or edit the file `$ORACLE_HOME/network/admin/tnsnames.ora` and add the following lines to the file:

   ```
   DB_NAME =
       (DESCRIPTION =
      (ADDRESS_LIST = (ADDRESS = (PROTOCOL = TCP)(HOST = HOSTNAME)(PORT = PORT)))
      (CONNECT_DATA = (SID = <DB_NAME>) )
   )
   ```

   Where:

   - *DBNAME* is the name of the database.
   - *HOSTNAME* is the hostname of the remote Network Manager NCIM topology database server, or the hostname of the Network Manager server, if the NCIM topology database is installed there.
   - *PORT* is the communication port of the remote Network Manager NCIM topology database server, or the hostname of the Network Manager server, if the NCIM topology database is installed there

4. Copy the following Oracle JAR file to the specified location: JAR file:

   - ojdbc6.jar

   Location: `$TCRHOME/lib/birt-runtime-2_2_2/ReportEngine/plugins/org.eclipse.birt.report.data.oda.jdbc_2.2.2.r22x_v20071206/drivers/`

Configuring Oracle data sources for Cognos:

Configure Oracle data sources for reports based on the Cognos data model. Oracle data sources for reports based on the BIRT data model must be configured separately.

1. To configure Oracle data sources for Cognos, run the following command for each database, substituting the appropriate parameters for each database:

   ```
   $TCRHOME/bin/trcmd.sh -dataSource -add data_source_name -dbType ORACLE
   -dbname db_name -openSessionSql "ALTER SESSION SET CURRENT_SCHEMA=
   data_source_name" -dbLogin db_user -dbPassword
   db_password -username user_name -password password -force
   ```

Where the following definitions apply to this command and to the commands in the following steps :

- *data_source_name* is the name of the data source that you are adding. In the following commands you will add the following data sources:
  - NCIM
  - NCPOLLDATA
  - PARAMETERS
  - NCPGUI
  - NCMONITOR
- *db_name* is the name of the database corresponding to the data source that you are configuring.
- *db_user* is the user name for that database.
- *db_password* is the password for that database.
- *user_name* is the user name for the WebSphere Application Server administrator user; by default, this is smadmin.
- *password* is the password for the WebSphere Application Server administrator user.

2. Run the following command to configure the NCIM data source:

```
$TCRHOME/bin/trcmd.sh -dataSource -add NCIM -dbType ORACLE
-dbname db_name -openSessionSql "ALTER SESSION SET CURRENT_SCHEMA = NCIM"
-dbLogin db_user -dbPassword db_password -username user_name -password
password -force
```

3. Run the following command to configure the NCPOLLDATA data source:

```
$TCRHOME/bin/trcmd.sh -dataSource -add NCPOLLDATA -dbType ORACLE
-dbname db_name -openSessionSql ALTER SESSION SET CURRENT_SCHEMA=NCPOLLDATA"
-dbLogin db_user -dbPassword db_password -username user_name -password
password -force
```

4. Run the following command to configure the PARAMETERS data source:

```
$TCRHOME/bin/trcmd.sh -dataSource -add PARAMETERS -dbType ORACLE
-dbname db_name -openSessionSql "ALTER SESSION SET CURRENT_SCHEMA=NCPOLLDATA"
-dbLogin db_user -dbPassword db_password -username user_name -password
password -force
```

5. Run the following command to configure the NCPGUI data source:

```
$TCRHOME/bin/trcmd.sh -dataSource -add NCPGUI -dbType ORACLE
-dbname db_name -openSessionSql "ALTER SESSION SET CURRENT_SCHEMA=NCPGUI"
-dbLogin db_user -dbPassword db_password -username user_name -password
password -force
```

6. Run the following command to configure the NCMONITOR data source:

```
$TCRHOME/bin/trcmd.sh -dataSource -add NCMONITOR -dbType ORACLE
-dbname db_name -openSessionSql "ALTER SESSION SET CURRENT_SCHEMA=NCMONITOR"
-dbLogin db_user -dbPassword db_password -username user_name -password
password -force
```

7. If you are using Tivoli Data Warehouse, configure the datasource NCPOLLDATA to point to the Tivoli Data Warehouse database.
   a. Change to the following directory (the following path is the default location):/opt/IBM/JazzSM/reporting/bin/.
   b. Run the following command: UNIX

```
trcmd.sh -dataSource -add data_source_name -connectionString
 "^User ID:^?Password:;LOCAL;JD-OR;URL=JDBC_database_URL;DRIVER_NAME=
oracle.jdbc.driver.OracleDriver" -
```

```
openSessionSql "ALTER SESSION CURRENT_SCHEMA=schema_name"
 -signonName database_user  -dbLogin database_user
 -dbPassword database_user_password -username jazz_username
-password jazz_password -force
```

Windows

```
trcmd.bat -dataSource -add data_source_name -connectionString
"^User ID:^?Password:;LOCAL;JD-OR;URL=JDBC_database_URL;
DRIVER_NAME= oracle.jdbc.driver.OracleDriver"  -
openSessionSql " ALTER SESSION SET
CURRENT_SCHEMA=schema_name" -signonName database_user -
dbLogin database_user  -dbPassword
database_user_password -username jazz_username -password
jazz_password -force
```

Replace the variables in the command using the following definitions:

- *jazz_username* is the username of the administrative user for Jazz for Service Management, for example `smadmin`.
- *jazz_password* is the password for this user.
- *data_source_name* is the name of the data source you want to configure. Use NCPOLLDATA to configure the connection to Tivoli Data Warehouse.
- *schema_name* is the name of the database schema.
- *JDBC_database_URL* is the URL for the JDBC database. The URL depends on the platform and other variables.

The following is an example of a JDBC URL: `jdbc:oracle://`*`hostname`*`:`*`port`*`/`*`database_name`*`:currentSchema=NCIM;"`

Where:

- *hostname* is the name of the host where the Tivoli Data Warehouse database is installed.
- *port* is the port on which to connect to the Tivoli Data Warehouse database. The default for Oracle databases is 1521.
- *database_name* is the name of the database. The default name of the Tivoli Data Warehouse database is WAREHOUS.
- *server* is the name of the Informix server.

jdbc_driver_class is the class name of the JDBC driver. The following values show the class names for different platforms.

- `oracle.jdbc.driver.OracleDriver`
- *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.

The following example shows the JDBC connection URL for Oracle: `jdbc:oracle://192.168.1.2:1521/itnm:NCIM`

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.
- The name of the topology database schema name, in uppercase, is NCIM.

Configuring Oracle data sources for BIRT:

If you use reports based on the BIRT data model, you must configure data sources. 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 the datasources `NCIM`, `PARAMETERS` and `NCPOLLDATA` to point to the NCIM database.

If you are using Tivoli Data Warehouse, configure the datasources `NCIM` and `PARAMETERS` to point to the NCIM database, and `NCPOLLDATA` to point to the Tivoli Data Warehouse database. Obtain the database and connection details from the database administrator before starting this task.

Tip: The reference documentation for each report shows you whether a particular report uses the BIRT or Cognos data model.

To configure the data sources for all reports based on the BIRT data model, complete the following steps.

1. If Tivoli Common Reporting is installed on the same server as Network Manager, configure the datasources `NCIM`, `PARAMETERS` and `NCPOLLDATA` to point to the NCIM database. Run the `configTCR.sh` script with a command similar to the following command: UNIX

   ```
   $NCHOME/precision/products/tnm/bin/configTCR.sh -d NCIM_database_password
    -p TIP_administrator_password
   ```

2. If Tivoli Common Reporting is installed on a different server to Network Manager, configure the datasources `NCIM`, `PARAMETERS` and `NCPOLLDATA` to point to the NCIM database. Run the `configRemoteTCR.sh` script with a command similar to the following command: UNIX

   ```
   $NCHOME/precision/products/tnm/bin/configRemoteTCR.sh -d database_name -e
   NCIM_username -h database_hostname  [-i install] -j
   Jazz_SM_admin_username -n database_port -p
   Jazz_SM_admin_password [-r PackagesDirectory]
   [-s Oracle_service_name] -t $JazzSM_HOME -z
   database_type
   ```

   Restriction: The `configRemoteTCR.sh` script is available in versions of Network Manager starting from V3.9 Fixpack 5.

3. If you are using Tivoli Data Warehouse, configure the datasources `NCPOLLDATA` to point to the Tivoli Data Warehouse database.

   a. Change to the following directory (the following path is the default location):`/opt/IBM/JazzSM/reporting/bin/`.

   b. Run the following command: UNIX

   ```
   trcmd.sh -modify -dataSources -reports
   -reportName "/content/package[@name='NetworkManager']/
   folder[@name='Performance Reports']/report
   [@name='Historical SNMP  Trend Quick View Report']"
   -username jazz_username -password jazz_password  -
   dataSourcename=data_source_name
   -setDatasource odaURL=JDBC_database_URL odaDriverClass=JDBC_driver_class
   odaUser=warehousdb_username odaPassword=warehousdb_password
   ```

   Windows

   ```
   trcmd.sh -modify -dataSources -reports
   -reportName "/content/package[@name='NetworkManager']/
   folder[@name='Performance Reports']/report
   ```

```
[@name='Historical SNMP  Trend Quick View Report']"
-username jazz_username -password jazz_password  -
dataSourcename=data_source_name
-setDatasource odaURL=JDBC_database_URL odaDriverClass=JDBC_driver_class
odaUser=warehousdb_username odaPassword=warehousdb_password
```

Replace the variables in the command using the following definitions:

- *jazz_username* is the username of the administrative user for the Tivoli Integrated Portal, for example `smadmin`.
- *jazz_password* is the password for this user.
- *data_source_name* is the name of the data source you want to configure. Use NCPOLLDATA to configure the connection to Tivoli Data Warehouse. Other allowed values are:
  - NCIM for reports using topology information.
  - PARAMETERS for reports using the NCPOLLDATA database or the NCPOLLDATA schema for report parameters.
- *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**

  `jdbc:oracle:thin:@`*`hostname`*`:`*`port`*`:`*`database_name`*

  Using the following values:

  hostname
  The name of the host where the TDW database is installed.

  port The port on which to connect to the TDW database. The default for Oracle databases is 1521.

  database_name
  The default name of the TDW database is WAREHOUS.

  server The name of the Informix server.

  The following example shows the JDBC connection URL for Oracle.

  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.
- *jdbc_driver_class* is the class name of the JDBC driver. The following values show the class names for different platforms.
- **JDBC Driver**

  `oracle.jdbc.driver.OracleDriver`
- *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 the NCPOLLDATA data source to Tivoli Data Warehouse

Oracle example command

The following command configure the NCPOLLDATA data source for historical reporting to use Tivoli Data Warehouse running on Oracle.

```
trcmd.sh -modify -dataSources -reports -reportName
"/content/package[@name='Network
Manager']/folder[@name='Performance Reports']/
report[@name='Historical SNMP
Trend Quick View Report']" -username jazz_username -password
jazz_password -dataSource name=data_source_name -setDatasource
odaURL=JDBC_database_URL odaDriverClass=JDBC_driver_class
odaUser=warehousdb_username odaPassword=warehousdb_password
```

Configuring the integration between Network Manager and Tivoli Common Reporting 3.1

Install Tivoli Common Reporting 3.1 on a separate server, and then configure the integration so that you can run reports on the Tivoli Common Reporting server directly from the GUI on the Network Manager server.

Before performing these configuration tasks make sure that the following items are in place:

- The same users exist on both the Tivoli Integrated Portal and Tivoli Common Reporting servers. This is necessary for single sign-on.
- A valid SSL certificate is installed on both Tivoli Integrated Portal and Tivoli Common Reporting server.This is necessary to ensure that content is not blocked, especially Tivoli Common Reporting 3.1 content being displayed on the Tivoli Integrated Portal server.
- In Internet Explorer ensure that the Tivoli Integrated Portal 3.1 server is added to the list of websites to be displayed in compatibility view.

Setting up LTPA token exchange:

Set up Lightweight Third Party Authentication (LTPA) token exchange between the Tivoli Integrated Portal server and the Tivoli Common Reporting 3.1 server to avoid password prompts when viewing reports in Tivoli Common Reporting 3.1.

Proceed as follows:

1. On the Tivoli Integrated Portal server, click **Settings** > **WebSphere Administrative Console** in the left-hand navigation panel to access the WebSphere Administrative Console.
2. Export the LTPA token. For more information see the topic "Managing LTPA keys from multiple WebSphere Application Server cells" in the WebSphere Application Server documentation.
3. On the Tivoli Common Reporting 3.1 server, click **Console Settings** > **WebSphere Administrative Console** > in the left-hand navigation strip to access the WebSphere Administrative Console.
4. Import the LTPA token. For more information see the topic "Managing LTPA keys from multiple WebSphere Application Server cells" in the WebSphere Application Server documentation.

Reassigning Tivoli Common Reporting roles:

By default Tivoli Integrated Portal contains a predefined role that controls whether users see the Tivoli Common Reporting 2.x launch point in the Tivoli Integrated Portal navigation. You must remove this role from all users and groups which you have given it on the Tivoli Integrated Portal server, and then on the Tivoli Common Reporting 3.1 server you must assign this role to relevant users and groups.

Proceed as follows:

1. In the Tivoli Integrated Portal left-hand navigation pane, click **Users and Groups** > **Roles**.
2. Identify the tcrPortalOperator role.
3. Remove this role from all users and groups to which it is assigned,
4. Delete the role.
5. On the Tivoli Common Reporting 3.1 server assign this role to relevant users and groups.

Configuring the user interface to point to the Tivoli Common Reporting 3.1 system:

You must create a Tivoli Integrated Portal page to present report data from the Tivoli Common Reporting 3.1 system.

Proceed as follows:

1. In the Tivoli Integrated Portal left-hand navigation pane, click **Settings** > **Pages**.
2. In the Pages page, click **New Page...**.
3. In the Page Settings page type a name for the page and the location where it should appear in the Tivoli Integrated Portal left-hand navigation pane. For example, you could call the page Common Reporting 3.1 and you could add it to the **Reporting** node.
4. Click **Page Layout** > **Freeform** and click **OK**. A new tab opens where you can define content to include in thi page.
5. Add a web wdiget to the page. To add the web widget, in the widget ribbon at the top of the page scroll to the right until the **Web Widget** portlet icon is visible; then drag the **Web Widget** portlet icon into the main page area.
6. Click **Edit Options** > **Personalize**.
7. In the Web Widget window, do the following: type the following for :
   - Type the following URL in the **Home Page** text field:
     `https://`*`TCR_server_name`*`:16311/tarf/servlet/dispatch`, where *TCR_server_name* is the resource name of the Tivoli Common Reporting 3.1 server.
   - Uncheck the **Show a browser control toolbar** setting.
   - The other settings can be left blank
8. Click **OK**.
9. Save the page.

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 27. 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.

Enabling failover

You can enable failover in your Network Manager environment to ensure that the different components are kept running and available.

About 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 can be implemented for each of the following products and components, which can be installed when you run the Network Manager installer:

- The Network Manager core components, including the root cause analysis component, Polling engine, and Event Gateway
- The topology database
- Tivoli Netcool/OMNIbus, including the ObjectServer (for event management)
- The Network Manager Web applications and the Tivoli Netcool/OMNIbus Web GUI, which are installed within the Tivoli Integrated Portal server framework

  Restriction: Network Manager does not support the Tivoli Integrated Portal load balancing feature that the Tivoli Netcool/OMNIbus Web GUI does.

You must decide for which components you want to implement failover, and the number of computers required for high availability.

About NCIM topology database high availability

Network Manager allows you to configure the Network Connectivity and Inventory Model (NCIM) topology database for high availability, minimizing the impact of computer or network failure. The following sections provide an overview of NCIM topology database high availability and explain how to configure it.

High availability refers to a computing environment in which the hardware and software components remain operational during planned outages (for example, regular maintenance operations) and unplanned outages (for example, unexpected hardware, network, and software failures). One component that needs to be operational all of the time is the NCIM topology database.

Note: In previous Network Manager releases, users could include an NCIM topology database failover configuration by using NCIM replication (also referred to as NCIM topology database replication). The NCIM replication feature has been replaced by the high availability feature that is provided by the supported database:

- If you have a DB2 database, you can use the High Availability Disaster Recovery (HADR) feature to set up failover for NCIM.
- Fix Pack 5 If you have an Oracle database, you can use the Real Application Clusters (RAC) feature to set up failover for NCIM.

To configure a failover configuration for the NCIM topology database and thus provide users a high availability environment for running database applications and accessing information stored in the NCIM topology database, you need to become familiar with the following background topics and tasks:

- High availability strategies provided by the database
- Failover architecture for NCIM topology database and Network Manager core processes
- Tasks associated with installing the database

High availability using DB2

You can use the DB2 HADR feature to set up data replication from a primary to a backup database. The primary database normally processes all or most of the application workload, while the backup database can take over the workload if the primary database fails, enabling the database to remain available to user applications. In a DB2 HADR environment, the backup database is called the standby database.

Using the HADR feature, the DB2 Automatic Client Reroute (ACR) provides rerouting of the Network Manager client connections to the appropriate primary NCIM server.

You can use IBM Tivoli System Automation for Multiplatforms (SA MP) to automatically promote a standby DB2 server to become the primary when the acting primary fails.

Note: DB2 provides the tools necessary for installing and configuring the NCIM topology database (and core processes) to use the DB2 HADR feature. For information on how to install and configure DB2, see Related information later for links to the DB2 Information Center.

Fix Pack 5

Clustering and high availability using Oracle RAC

Oracle provides the Real Application Clusters (RAC) feature for clustering and high availability in Oracle database environments. Using Oracle RAC, you can create a high availability setup for your NCIM topology database. For information on how to install and configure Oracle RAC, see Related information later for a link to the Oracle documentation.

Failover architecture for NCIM topology database and Network Manager core processes

Failover of the Network Manager core processes can be implemented by setting up primary and backup Network Manager installations that run on different servers and domains. Both installations can either connect to a single Tivoli Netcool/OMNIbus ObjectServer or to a virtual pair of ObjectServers. Network Manager failover can be implemented with NCIM topology database high availability or without NCIM topology database high availability. If you choose to implement failover with NCIM topology database high availability, you will do so through the high availability feature that is provided by the supported database. For example, to set up a failover configuration for the NCIM topology database if you have a DB2 database, you can use the DB2 high availability disaster recovery (HADR) feature. Similarly, if you have a Oracle database, you can use the Real Application Clusters (RAC) feature for NCIM failover.

Tasks associated with installing the database

A DB2 database can be installed and configured by Network Manager. To use an independent DB2 or Oracle database, configure it as described in "Setting up a topology database" on page 56.

Related concepts:

"Network Manager failover architecture (core processes)" on page 281
Failover of the Network Manager core processes can be implemented by setting up primary and backup Network Manager installations that run on different servers. Both installations can either connect to a single Tivoli Netcool/OMNIbus ObjectServer or to a virtual pair of ObjectServers.

Related tasks:

"Installing and configuring DB2 databases on UNIX" on page 60
To use a DB2 database as the topology database on UNIX, you must install DB2, configure an instance, and create a database before Network Manager is installed.

Related information:

IBM DB2 Version 10.1 Information Center
For more information on DB2 10.1 HADR, search the IBM DB2 Version 10.1 Information Center. Suggested search terms include "high availability".

IBM DB2 Version 9.7 Information Center
For more information on DB2 9.7 HADR, search the IBM DB2 Version 9.7 Information Center. Suggested search terms include "high availability".

Oracle Database Online Documentation

Failover architectures

Network Manager failover is implemented independently of failover in the products and components with which it integrates. Before configuring failover, you must understand the failover architectures that can be implemented to help ensure high availability of your Network Manager installation.

A Network Manager failover installation contains a primary and a backup Network Manager server on which the core components are installed. If the primary server fails due to problems with the hardware or software, the backup server assumes the role of the primary server. For a more robust environment, you can additionally include one or more of the following failover configurations:

- A primary and a backup Tivoli Netcool/OMNIbus ObjectServer.
- Tivoli Netcool/OMNIbus Web GUI data source failover.

  Restriction: Network Manager does not support the Tivoli Integrated Portal load balancing feature that the Tivoli Netcool/OMNIbus Web GUI does.
- An NCIM topology database high availability configuration

  Note: In previous Network Manager releases, users could include an NCIM topology database failover configuration by using NCIM replication (also referred to as NCIM topology database replication). The NCIM replication feature has been replaced by the high availability feature that is provided by the supported database:
  - If you have a DB2 database, you can use the High Availability Disaster Recovery (HADR) feature to set up failover for NCIM.
  - Fix Pack 5 If you have an Oracle database, you can use the Real Application Clusters (RAC) feature to set up failover for NCIM.

  This NCIM topology database high availability configuration ensures that network polling can continue on the backup installation, and topology views are replicated.

To accommodate either hardware or software failure, and for optimum performance of your environment, implement your failover solution on more than one computer.

Related information:

IBM DB2 Version 10.1 Information Center
For more information on DB2 10.1 HADR, search the IBM DB2 Version 10.1 Information Center. Suggested search terms include "high availability".

IBM DB2 Version 9.7 Information Center
For more information on DB2 9.7 HADR, search the IBM DB2 Version 9.7 Information Center. Suggested search terms include "high availability".

Oracle Database Online Documentation

ObjectServer failover architecture

You can deploy Tivoli Netcool/OMNIbus by using a scalable multitiered architecture, so that the system can continue to operate to full capacity (and with minimal event loss) in the event of ObjectServer, ObjectServer Gateway, or proxy server failure.

The components in the architecture sit within three tiers (or layers): collection, aggregation, and display. The basic failover configuration consists of a primary ObjectServer and a backup ObjectServer that are connected by a bidirectional ObjectServer Gateway in the aggregation layer, with no collection or display layers connected. The modular design of the multitiered architecture means that any system can start with a single pair of aggregation ObjectServers, and then have collection or display components added at any time in the future.

The following figure shows an example of the basic failover configuration in the aggregation layer.

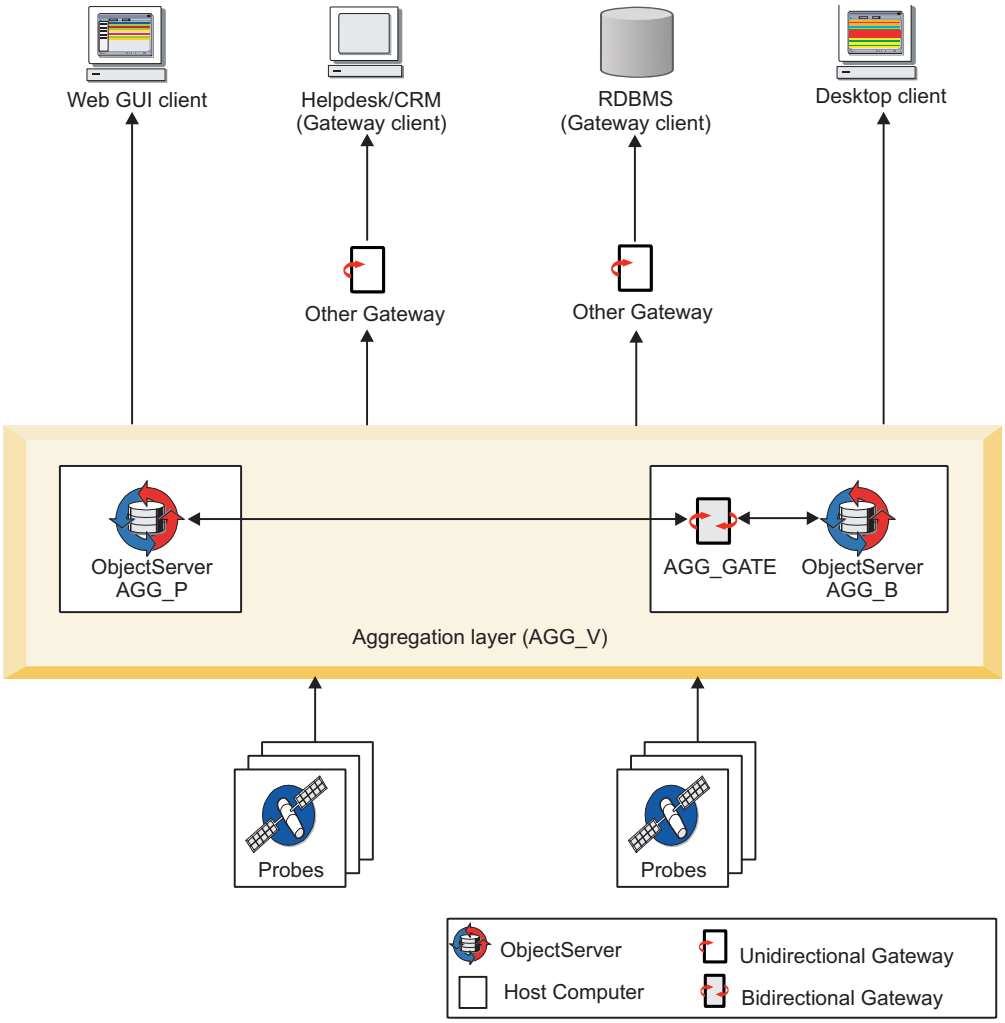

Figure 14. ObjectServer failover architecture

To minimize the impact of computer failure, the primary ObjectServer (AGG_P) and backup ObjectServer (AGG_B) run on two separate computers. The bidirectional ObjectServer Gateway (AGG_GATE) runs on the backup ObjectServer computer, and synchronizes the ObjectServers. The primary and backup

ObjectServers are configured as a virtual aggregation pair (AGG_V) to which probes, and other clients such as the Event Gateway, can directly connect. The concept of a virtual pair helps to facilitate seamless fail over to the backup ObjectServer if the primary ObjectServer becomes unavailable, and fail back when the primary ObjectServer is active again. In the figure, example targets to which alerts can be forwarded from the aggregation layer are also shown.

For full information about setting up ObjectServer failover in the collection, aggregation, and display layers of the multitiered architecture, see the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Related concepts:

"Network Manager failover architecture (core processes)" on page 281
Failover of the Network Manager core processes can be implemented by setting up primary and backup Network Manager installations that run on different servers. Both installations can either connect to a single Tivoli Netcool/OMNIbus ObjectServer or to a virtual pair of ObjectServers.

Related tasks:

"Configuring ObjectServer failover" on page 300
The way in which you configure ObjectServer failover is dependent on the Tivoli Netcool/OMNIbus version.

About the Tivoli Netcool/OMNIbus failover configuration files:

Tivoli Netcool/OMNIbus V7.3 or later, provides a set of configuration files that you can apply to ObjectServers and ObjectServer Gateways in order to implement the multitiered architecture.

These files are available in the `$NCHOME/omnibus/extensions/multitier` directory, and include:

- SQL import files that can be applied to each ObjectServer, in order to update the database schema with the required configuration; for example, additional columns, conversions, and automations
- ObjectServer Gateway files that can be used to configure the gateways in the architecture

Important:

- When using the configuration files supplied in Tivoli Netcool/OMNIbus V7.3 or later, you must adhere to the defined naming convention for the components in each layer of the multitiered architecture. To implement failover in the aggregation layer, use the naming conventions depicted in Figure 14 on page 279; that is, AGG_P for the primary ObjectServer, AGG_B for the backup ObjectServer, AGG_V for the virtual pair, and AGG_GATE for the bidirectional ObjectServer Gateway.
- In earlier versions of Tivoli Netcool/OMNIbus, no configuration files are provided, and it is not mandatory to comply with these naming conventions.

For further information about the multitiered configuration files, and the naming conventions for the components in the multitiered architecture, see the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide* at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Network Manager failover architecture (core processes)

Failover of the Network Manager core processes can be implemented by setting up primary and backup Network Manager installations that run on different servers. Both installations can either connect to a single Tivoli Netcool/OMNIbus ObjectServer or to a virtual pair of ObjectServers.

When you connect to a Network Manager server, the associated domain under which the processes run needs to be identified. Network Manager provides a virtual domain that can be used when running in failover mode. Any connection to this virtual domain is routed to the Network Manager installation that is running as the primary server in the failover architecture. This routing capability is provided by the Virtual Domain component.

The following figure shows the high-level failover architecture for the primary and backup Network Manager core processes, which are set up in two separate domains.

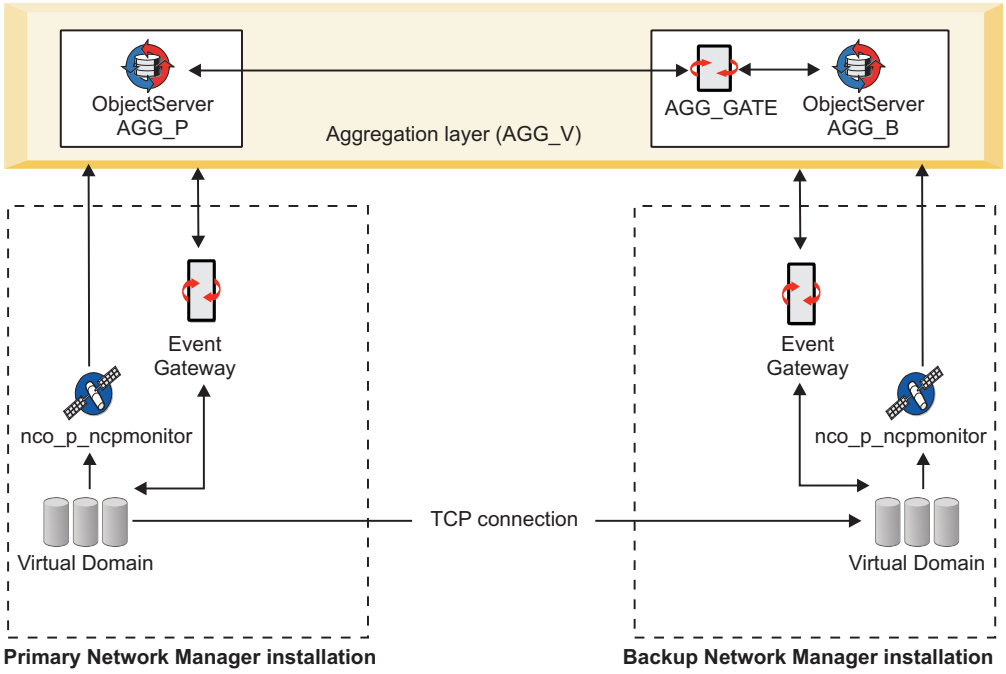

Figure 15. Network Manager failover architecture

In the figure, both the primary and backup installations connect to a virtual pair of ObjectServers.

In each domain:

- The Virtual Domain component (**ncp_virtualdomain**) manages failover, and raises health check events to indicate whether the domain is healthy.
- The Probe for Tivoli Netcool/OMNIbus (**nco_p_ncpmonitor**) connects to the virtual ObjectServer pair, and forwards the health check events.
- The Event Gateway (**ncp_g_event**) connects to the virtual ObjectServer pair, reads in all health check events, and then passes the events to the Virtual Domain component.

  These health check events are used to trigger failover.

A TCP socket connection is required between the Virtual Domain processes, to copy data from the primary domain to the backup domain. This ensures that the topology is in sync when failover occurs.

Note: If you implement failover, then you must ensure that both the primary and backup installations are using identical encryption keys. If the encryption keys are not identical, then the backup poller does not function correctly during failover. To ensure that both the primary and backup installations are using identical encryption keys, copy the following file from the primary server to the same location on the backup server: `$NCHOME/etc/security/keys/conf.key`. If you enter all SNMP community strings on the command line and do not encrypt them, you do not need to do this task. For more information on changing the encryption key, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

NCIM implementations for failover

You can set up Network Manager failover with NCIM topology database high availability. This failover configuration protects against data loss by replicating data changes from the source NCIM topology database in the primary Network Manager domain to one or more target NCIM topology databases in the backup Network Manager domain. The source NCIM topology database is referred to as the primary database and the target NCIM topology database is referred to as the standby database. This approach removes the single point of failure because both the primary and backup Network Manager domains connect to whichever database is acting as the primary database.

In any failover configuration, both the primary and backup Network Manager domains connect to the same database, even with database high availability configured. The main difference is that with high availability, the database is replicated on the standby database server.

Note: In previous Network Manager releases, users could include an NCIM topology database failover configuration by using NCIM replication (also referred to as NCIM topology database replication). The NCIM replication feature has been replaced by the high availability feature that is provided by the supported database:

- If you have a DB2 database, you can use the High Availability Disaster Recovery (HADR) feature to set up failover for NCIM.
- Fix Pack 5 If you have an Oracle database, you can use the Real Application Clusters (RAC) feature to set up failover for NCIM.

Regardless of whether failover is configured with or without NCIM topology database high availability, all entities in the topology are stored under the primary domain name, and all poll policies are configured for the primary domain. There is no entry in the domainMgr table for the backup domain. As a result, the NmosDomainName field for an event in the alerts.status table will always be populated with the primary domain name when failover is configured.

Note: To configure NCIM topology database high availability using DB2 HADR, set up the HADR environment by following the instructions provided in the DB2 documentation. See Related information later for links to your DB2 Information Center. You then perform tasks to configure Network Manager to work with DB2 HADR. Fix Pack 5 If you have an Oracle database, set up the Oracle RAC environment using the instructions provided in the Oracle documentation. See

related links later for a link to the Oracle documentation. You then perform tasks to configure Network Manager to work in the Oracle RAC environment.

Related concepts:

"ObjectServer failover architecture" on page 279
You can deploy Tivoli Netcool/OMNIbus by using a scalable multitiered architecture, so that the system can continue to operate to full capacity (and with minimal event loss) in the event of ObjectServer, ObjectServer Gateway, or proxy server failure.

"Failover on the backup installation without NCIM replication" on page 291
This failover configuration has no NCIM topology database on the backup installation.

"Failover on the backup installation with NCIM replication" on page 293
This failover configuration includes a copy of the NCIM topology database on the backup installation. All processes on the backup installation point to the NCIM topology database on the backup installation.

Fix Pack 4 "Failover on the backup installation" on page 295
All processes on the backup installation point to the NCIM topology database on the primary installation and this primary NCIM topology database can be a stand alone database or one configured for high availability.

Fix Pack 4 "About NCIM topology database high availability" on page 276
Network Manager allows you to configure the Network Connectivity and Inventory Model (NCIM) topology database for high availability, minimizing the impact of computer or network failure. The following sections provide an overview of NCIM topology database high availability and explain how to configure it.

Related tasks:

"Configuring failover of the Network Manager core processes" on page 307
You can configure failover of the Network Manager core processes by using the `$NCHOME/etc/precision/ConfigItnm.cfg` file to enable failover.

"Installing and configuring DB2 databases on UNIX" on page 60
To use a DB2 database as the topology database on UNIX, you must install DB2, configure an instance, and create a database before Network Manager is installed.

Fix Pack 4 "Configuring Network Manager to work with DB2 HADR or Oracle RAC" on page 313
You can configure Network Manager core processes to use the DB2 catalog and the Network Manager GUI to operate in the DB2 high availability disaster recovery (HADR) environment. Fix Pack 5 Similarly, you can also configure Network Manager core processes and the Network Manager GUI to operate in the Oracle Real Application Clusters (RAC) environment.

Related information:

IBM DB2 Version 10.1 Information Center
For more information on DB2 10.1 HADR, search the IBM DB2 Version 10.1 Information Center. Suggested search terms include "high availability".

IBM DB2 Version 9.7 Information Center
For more information on DB2 9.7 HADR, search the IBM DB2 Version 9.7 Information Center. Suggested search terms include "high availability".

Oracle Database Online Documentation

Tivoli Netcool/OMNIbus Web GUI data source failover

The Web GUI implements data source failover. If a primary and a backup ObjectServer are available, you can set up connections to both ObjectServers so that if the primary ObjectServer fails, the Web GUI will fail over and use the backup ObjectServer as the source of its events.

Related concepts:

"Tivoli Netcool/OMNIbus Web GUI data sources" on page 159
A data source is another term for an ObjectServer or ObjectServer failover pair used by the Web GUI for event information.

Related tasks:

"Configuring data source failover for the Tivoli Netcool/OMNIbus Web GUI" on page 304
If you have a failover pair of ObjectServers to which the Web GUI should connect, you can configure data source failover by using the `ncwDataSourceDefinitions.xml` data source configuration file in your Web GUI installation.

Server allocation for failover

Any primary system must be installed on a separate host to a backup system, so that if the primary host fails, the backup host is unaffected.

Ideally, the primary ObjectServer, backup ObjectServer, primary Network Manager server, backup Network Manager server and Tivoli Integrated Portal server would each be installed on separate hosts. However, this might not be practical.

Related reference:

"Constraints for installing and starting components" on page 15
Some components must be installed and started before others. Use this information as well as the installation examples to understand the order in which you must install and start components.

Example failover hosting without NCIM topology database high availability:

This is an example of failover hosting where the failover configuration does not include a copy of the NCIM topology database on the backup installation.

In any failover configuration, both the primary and backup Network Manager domains connect to the same database, but in a failover set up without NCIM topology database high availability there is no database replication on a standby server.

The following figure shows an example of hosting ObjectServer and Network Manager failover using four host machines.

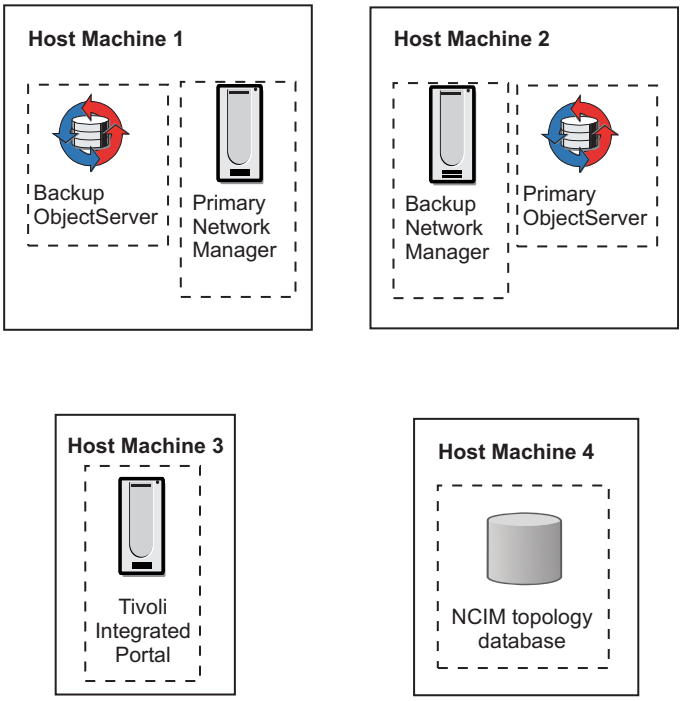

Figure 16. Example failover hosting

For performance reasons, the NCIM topology database requires a high bandwidth connection to the Tivoli Integrated Portal server. If host machine 3 has multiple CPUs and sufficient memory, you can install NCIM on host machine 3.

Install the core components on both host machines 1 and 2, and install the Web applications on host machine 3. Install the NCIM topology database on host machine 4.

Note: If you implement failover without NCIM replication and you entered SNMP community strings using the Discovery Configuration GUI, then you must ensure that both the primary and backup installations are using identical encryption keys. If the encryption keys are not identical, then the backup poller does not function correctly during failover. To ensure that both the primary and backup installations are using identical encryption keys, copy the following file from the primary server to the same location on the backup server: `$NCHOME/etc/security/keys/conf.key`. If you enter all SNMP community strings on the command line and do not encrypt them, you do not need to do this task. For more information on changing the encryption key, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Example failover hosting with NCIM topology database high availability:

This is an example of failover hosting where the failover configuration includes a copy of the NCIM topology database on the backup installation.

In any failover configuration, both the primary and backup Network Manager domains connect to the same database, but in a failover set up with database high availability configured, the database is replicated on the standby database server.

Note: In previous Network Manager releases, users could include an NCIM topology database failover configuration by using NCIM replication (also referred

to as NCIM topology database replication). The NCIM replication feature has been replaced by the high availability feature that is provided by the supported database:

- If you have a DB2 database, you can use the High Availability Disaster Recovery (HADR) feature to set up failover for NCIM.
- Fix Pack 5 If you have an Oracle database, you can use the Real Application Clusters (RAC) feature to set up failover for NCIM.

The following figure shows an example of hosting ObjectServer and Network Manager failover using five host machines.

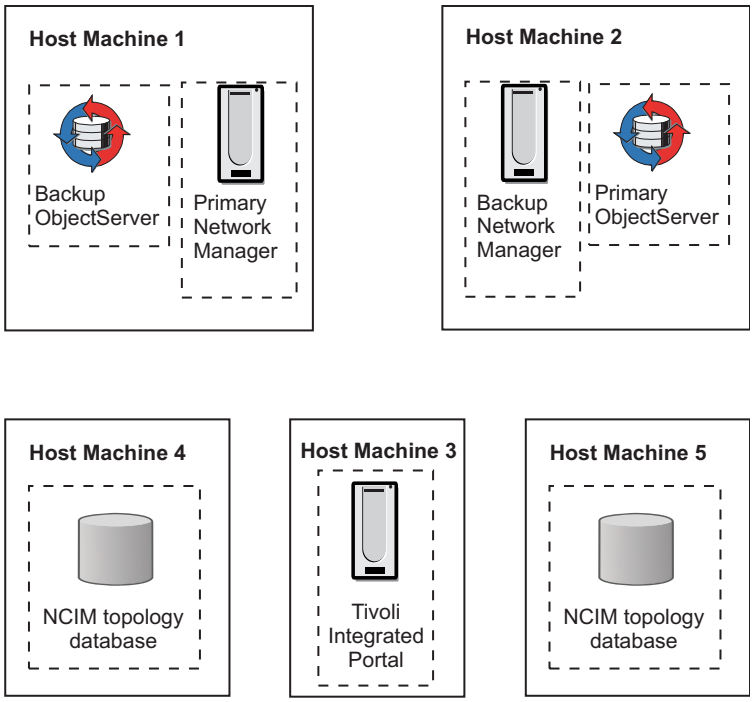

Figure 17. Example failover hosting with backup NCIM topology database

For performance reasons, the NCIM topology database requires a high bandwidth connection to the Tivoli Integrated Portal server. If host machine 3 has multiple CPUs and sufficient memory, you can install the primary NCIM on host machine 3.

Install the core components on both host machines 1 and 2, and install the Web applications on host machine 3. Install the primary NCIM topology database on host machine 4 and the backup NCIM topology database on host machine 5.

Failover operation of the Network Manager core processes

Failover of the Network Manager core processes is managed by the Virtual Domain process, **ncp_virtualdomain**. Use this information to understand how Network Manager failover and failback are triggered.

Health check events and failover

Failover is governed by health checks, which are configured to run periodically to assess the health of the primary and backup Network Manager domains.

In the failover environment, all the processes in the primary and backup domains are started by the master process controller, **ncp_ctrl**. In each domain, **ncp_ctrl** also regularly monitors the processes that are under its control, and stores their status in the state.services table. The Virtual Domain process applies filters (which are defined in the state.filters table) against the status records of some of the processes, and generates health check events to indicate whether a domain is healthy. The filters are applied to:

- **ncp_poller**, the Polling engine

  Multiple filters can be defined for the Polling engine, one for each poller defined in the `CtrlServices.cfg` file.
- **ncp_g_event**, the Event Gateway
- **ncp_model**, the topology manager

Health check events are generated locally within each domain, and can also be generated remotely by one domain on behalf of the other:

- Local domain: If every status record passes the filters, the Network Manager server is deemed healthy, and Virtual Domain generates a health check resolution event for that domain. Each domain indicates to the other that it is healthy, by sending a resolution event, which is routed via the ObjectServer. A domain expects to receive a resolution event at an interval configured in the Virtual Domain process schema file (`$NCHOME/etc/precision/VirtualDomainSchema.cfg`).

  If one or more filters fail, indicating the failure of one or more local processes, Virtual Domain generates a health check problem event, and additionally routes the problem event to the other domain.
- Remote domain: If a local domain detects that its remote counterpart has not generated a health check resolution event in the configured interval, the local domain generates a synthetic health check problem event for the remote domain. For example, if the backup domain does not receive a health check resolution event from the primary domain, the backup domain generates a health check problem event for the primary domain.

Health check events are also generated when connectivity to the NCIM database is lost.

Health check events have the event identifier "ItnmHealthChk" in the EventId field of the alerts.status table.

Related concepts:

“Network Manager failover and failback” on page 290
Failover can be initiated by either the primary or backup domain, and is triggered when a health check problem event is generated for the primary domain. Failback is triggered by a subsequent health check resolution event for the primary domain.

Related tasks:

“Configuring parameters for health checks” on page 321
If required, you can configure preferred conditions under which health check events are generated, by specifying identical OQL inserts to the Virtual Domain process schema file (`VirtualDomainSchema.cfg`) on both the primary and backup servers.

Related reference:

"Network Manager status events" on page 163
Network Manager can generate events that show the status of various Network Manager processes. These events are known as Network Manager status events and have the alerts.status AlertGroup field value of `ITNM Status`.

Process flow for health check events:

Health check resolution events are generated by each Network Manager server to indicate that it is in good health. A health check problem event is one of the triggers for Network Manager failover.

The following figure shows the progression through the system of a health check event that is generated by the primary Network Manager server.

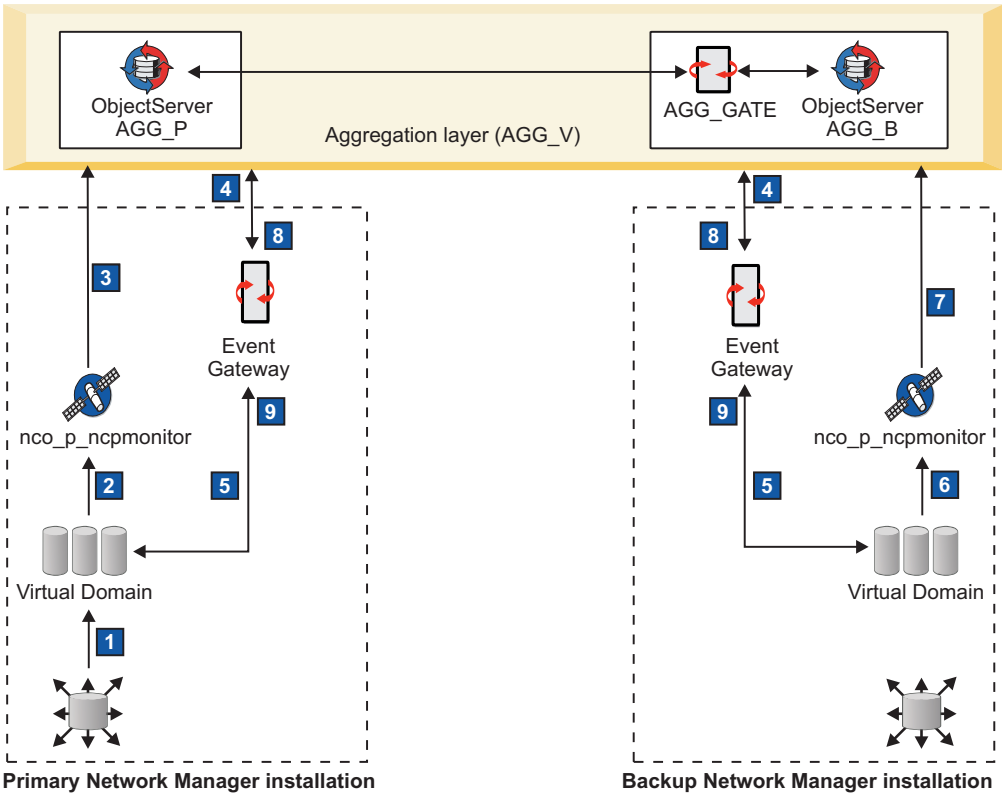

Figure 18. Process flow of a health check event

1 Status report

The **`ncp_ctrl`** process reports on the status of its managed services.

2 Health diagnosis

The Virtual Domain process uses its filters to perform a health check diagnosis:

- If the system is in good health, Virtual Domain generates a health check resolution event and sends it to the Probe for Tivoli Netcool/OMNIbus. By default, health check events are sent to the probe every 60 seconds.
- If the system is in poor health, Virtual Domain generates a health check problem event and sends it to the Probe for Tivoli Netcool/OMNIbus.

3 Health check event forwarded to the ObjectServer
The Probe for Tivoli Netcool/OMNIbus forwards the health check event to the ObjectServer.

4 Health check event forwarded to the primary and backup Event Gateway
The ObjectServer sends the health check event to the Event Gateway of the primary and backup servers.

5 Health check event sent back to the primary and backup Virtual Domain
The primary Event Gateway sends the health check event back to the Virtual Domain on the primary server. The backup Event Gateway also sends the health check event to the Virtual Domain on the backup server.

For a health check resolution event, Virtual Domain checks the time stamp on the event to ensure the event is not older than 5 minutes, and updates its state.domains table to show that the primary server is in good health. (The Event Gateway also listens for health check events from the backup server. The state.domains table records the current state of both primary and backup servers.)

For a health check problem event, Virtual Domain updates its state.domains table to show that the primary server is in poor health. Virtual Domain switches the backup server to active mode, and the primary server goes on standby.

6 Health check failure generated on behalf of primary domain
If the backup server does not receive a health check resolution event from the primary server within the configured interval of 5 minutes, this indicates that the primary server is not functioning properly or not communicating properly with the ObjectServer. The backup Virtual Domain sends a health check problem event to the Probe for Tivoli Netcool/OMNIbus on behalf of the primary server. Virtual Domain updates its state.domains table to show that the primary server is in poor health.

7 , 8 , and 9 Failover triggered
The probe sends the health check problem event to the ObjectServer, which then forwards the health check problem event to the Event Gateway on both the primary and backup Network Manager servers:

- The Event Gateway on the backup server sends the health check problem event to the Virtual Domain, which then switches the backup server to active mode.
- If the primary Event Gateway is operational, it forwards the health check problem event to the primary Virtual Domain. If Virtual Domain is operational, it switches the primary server to standby mode.

When the backup server generates a health check resolution event, the process flow is identical to that for the primary server. Regularly-updated health check resolution events for both primary and backup servers are held in the ObjectServer and can be viewed using, for example, the Active Event List (AEL).

If the health check problem event is generated by the backup server to indicate that the backup server is in poor health, the same processes apply, except that the primary server is not put on standby, and the backup server is not switched to active mode. The health check problem event for the backup server is present in the ObjectServer and can be viewed using, for example, the Active Event List.

Note: The Probe for Tivoli Netcool/OMNIbus and Event Gateway in both domains must be configured to access the same ObjectServer, in order for health check events to be successfully routed around the system.

Network Manager failover and failback

Failover can be initiated by either the primary or backup domain, and is triggered when a health check problem event is generated for the primary domain. Failback is triggered by a subsequent health check resolution event for the primary domain.

An ItnmFailover event is generated by **ncp_virtualdomain** when a Network Manager domain fails over or fails back.

Failing over

When failover occurs, the primary Network Manager domain goes into standby mode (if it is still running), and the backup domain becomes active.

The following changes occur when the backup domain becomes active:

- The Event Gateway synchronizes the events with the ObjectServer.
- The **ncp_poller** process resumes polling.
- The Event Gateway switches from the standby filter (StandbyEventFilter) to the incoming event filter (EventFilter).
- Network Manager continues to monitor the network and perform RCA. However, network discovery is not performed, and the network topology remains static.

When a primary Network Manager server goes into standby mode, the following changes occur:

- The Event Gateway switches from the incoming event filter (EventFilter) to the standby filter (StandbyEventFilter).
- The **ncp_poller** process suspends all polls.

For further information about the standby filter and incoming event filter, see the *IBM Tivoli Network Manager IP Edition Event Management Guide*.

Failing back

When a primary Network Manager server in standby mode resumes normal operation, it generates a health check resolution event.

The health check resolution event passes through the system, and the recovered Network Manager server becomes active again.

When the Virtual Domain process on the backup Network Manager server receives the health check resolution event, Virtual Domain switches the backup server back to standby mode.

The GenericClear automation in the ObjectServer is triggered by the health check resolution event, and clears the existing health check problem event.

Related concepts:

"Health check events and failover" on page 287
Failover is governed by health checks, which are configured to run periodically to assess the health of the primary and backup Network Manager domains.

Failover on the backup installation without NCIM replication:

This failover configuration has no NCIM topology database on the backup installation.

When you install the backup server, the system automatically creates a network domain named Backup during the installation process. This is not a real domain, it is not used in NCIM, and users cannot take any action using this domain. Ensure that there is no such backup domain on the backup installation. If present, you can delete this domain using the `domain_drop.pl` script.

The following figure shows an example Network Manager failover architecture, where the NCIM topology database is not installed as part of the backup Network Manager installation.

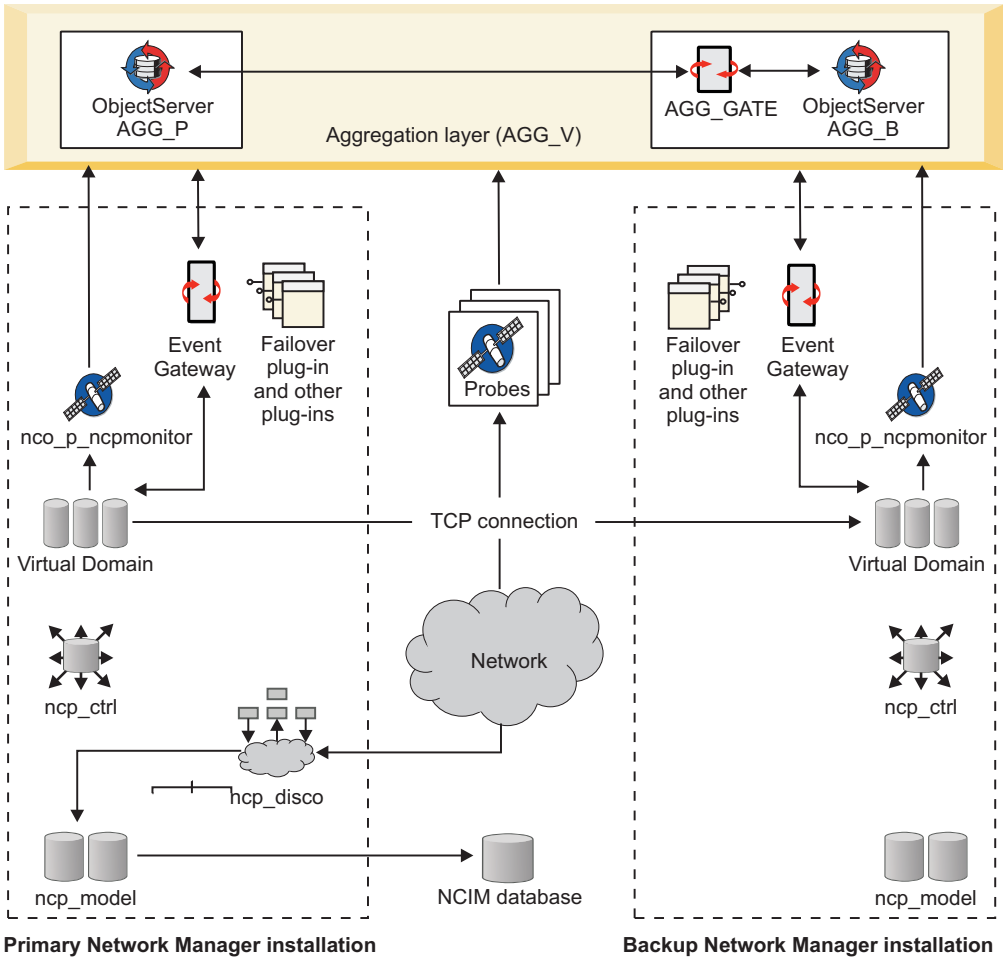

Figure 19. Example failover architecture

Discovery

Although the Discovery engine (**ncp_disco**) and the SNMP Helper Server (**ncp_d_helpserv**) are run, the backup Network Manager server is not used for network discovery. When the backup domain is active, the topology does not change.

Web applications
The Web applications do not automatically connect to the backup domain when it becomes active, but these applications can be manually configured to connect.

NCIM When failover is configured without NCIM replication, the backup **ncp_model** process does not update the NCIM database. However, the **ncp_model** process continues to provide topology services to processes such as the Event Gateway. The NCIM database used by the Network Views and the Hop View continues to hold the most current version of the network topology until the primary Network Manager server is restored and the system fails back.

Note: If you implement failover without NCIM replication and you entered SNMP community strings using the Discovery Configuration GUI, then you must ensure that both the primary and backup installations are using identical encryption keys. If the encryption keys are not identical, then the backup poller does not function correctly during failover. To ensure that both the primary and backup installations are using identical encryption keys, copy the following file from the primary server to the same location on the backup server: `$NCHOME/etc/security/keys/conf.key`. If you enter all SNMP community strings on the command line and do not encrypt them, you do not need to do this task. For more information on changing the encryption key, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Polling
When the backup domain is in standby mode, the Polling engine runs, but with polls suspended. When the backup domain becomes active, its **ncp_poller** process starts polling, and uses the SNMP target details and poll policies from the primary domain.

Virtual Domain
The Virtual Domain component opens a socket connection to the Virtual Domain of the primary Network Manager server. The topology data and any subsequent topology updates are copied from the **ncp_model** process on the primary server to the **ncp_model** process on the backup server.

Event Gateway
When the backup domain is in standby mode, the Event Gateway does not perform event enrichment on the ObjectServer. When the backup domain becomes active, the Event Gateway switches from the standby filter (StandbyEventFilter) to the incoming event filter (EventFilter).

Related concepts:

"Network Manager failover architecture (core processes)" on page 281
Failover of the Network Manager core processes can be implemented by setting up primary and backup Network Manager installations that run on different servers. Both installations can either connect to a single Tivoli Netcool/OMNIbus ObjectServer or to a virtual pair of ObjectServers.

Related reference:

"Limitations of the Network Manager failover process" on page 298
A number of limitations apply for the failover process.

Failover on the backup installation with NCIM replication:

This failover configuration includes a copy of the NCIM topology database on the backup installation. All processes on the backup installation point to the NCIM topology database on the backup installation.

The following figure shows an example Network Manager failover architecture, where the NCIM topology database is installed as part of the backup Network Manager installation.

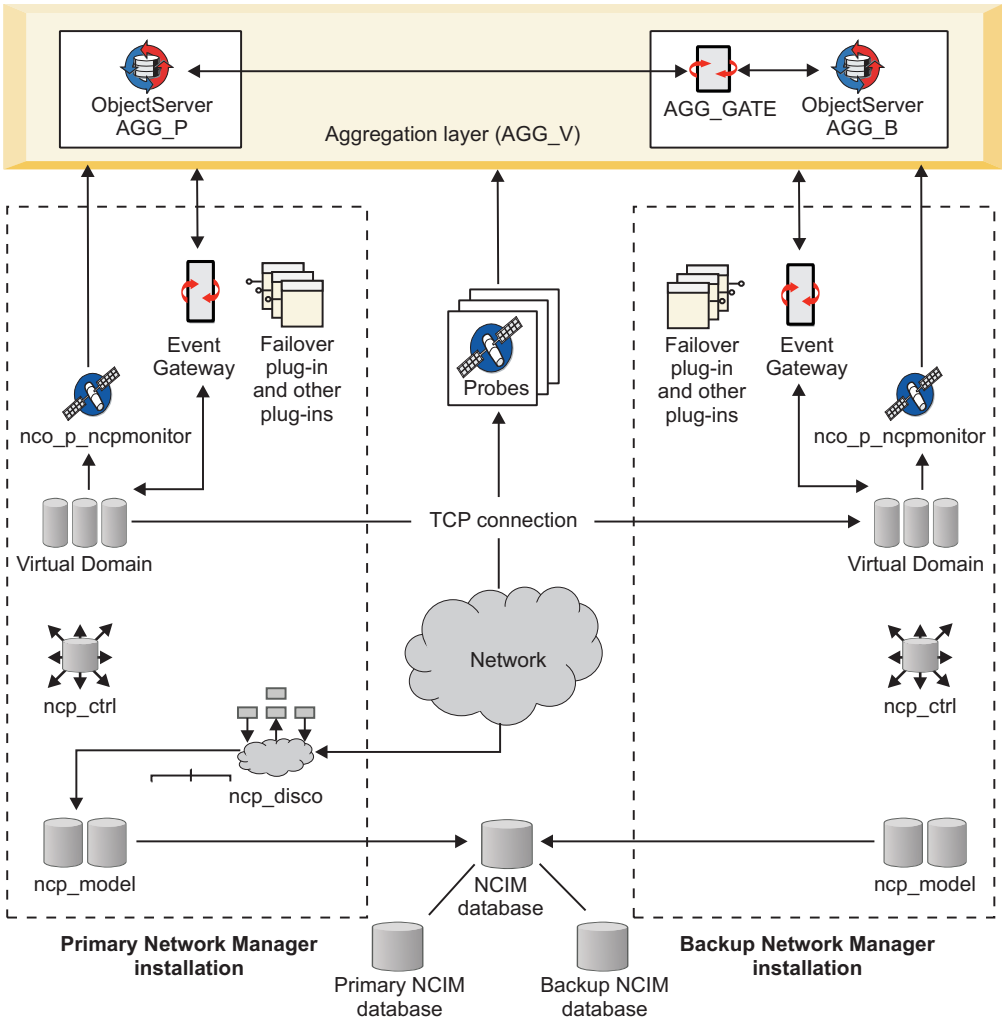

Figure 20. Example failover architecture

Discovery

Although the Discovery engine (**ncp_disco**) and the SNMP Helper Server (**ncp_d_helpserv**) are run, the backup Network Manager server is not used for network discovery. When the backup domain is active, the topology does not change.

Web applications

The Web applications do not automatically connect to the backup domain when it becomes active, but these applications can be manually configured to connect.

NCIM When failover is configured with NCIM replication, the **ncp_model** process

updates the NCIM database. The **ncp_model** process maintains the value of entityId for each entity in NCIM when transferring topology to the backup NCIM database. This ensures that the data in the backup NCIM topology database is an exact replica of the data in the primary NCIM database, and also ensures consistent event correlation when the backup installation takes over. Network topology views are also replicated on the backup. The NCIM database continues to hold the most current version of the network topology until the primary Network Manager server is restored and the system fails back.

Note: Topology views must be added, updated, or deleted only on the primary server. Any additions or changes to network views on the backup server while it is active, are not propagated to the primary server.

Virtual Domain

The Virtual Domain process opens a socket connection to the Virtual Domain of the primary Network Manager server. The topology data, and any subsequent topology updates, are copied from the **ncp_model** process on the primary Network Manager server to the **ncp_model** process on the backup Network Manager server.

Poll configuration data is also copied from the primary to the backup server. The Virtual Domain process on the primary server periodically checks the timestamp on the poller configuration file. If the file is seen to have been updated, Virtual Domain will transfer the file to the backup server and then call the `get_policies.pl` script using **ncp_ctrl** to import the poller configuration to the backup NCIM topology database.

The Virtual Domain component periodically checks the timestamp on the network view configuration file. If the file is seen to have been updated, Virtual Domain will transfer the file to the backup server and then call the `networkViewUtil.pl` script using **ncp_ctrl** to import the network view configuration to the backup NCIM topology database.

Polling

When the backup domain is in standby mode, the Polling engine runs, but with polls suspended. Because the SNMP configuration data (from the `SnmpStackSecurityInfo.cfg` file) and poll configuration data are copied from the primary to the backup domain when the TCP connection is established, and are updated at periodic intervals, polls are kept up to date in the backup domain.

Note:

- Only changes to active policies and related definitions are replicated to the backup server. For example, if you create a poll policy but do not enable it, the policy is not copied to the backup server.
- Polling policies must be added, updated, or deleted only on the primary server. Any poll policy additions or changes made on the backup server while it is active, are not propagated to the primary server.

The **ncp_poller** process reads the SNMP configuration directly from its configuration file rather than relying on the discovery SNMP helper to read this file.

Event Gateway

When the backup domain is in standby mode, the Event Gateway does not perform event enrichment on the ObjectServer. When the backup domain

becomes active, the Event Gateway switches from the standby filter (StandbyEventFilter) to the incoming event filter (EventFilter).

Related concepts:

"Network Manager failover architecture (core processes)" on page 281
Failover of the Network Manager core processes can be implemented by setting up primary and backup Network Manager installations that run on different servers. Both installations can either connect to a single Tivoli Netcool/OMNIbus ObjectServer or to a virtual pair of ObjectServers.

Related reference:

"Limitations of the Network Manager failover process" on page 298
A number of limitations apply for the failover process.

Failover on the backup installation: Fix Pack 4

All processes on the backup installation point to the NCIM topology database on the primary installation and this primary NCIM topology database can be a stand alone database or one configured for high availability.

Note: In previous Network Manager releases, users could include an NCIM topology database failover configuration by using NCIM replication (also referred to as NCIM topology database replication). The NCIM replication feature has been replaced by the high availability feature that is provided by the supported database:

- If you have a DB2 database, you can use the High Availability Disaster Recovery (HADR) feature to set up failover for NCIM.
- Fix Pack 5 If you have an Oracle database, you can use the Real Application Clusters (RAC) feature to set up failover for NCIM.

The DB2 HADR feature in Network Manager 3.9 Fix Pack 4 is available with DB2 9.7 and DB2 10.1.

The following figure shows an example Network Manager failover architecture, where the NCIM topology database is configured for high availability.

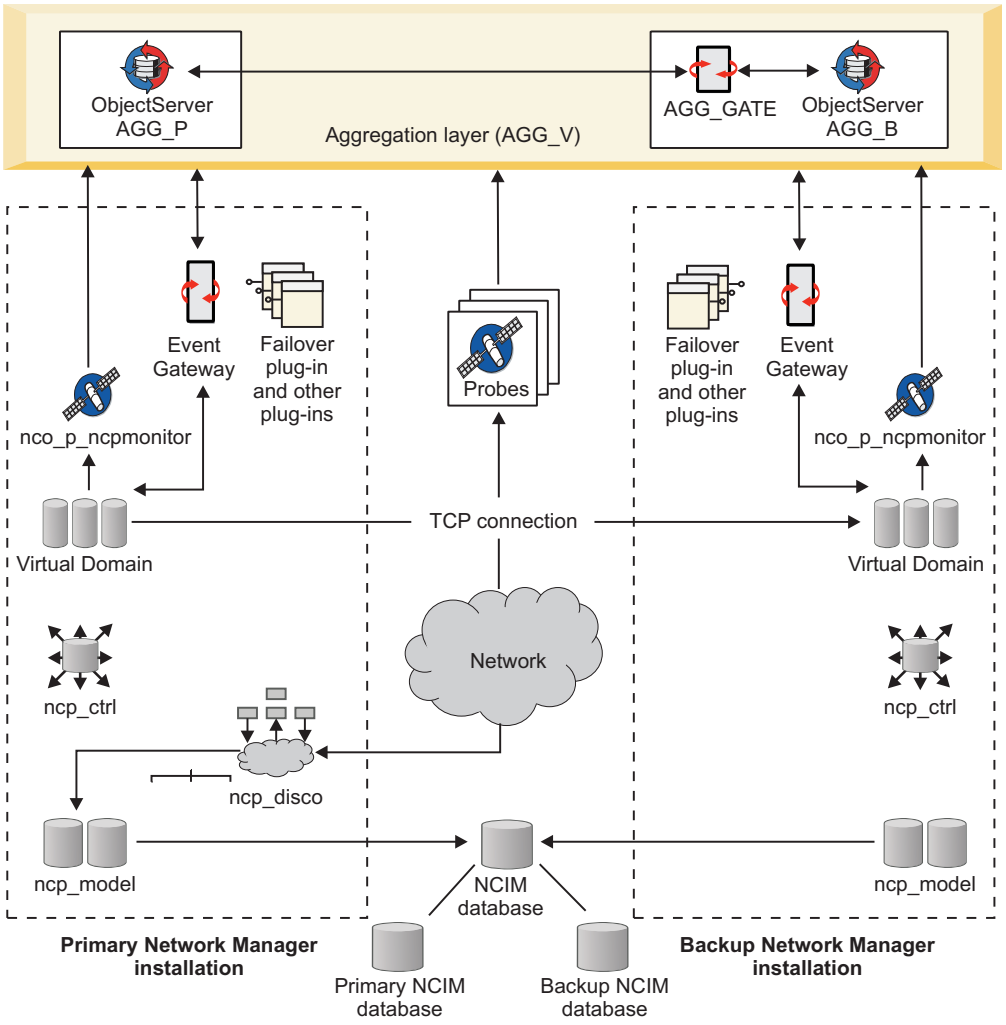

Figure 21. Example failover architecture with NCIM high availability

The following figure differs from the previous one in that the NCIM topology database is not configured for high availability.

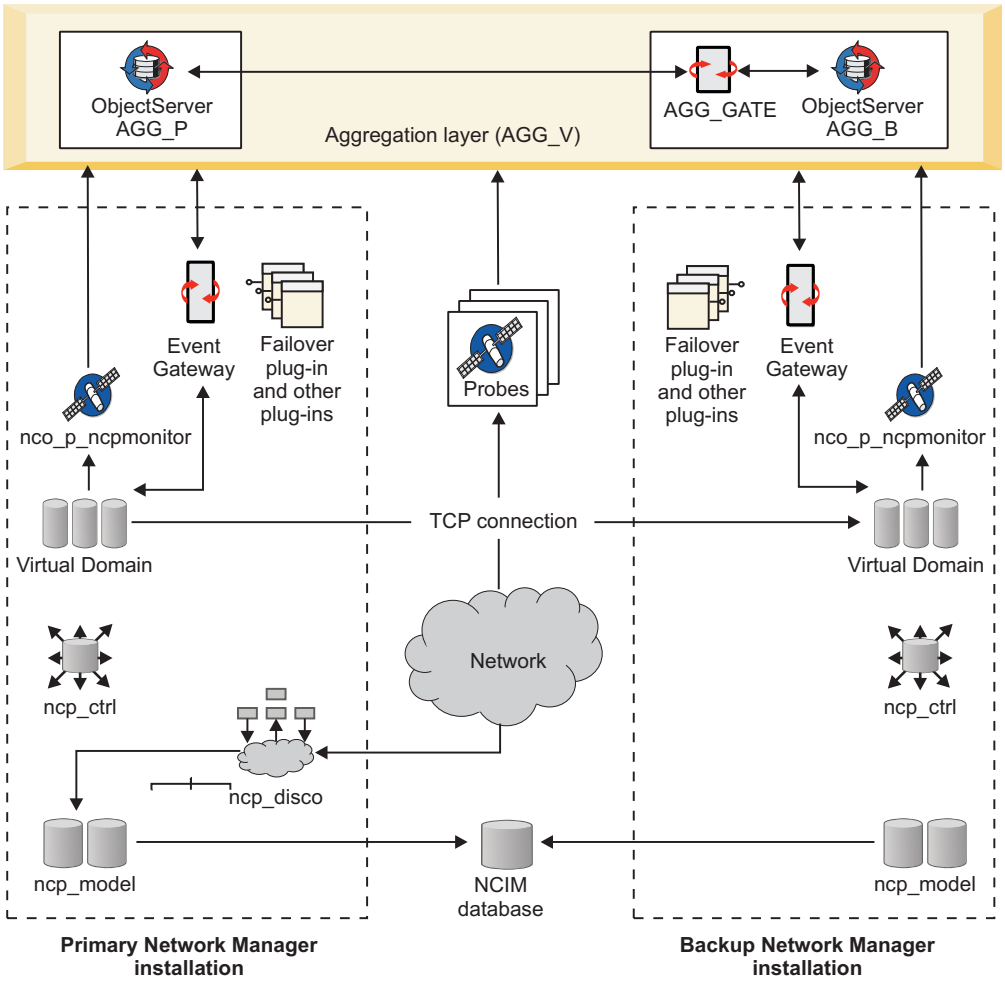

Figure 22. Example failover architecture without NCIM high availability

Discovery

Although the Discovery engine (**ncp_disco**) and the SNMP Helper Server (**ncp_d_helpserv**) are run, the backup Network Manager server is not used for network discovery. When the backup domain is active, the topology does not change.

NCIM The backup **ncp_model** process does not update the NCIM topology database. However, the **ncp_model** process continues to provide topology services to processes such as the Event Gateway. The NCIM topology database used by the Network Views and the Hop View continues to hold the most current version of the network topology until the primary Network Manager server is restored and the system fails back.

Polling

When the backup domain is in standby mode, the Polling engine runs, but with polls suspended. When the backup domain becomes active, its **ncp_poller** process starts polling, and uses the SNMP target details and poll policies from the primary domain.

The **ncp_poller** process reads the SNMP configuration directly from its configuration file rather than relying on the discovery SNMP helper to read this file.

Virtual Domain
The backup Virtual Domain component opens a socket connection to the Virtual Domain of the primary Network Manager server. The topology data and any subsequent topology updates are copied from the ncp_model process on the primary server to the **ncp_model** process on the backup server.

Event Gateway
When the backup domain is in standby mode, the Event Gateway does not perform event enrichment on the ObjectServer. When the backup domain becomes active, the Event Gateway switches from the standby filter (StandbyEventFilter) to the incoming event filter (EventFilter).

Related concepts:

"Network Manager failover architecture (core processes)" on page 281
Failover of the Network Manager core processes can be implemented by setting up primary and backup Network Manager installations that run on different servers. Both installations can either connect to a single Tivoli Netcool/OMNIbus ObjectServer or to a virtual pair of ObjectServers.

Fix Pack 4 "About NCIM topology database high availability" on page 276
Network Manager allows you to configure the Network Connectivity and Inventory Model (NCIM) topology database for high availability, minimizing the impact of computer or network failure. The following sections provide an overview of NCIM topology database high availability and explain how to configure it.

Related reference:

"Limitations of the Network Manager failover process"
A number of limitations apply for the failover process.

Limitations of the Network Manager failover process

A number of limitations apply for the failover process.

The discovery process (**ncp_disco**) performs network discovery only in the primary domain.

The backup domain is not used for network discovery, so when the backup domain is active, do not attempt to configure a discovery. Also, when the backup domain is active, do not edit the discovered network topology to manually add or remove devices and connections.

Restriction: Network Manager does not support the Tivoli Integrated Portal load balancing feature that the Tivoli Netcool/OMNIbus Web GUI does.

If you are running more than one Tivoli Integrated Portal server, they each run independently. If one of the Tivoli Integrated Portal servers fails, any remaining servers continue to run as individual entities. To minimize the effect of a server failing:

- Set up each Tivoli Integrated Portal server with its own unique URL for authentication.
- Ensure that each of the servers is configured with the same set of users, roles, groups, preference profiles, and resources such as pages, views, portlets, and reports.
- Configure the servers to whatever the database high availability requires. For example, for DB2 you would configure the servers according the requirements of

the DB2 HADR feature. Fix Pack 5 Similarly, if you have a Oracle database, you would configure the servers according to the requirements of the Real Application Clusters (RAC) feature.

Note: Failover is not supported for the ITM monitoring agents in the Network Manager failover architecture.

Related tasks:

"Configuring failover of the Network Manager core processes" on page 307
You can configure failover of the Network Manager core processes by using the `$NCHOME/etc/precision/ConfigItnm.cfg` file to enable failover.

Related information:

IBM DB2 Version 10.1 Information Center
For more information on DB2 10.1 HADR, search the IBM DB2 Version 10.1 Information Center. Suggested search terms include "high availability".

IBM DB2 Version 9.7 Information Center
For more information on DB2 9.7 HADR, search the IBM DB2 Version 9.7 Information Center. Suggested search terms include "high availability".

Oracle Database Online Documentation

Configuring failover

Use this information to configure failover in your primary and backup Network Manager installations. Guidelines are also provided to optionally configure failover of the integrating products and components. You must use the documentation for these products and components as the first point of reference.

Before you begin to configure failover, determine whether you want to implement a complete failover solution for all the components, or failover for Network Manager and a subset of components. Also decide on the number of computers and the deployment options.

As a prerequisite to configuring failover:

- You must have installed and configured IBM Tivoli Netcool/OMNIbus. If you intend to run a primary and backup ObjectServer in failover mode, you require two ObjectServer installations.

  Tip: If you are using IBM Tivoli Netcool/OMNIbus V7.3 or later, with the supplied failover configuration files, be sure to adhere to the naming conventions for your ObjectServers and ObjectServer Gateways.
- You must have installed a topology database. For NCIM replication, you require two topology databases.
- Fix Pack 4 For NCIM topology database high availability, you require two topology databases. Fix Pack 4

  Note: Users can include an NCIM topology database failover configuration by using NCIM replication (also referred to as NCIM topology database replication) or by using an NCIM topology database high availability feature that is provided by theDB2 database. Specifically, DB2 provides a feature called high availability disaster recovery (HADR) that you use to configure a failover configuration for the NCIM topology database.

TheDB2 HADR feature in Network Manager 3.9 Fix Pack 4 is available with DB2 9.7 and DB2 10.1.

- You must have installed and configured the Web GUI and the Network Manager Web applications within the Tivoli Integrated Portal server framework.
- You must have installed the Network Manager core processes on the designated primary and backup servers, under two separate domains.

Related concepts:

"About the Tivoli Netcool/OMNIbus failover configuration files" on page 280
Tivoli Netcool/OMNIbus V7.3 or later, provides a set of configuration files that you can apply to ObjectServers and ObjectServer Gateways in order to implement the multitiered architecture.

Related reference:

"Constraints for installing and starting components" on page 15
Some components must be installed and started before others. Use this information as well as the installation examples to understand the order in which you must install and start components.

Configuring ObjectServer failover

The way in which you configure ObjectServer failover is dependent on the Tivoli Netcool/OMNIbus version.

In a Tivoli Netcool/OMNIbus installation, each computer on which the Tivoli Netcool/OMNIbus components run must be configured with server communication information that enables the components in the architecture to run and communicate with one another. Configure the connections data file with all the component details, as follows:

- UNIX Linux Update the communication information for all the Tivoli Netcool/OMNIbus server components in your deployment by manually editing the connections data file `$NCHOME/etc/omni.dat`, which is used to create the interfaces file.

  A suggested good practice is to add all the components in the entire deployment to a single `omni.dat` file, which can then be distributed to the `$NCHOME/etc` directory in all the computers in the deployment. You can then generate the interfaces file from each computer by running the **`$NCHOME/bin/nco_igen`** command. (Interfaces files are named `$NCHOME/etc/interfaces.`*arch*, where *arch* is the operating system name.)

- Windows Configure server communication information on each computer by using the Server Editor, which is available by clicking **Start** > **All Programs** > **NETCOOL Suite** > **System Utilities** > **Servers Editor**. The information is saved in the connections data file `%NCHOME%\ini\sql.ini`.

Sample configuration for the basic failover architecture (aggregation layer only)

The following sample configuration shows the server communications details for the basic failover architecture in the `$NCHOME/etc/omni.dat` file, where:

- AGG_P is the name of the primary ObjectServer.
- AGG_B is the name of the backup ObjectServer.
- AGG_V is the name of the virtual ObjectServer pair.
- AGG_GATE is the name of the birdirectional ObjectServer Gateway.
- NCO_PA represents the default name for the process agent. (If you have configured process agents to manage the Tivoli Netcool/OMNIbus processes and

run external procedures, each uniquely-named process agent must be added with the appropriate host name and port number.)

- NCO_PROXY represents the default name for the proxy server. (If you have configured one or more proxy servers to reduce the number of direct probe connections to the ObjectServers, each uniquely-named proxy server must be added with the appropriate host name and port number.)

```
[AGG_P]
{
        Primary: primary_host.ibm.com 4100
}

[AGG_B]
{
        Primary: backup_host.ibm.com 4150
}

[AGG_V]
{
        Primary: primary_host.ibm.com 4100
        Backup: backup_host.ibm.com 4150
}

[AGG_GATE]
{
        Primary: backup_host.ibm.com 4105
}

[NCO_PA]
{
        Primary: primary_host.ibm.com 4200
}

[NCO_PROXY]
{
        Primary: primary_host.ibm.com 4400
}
```

For further details about configuring server communication information, process agents, and proxy servers, see the Tivoli Netcool/OMNIbus documentation at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm.

Related concepts:

"ObjectServer failover architecture" on page 279
You can deploy Tivoli Netcool/OMNIbus by using a scalable multitiered architecture, so that the system can continue to operate to full capacity (and with minimal event loss) in the event of ObjectServer, ObjectServer Gateway, or proxy server failure.

Configuring ObjectServers and gateways for failover:

The following procedures provide guidance for setting up ObjectServer failover in Tivoli Netcool/OMNIbus.

"Tivoli Netcool/OMNIbus V7.3 or later" on page 302: Configuring failover
"Tivoli Netcool/OMNIbus V7.2.1 or earlier" on page 303: Configuring failover

For the most recent and complete information about ObjectServer failover, see the Tivoli Netcool/OMNIbus documentation at http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html. The Tivoli Netcool/OMNIbus documentation should always be the first point of reference,

and takes precedence over the information shown in the Network Manager documentation.

Tivoli Netcool/OMNIbus V7.3 or later:
To configure failover:

1. If not yet done, create the primary aggregation ObjectServer AGG_P on the designated computer, and apply the SQL customization by running the **nco_dbinit** command with the supplied `aggregation.sql` import file:

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server AGG_P -customconfigfile
   $NCHOME/omnibus/extensions/multitier/objectserver/aggregation.sql
   ```

   If the ObjectServer is already installed and running, apply the `aggregation.sql` import file against the ObjectServer, as follows:

   UNIX Linux
   ```
   $NCHOME/omnibus/bin/nco_sql -server AGG_P -user
   user_name –password password < $NCHOME/omnibus/extensions/multitier/
   objectserver/aggregation.sql
   ```

   Windows
   ```
   "%NCHOME%\omnibus\bin\isql" -S AGG_P -U user_name -P password
   -i "%NCHOME%\omnibus\extensions\multitier\objectserver\aggregation.sql"
   ```

2. Start the primary ObjectServer (if necessary):

   ```
   $NCHOME/omnibus/bin/nco_objserv -name AGG_P &
   ```

   If you installed Tivoli Netcool/OMNIbus using the Network Manager installer, you can, as an alternative, run the **itnm_start** command in the `$NCHOME/precision/bin` directory:

   UNIX Linux
   ```
   itnm_start nco
   ```

3. Create (or update) the backup aggregation ObjectServer AGG_B on another computer, and apply the SQL customization, as described in step 1. When you apply the SQL customization, the **BackupObjectServer** property is automatically set to `TRUE` and the automations required by the backup ObjectServer are enabled.
4. Start the backup ObjectServer (if necessary), as described in step 2.
5. On the computer where the backup ObjectServer is installed, configure the bidirectional aggregation ObjectServer Gateway AGG_GATE:
   a. Copy the multitiered property files for the gateway from the `$NCHOME/omnibus/extensions/multitier/gateway` location, to the default location (`$NCHOME/omnibus/etc`) where configuration and properties files are held:
      - `AGG_GATE.map`
      - `AGG_GATE.props`
      - `AGG_GATE.tblrep.def`

   b. Start the gateway AGG_GATE:

      ```
      $NCHOME/omnibus/bin/nco_g_objserv_bi -propsfile $NCHOME/omnibus/etc/
      AGG_GATE.props &
      ```

Tivoli Netcool/OMNIbus V7.2.1 or earlier:
To configure failover:

1. If not yet done, create the primary ObjectServer on the designated computer by running the **nco_dbinit** command:

   ```
   $NCHOME/omnibus/bin/nco_dbinit -server server_name
   ```

   Where *server_name* is the designated name; for example, NETCOOLPRI.
2. Start the primary ObjectServer (if necessary):

   ```
   $NCHOME/omnibus/bin/nco_objserv -name server_name &
   ```
3. If not yet done, create the backup ObjectServer on another computer, as described in step 1.
4. Configure the backup ObjectServer by editing its properties file ($NCHOME/omnibus/etc/*server_name*.props), and set the **BackupObjectServer** property to True.
5. Start the backup ObjectServer, as described in step 2.
6. On the computer where the backup ObjectServer is installed, configure the bidirectional ObjectServer Gateway to exchange alert data between the primary and backup ObjectServers:
   a. Create the directory $NCHOME/omnibus/gates/*gateway_name*, for the gateway configuration files.
   b. Copy all of the files in $NCHOME/omnibus/gates/objserv_bi to the $NCHOME/omnibus/gates/*gateway_name* directory.
   c. Rename the $NCHOME/omnibus/gates/*gateway_name*/objserv_bi.map file to *gateway_name*.map.
   d. Rename the $NCHOME/omnibus/gates/*gateway_name*/objserv_bi.props file to *gateway_name*.props.
   e. Edit the following entries in the *gateway_name*.props file:

      ```
      # Common Netcool/OMNIbus Properties.
      MessageLog   : '$OMNIHOME/log/gateway_name.log'

      # Common Gateway Properties.
      Gate.MapFile   : '$OMNIHOME/gates/gateway_name/gateway_name.map'
      Gate.StartupCmdFile  : '$OMNIHOME/gates/gateway_name/objserv_bi.startup.cmd'

      # Bidirectional ObjectServer Gateway Properties.
      Gate.ObjectServerA.Server  : 'primary_ObjectServer'
      Gate.ObjectServerA.Username  : 'user_name'
      Gate.ObjectServerA.Password  : 'password'
      Gate.ObjectServerA.TblReplicateDefFile:
         '$OMNIHOME/gates/gateway_name/objserv_bi.objectservera.tblrep.def'

      Gate.ObjectServerB.Server  : 'backup_ObjectServer'
      Gate.ObjectServerB.Username  : 'user_name'
      Gate.ObjectServerB.Password  : 'password'
      Gate.ObjectServerB.TblReplicateDefFile:
         '$OMNIHOME/gates/gateway_name/objserv_bi.objectserverb.tblrep.def'
      ```

      Substitute *gateway_name* with the name assigned to the gateway, *primary_ObjectServer* and *backup_ObjectServer* with the ObjectServer names, and specify the user name and password for connecting to the ObjectServers.
   f. Copy the $NCHOME/omnibus/gates/*gateway_name*/*gateway_name*.props file to $NCHOME/omnibus/etc/*gateway_name*.props.
   g. Start the gateway:

      ```
      $NCHOME/omnibus/bin/nco_g_objserv_bi &
      ```

Connecting to an ObjectServer failover pair

Each Network Manager installation that connects to an ObjectServer needs a copy of the Tivoli Netcool/OMNIbus interfaces file (on UNIX or Linux), or connections data file (on Windows).

Assuming that server communication information has been configured in your Tivoli Netcool/OMNIbus installations, the `$NCHOME/etc/interfaces.arch` file (where *arch* represents the operating system name), or `%NCHOME%\ini\sql.ini` file should be available in the NCHOME installation location.

To ensure that Network Manager processes can connect to an ObjectServer failover pair, perform either of the following steps on the primary and backup Network Manager servers:

- If Network Manager and Tivoli Netcool/OMNIbus are installed on the same computer, but in different NCHOME locations, copy the `$NCHOME/etc/interfaces.arch` file or `%NCHOME%\ini\sql.ini` file from the Tivoli Netcool/OMNIbus NCHOME location to the NCHOME installation location for Network Manager. If the two products are installed in the same NCHOME location, no action needs to be taken.
- If Network Manager and Tivoli Netcool/OMNIbus are installed on different computers, copy the `$NCHOME/etc/interfaces.arch` file or `%NCHOME%\ini\sql.ini` file from the Tivoli Netcool/OMNIbus NCHOME location to the NCHOME installation location on the computer where Network Manager is installed.

  For more information about configuring server communication information and generating the Tivoli Netcool/OMNIbus `interfaces.arch` file or `sql.ini` file, see the Tivoli Netcool/OMNIbus documentation at http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html.

Related tasks:

"Configuring ObjectServer failover" on page 300
The way in which you configure ObjectServer failover is dependent on the Tivoli Netcool/OMNIbus version.

"Configuring failover using the ConfigItnm.cfg file" on page 308
When you use the `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` file to configure failover, the Network Manager processes will read the file on startup to identify whether they are running in the primary or backup domain. Similarly, the **ncp_model** process will identify whether NCIM replication is in use, and run appropriately for that configuration.

Configuring data source failover for the Tivoli Netcool/OMNIbus Web GUI

If you have a failover pair of ObjectServers to which the Web GUI should connect, you can configure data source failover by using the `ncwDataSourceDefinitions.xml` data source configuration file in your Web GUI installation.

This file is located in *webgui_home_dir*`/etc/datasources`, where *webgui_home_dir* is the installation directory for the Web GUI V7.3.1; for example, `$NCHOME/omnibus_webgui`.

To configure data source failover:

1. On the Tivoli Integrated Portal server where the Web GUI is installed, edit the data source configuration file as follows:
   a. Use the `name` attribute of the <ncwDataSourceEntry> element to specify a label for the failover pair of ObjectServers; for example, `VirtualObjectServerPair`.

b. Define the connection details for the primary and backup ObjectServers by using the <ncwDataSourceDefinition> element and its child elements.

   Note: The `name` attribute values of both the <ncwDataSourceEntry> and <ncwDataSourceDefinition> elements must be identical. You must also define the ObjectServer connections by using the ObjectServer host names and port numbers, rather than the ObjectServer names that are configured in the `omni.dat` or `sql.ini` file.

   For an example of the configuration required, see the sample code in "Sample ncwDataSourceDefinitions.xml configuration for data source failover" on page 306.

c. Restart the Tivoli Integrated Portal server for the changes to take effect. Use one of the following commands or methods:

   - UNIX Linux `itnm_start tip`
   - UNIX Linux `startServer.sh server1`
   - Windows `startServer.bat server1`
   - Windows From the Windows Control Panel, double-click **Administrative Tools** and then **Services**. From the Services window, locate, and start, the **Tivoli Integrated Portal** service.

   For the most recent and complete information about configuring data source failover in the Web GUI, see the Tivoli Netcool/OMNIbus Web GUI documentation at http://www-01.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html. The Web GUI documentation should always be the first point of reference, and takes precedence over the information shown in the Network Manager documentation.

2. You must also set WebTopDataSource value in `ModelNcimDb.`*`domain_name`*`.cfg` file to the same value as the <ncwDataSourceEntry> is set to in the `ncwDataSourceDefinitions.xml` file. Using the settings in the "Sample ncwDataSourceDefinitions.xml configuration for data source failover" on page 306, the following example shows what changes you need to make:

   a. Go to `NCHOME/etc/precision/ModelNcimDb.`*`domain_name`*`.cfg` file and open it for editing.

   b. Find the insert that defines the WebTopDataSource:

```
insert into dbModel.access
(
EnumGroupFilter,
TransactionLength,
ValidateCacheFile,
WebTopDataSource
)
values
(
"enumGroup in ('ifAdminStatus', 'ifOperStatus', 'sysServices', 'ifType',
'cefcFRUPowerAdminStatus', 'cefcFRUPowerOperStatus', 'TruthValue',
'entSensorType', 'entSensorScale', 'entSensorStatus',
'cefcModuleAdminStatus', 'cefcModuleOperStatus', 'ipForwarding',
'cefcPowerRedundancyMode', 'EntityType', 'ospfIfState', 'ospfIfType',
'dot3StatsDuplexStatus', 'accessProtocol')",
500,
0,
"OS"
);
```

   c. Change the WebTopDataSource value in the following insert query to match the data source configured in the <ncwDataSourceEntry> (in this case, change the value `OS` to `VirtualObjectServerPair`):

```
insert into dbModel.access
(
EnumGroupFilter,
TransactionLength,
ValidateCacheFile,
WebTopDataSource
)
values
(
"enumGroup in ('ifAdminStatus', 'ifOperStatus', 'sysServices', 'ifType',
'cefcFRUPowerAdminStatus', 'cefcFRUPowerOperStatus', 'TruthValue',
'entSensorType', 'entSensorScale', 'entSensorStatus',
'cefcModuleAdminStatus', 'cefcModuleOperStatus', 'ipForwarding',
'cefcPowerRedundancyMode', 'EntityType', 'ospfIfState', 'ospfIfType',
'dot3StatsDuplexStatus', 'accessProtocol')",
500,
0,
"VirtualObjectServerPair"
);
```

Note: The Web GUI data source name is the name for the connection, and it has to be the same as what is set in the Web GUI. The name might not always be the same as the ObjectServer name.

d. Make this change on both the primary and backup core Network Manager servers.

e. Restart ncp_ctrl.

Sample ncwDataSourceDefinitions.xml configuration for data source failover

In the following sample code, the bold text identifies the values that are applicable to data source failover.

```
<ncwDefaultDataSourceList>
    <ncwDataSourceEntry name="VirtualObjectServerPair"/>
</ncwDefaultDataSourceList>

...

<ncwDataSourceDefinition type="singleServerOSDataSource" name="VirtualObjectServerPair" enabled="true">
    <ncwFailOverPairDefinition>
        <!--
         ! The primary ObjectServer to connect to.
         ! - host : The hostname or IP address of the server the ObjectServer is installed on.
         ! - port : The port number the ObjectServer is listening on.
         ! - ssl  : Enables SSL connection to the ObjectServer. [false|true]
         ! - minPoolSize : Specifies the minimum number of connections that will be added to the connection pool. Default value is 5.
         ! - maxPoolSize : Specifies the maximum number of connections that will be added to the connection pool. Default value is 10.
         !-->
        <ncwPrimaryServer>
            <ncwOSConnection host="AGG_P_hostname" port="AGG_P_port" ssl="false" minPoolSize="5" maxPoolSize="10"/>
        </ncwPrimaryServer>
        <!--
         ! The optional failover ObjectServer to connect to.
         !-->
        <ncwBackUpServer>
            <ncwOSConnection host="AGG_B_hostname" port="AGG_B_port" ssl="false" minPoolSize="5" maxPoolSize="10"/>
        </ncwBackUpServer>
</ncwFailOverPairDefinition>

</ncwDataSourceDefinition>
```

Configuring ObjectServer authentication

If you are using an ObjectServer as the central user registry for user management and authentication, and you want the ObjectServer to be in a federated repository, you must use the script provided with Tivoli Integrated Portal to configure the Virtual Member Manager adapter for the ObjectServer. Configure the adapter for both of the ObjectServers in the failover pair.

On each Tivoli Integrated Portal server where the Network Manager Web applications and the Web GUI are installed:

1. Go to the *tip_home_dir*/bin directory.
2. Enter the following command at the command line:

   confvmm4ncos *user password address port address2 port2*

   Where:

   - *user* is the ID of a user with administrative privileges for the ObjectServers.
   - *password* is the password for the user ID.
   - *address* is the IP address of the primary ObjectServer.
   - *port* is the port number used by the primary ObjectServer.
   - *address2* is the IP address of the backup ObjectServer.
   - *port2* is the port number used by the backup ObjectServer.
3. Restart the Tivoli Integrated Portal server by using one of the following commands or methods:

   - UNIX Linux `itnm_start tip`
   - UNIX Linux `startServer.sh server1`
   - Windows `startServer.bat server1`
   - Windows From the Windows Control Panel, double-click **Administrative Tools** and then **Services**. From the Services window, locate, and start, the **Tivoli Integrated Portal** service.

Configuring failover of the Network Manager core processes

You can configure failover of the Network Manager core processes by using the $NCHOME/etc/precision/ConfigItnm.cfg file to enable failover.

You must also use the $NCHOME/etc/precision/ServiceData.cfg file to set up a TCP socket connection between the primary and backup Network Manager domains.

Related concepts:

"Network Manager failover architecture (core processes)" on page 281
Failover of the Network Manager core processes can be implemented by setting up primary and backup Network Manager installations that run on different servers. Both installations can either connect to a single Tivoli Netcool/OMNIbus ObjectServer or to a virtual pair of ObjectServers.

Configuring failover using the ConfigItnm.cfg file:

When you use the $NCHOME/etc/precision/ConfigItnm.*DOMAIN*.cfg file to configure failover, the Network Manager processes will read the file on startup to identify whether they are running in the primary or backup domain. Similarly, the **ncp_model** process will identify whether NCIM replication is in use, and run appropriately for that configuration.

The ConfigItnm.*DOMAIN*.cfg file contents must be identical on both the primary and backup domain servers.

To configure failover by using the ConfigItnm.*DOMAIN*.cfg file:

1. On the primary Network Manager server, edit the $NCHOME/etc/precision/ConfigItnm.*PRIMARY_DOMAIN*.cfg file as follows:
   a. Enable failover and optionally enable NCIM replication, and specify the primary, backup, and virtual domain names for the Network Manager processes. You can insert the required values in the itnmDomain.failover table by editing the following section in the file:

```
insert into itnmDomain.failover
(
    FailoverEnabled,
    IsReplicatingNcim,
    PrimaryDomainName,
    BackupDomainName,
    VirtualDomainName
)
values
(
    0,
    0,
    "NCOMS_P",
    "NCOMS_B",
    "NCOMS_V"
);
```

   Complete the values section as follows, in the order listed:

Column	Required value
FailoverEnabled	Specify 1 to enable failover for the defined primary and backup domains. The default value of 0 means that failover is disabled.
IsReplicatingNcim	Specify 1 to forceNetwork Manager to replicate the NCIM topology database in the primary domain to a second independent NCIM database in the backup domain. The default value of 0 means that both domains will share the same NCIM database and that Network Manager will not replicate the NCIM topology database.
PrimaryDomainName	Replace NCOMS_P with the actual name of the Network Manager primary domain in the failover pair.
BackupDomainName	Replace NCOMS_B with the actual name of the Network Manager backup domain in the failover pair.
VirtualDomainName	Replace NCOMS_V with a designated name for the Network Manager virtual domain in the failover pair.

b. Specify the name of the ObjectServer to which the Probe for Tivoli Netcool/OMNIbus and the Event Gateway will connect. Insert the required value in the `itnmDomain.objectServer` table by editing the following section in the file:

```
insert into itnmDomain.objectServer
(
    ServerName
)
values
(
    "NCOMS"
);
```

Complete the `values` section as follows:

Column	Required value
`ServerName`	If you are using Tivoli Netcool/OMNIbus V7.3 or later, and have configured ObjectServer failover using the supplied multitiered configuration files and naming conventions for the multitiered configuration, specify `AGG_V` as the name of the virtual aggregation pair. The initial value shown is either the name of the ObjectServer that was installed by the Network Manager installer, or `NCOMS` if no ObjectServer was installed. For earlier versions of Tivoli Netcool/OMNIbus, specify the alternative name defined for the ObjectServer virtual pair. If ObjectServer failover is not configured, specify the name of the single ObjectServer being used.

Note: No additional failover configuration is required in the probe properties file. The default probe property settings provide adequate support for failover when the probe runs.

2. Save the file.
3. Copy the entire contents of the `$NCHOME/etc/precision/ConfigItnm.`*`PRIMARY_DOMAIN`*`.cfg` file on the primary server to the `$NCHOME/etc/precision/ConfigItnm.`*`BACKUP_DOMAIN`*`.cfg` file on the backup server.

Related tasks:

"Configuring failover using the CtrlServices.cfg file" on page 310
The `$NCHOME/etc/precision/CtrlServices.cfg` file for the master process controller, **`ncp_ctrl`**, provides an alternative method for configuring failover of the Network Manager core components. This file requires individual command-line options to be specified for the **`ncp_virtualdomain`**, **`ncp_model`**, **`ncp_g_event`**, and **`ncp_poller`** processes in the primary and backup domain servers.

Configuring failover using the CtrlServices.cfg file:

The $NCHOME/etc/precision/CtrlServices.cfg file for the master process controller, **ncp_ctrl**, provides an alternative method for configuring failover of the Network Manager core components. This file requires individual command-line options to be specified for the **ncp_virtualdomain**, **ncp_model**, **ncp_g_event**, and **ncp_poller** processes in the primary and backup domain servers.

Note: Usage of the failover command-line options such as -virtualDomain and -backupDomain in the CtrlServices.cfg file is retained mainly for compatibility with earlier versions of Network Manager. The preferred method for configuring failover is to use the $NCHOME/etc/precision/ConfigItnm.*DOMAIN*.cfg file.

If you require information about configuring failover using the CtrlServices.cfg file, see the Network Manager V3.8 documentation at http://www-01.ibm.com/support/knowledgecenter/SSSHRK_3.8.0/com.ibm.networkmanagerip.doc_3.8/itnm/ip/wip/install/task/nmip_ins_conffailoverprocessctrl.html.

Related tasks:

"Configuring failover using the ConfigItnm.cfg file" on page 308
When you use the $NCHOME/etc/precision/ConfigItnm.*DOMAIN*.cfg file to configure failover, the Network Manager processes will read the file on startup to identify whether they are running in the primary or backup domain. Similarly, the **ncp_model** process will identify whether NCIM replication is in use, and run appropriately for that configuration.

"Switching to failover configuration with NCIM topology database high availability" on page 312
You can modify an existing failover architecture to include NCIM topology database high availability.

Configuring the TCP socket connection between the domains:

A TCP socket connection is required between the Virtual Domain processes in the primary and backup domains so that the topology data and topology updates can be copied to the backup domain.

To configure the TCP connection:

1. On the primary Network Manager server, manually start the **ncp_virtualdomain** process from the $NCHOME/precision/bin directory:

   ```
   ncp_virtualdomain -domain PRIMARYDOMAIN_NAME
   ```

   When the **ncp_virtualdomain** process starts for the first time, it writes a line to the $NCHOME/etc/precision/ServiceData.cfg file, which lists TCP and multicast connection information for Network Manager processes. This line references ncp_virtualdomain, and includes the port on which the Virtual Domain component on the primary server accepts TCP connections from the backup server. For example:

   ```
   SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ADDRESS: 127.123.209.55 PORT: 1234
    SERVERNAME: myhostname DYNAMIC: NO
   ```

   Tip: The DYNAMIC:NO setting forces the **ncp_virtualdomain** process to use the same address and port the next time that it starts.
2. Save the file.
3. Stop the **ncp_virtualdomain** process.
4. Copy the SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ... line from the $NCHOME/etc/precision/ServiceData.cfg file on the primary server into the

$NCHOME/etc/precision/ServiceData.cfg file on the backup server. Ensure that only a single SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ... line is present in the file.

Important: The SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ... line must be identical in the $NCHOME/etc/precision/ServiceData.cfg file in both domains.

For further information about inter-process communication and the ServiceData.cfg file, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Related tasks:

"Defining a fixed port for the TCP socket connection"
To avoid firewall issues or port conflicts, you can define a fixed port for the TCP socket connection that enables the Virtual Domain process on the backup server to connect to the process on the primary server.

Defining a fixed port for the TCP socket connection:

To avoid firewall issues or port conflicts, you can define a fixed port for the TCP socket connection that enables the Virtual Domain process on the backup server to connect to the process on the primary server.

On initial startup, the **ncp_virtualdomain** process on the primary server adds a line to the NCHOME/etc/precision/ServiceData.cfg file, with information about its connection details, including the port number. To define a fixed port, you must replace the initial port number with your required value.

To configure a fixed port for failover:

1. Edit the $NCHOME/etc/precision/ServiceData.cfg file on the primary server as follows:
   a. Locate the line that references ncp_virtualdomain. For example:

      ```
      SERVICE: ncp_virtualdomain DOMAIN: VIRTUAL ADDRESS: 127.123.209.55
       PORT: 1234 SERVERNAME: myhostname DYNAMIC: NO
      ```

      In this example, the primary **ncp_virtualdomain** process accepts connections from the backup on port 1234.
   b. Change the PORT setting to the required value.
   c. Make a note of the port number, and save and close the ServiceData.cfg file.
2. On the backup server, edit the $NCHOME/etc/precision/ServiceData.cfg file by updating the port number specified on the line that references ncp_virtualdomain.

   Important: This line must be identical in the $NCHOME/etc/precision/ServiceData.cfg file in both domains.

   For further information about the ServiceData.cfg file, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Related tasks:

"Configuring the TCP socket connection between the domains" on page 310
A TCP socket connection is required between the Virtual Domain processes in the primary and backup domains so that the topology data and topology updates can be copied to the backup domain.

Switching to failover configuration with NCIM topology database high availability:

You can modify an existing failover architecture to include NCIM topology database high availability.

Note: In previous Network Manager releases, users could include an NCIM topology database failover configuration by using NCIM replication (also referred to as NCIM topology database replication). The NCIM replication feature has been replaced by the high availability feature that is provided by the supported database:

- If you have a DB2 database, you can use the High Availability Disaster Recovery (HADR) feature to set up failover for NCIM.
- Fix Pack 5 If you have an Oracle database, you can use the Real Application Clusters (RAC) feature to set up failover for NCIM.

To configure NCIM topology database high availability:

1. Set up NCIM topology database high availability by using the high availability feature that is provided by the supported database.

   DB2 If you have a DB2 database, follow the procedures described in the DB2 documentation to configure a failover configuration for the NCIM topology database using the HADR feature. See Related information later for links to your DB2 Information Center.

   Oracle Fix Pack 5 If you have a Oracle database, follow the procedures described in the Oracle documentation to set up the Real Application Clusters (RAC) high availability environment. Using Oracle RAC, you can create a high availability setup for your NCIM topology database. For information on how to install and configure Oracle RAC, see Related information later for a link to the Oracle documentation.
2. Configure Network Manager to work with the supported database as described in "Configuring Network Manager to work with DB2 HADR or Oracle RAC" on page 313.

Related concepts:

Fix Pack 4 "About NCIM topology database high availability" on page 276
Network Manager allows you to configure the Network Connectivity and Inventory Model (NCIM) topology database for high availability, minimizing the impact of computer or network failure. The following sections provide an overview of NCIM topology database high availability and explain how to configure it.

Related tasks:

"Configuring failover using the ConfigItnm.cfg file" on page 308
When you use the `$NCHOME/etc/precision/ConfigItnm.DOMAIN.cfg` file to configure failover, the Network Manager processes will read the file on startup to identify whether they are running in the primary or backup domain. Similarly, the **ncp_model** process will identify whether NCIM replication is in use, and run appropriately for that configuration.

"Configuring failover using the CtrlServices.cfg file" on page 310
The `$NCHOME/etc/precision/CtrlServices.cfg` file for the master process controller, **ncp_ctrl**, provides an alternative method for configuring failover of the Network Manager core components. This file requires individual command-line options to be specified for the **ncp_virtualdomain**, **ncp_model**, **ncp_g_event**, and **ncp_poller** processes in the primary and backup domain servers.

Fix Pack 4 “Configuring Network Manager to work with DB2 HADR or Oracle RAC”
You can configure Network Manager core processes to use the DB2 catalog and the Network Manager GUI to operate in the DB2 high availability disaster recovery (HADR) environment. Fix Pack 5 Similarly, you can also configure Network Manager core processes and the Network Manager GUI to operate in the Oracle Real Application Clusters (RAC) environment.

Related information:

IBM DB2 Version 10.1 Information Center
For more information on DB2 10.1 HADR, search the IBM DB2 Version 10.1 Information Center. Suggested search terms include "high availability".

IBM DB2 Version 9.7 Information Center
For more information on DB2 9.7 HADR, search the IBM DB2 Version 9.7 Information Center. Suggested search terms include "high availability".

Oracle Database Online Documentation

Configuring Network Manager to work with DB2 HADR or Oracle RAC

You can configure Network Manager core processes to use the DB2 catalog and the Network Manager GUI to operate in the DB2 high availability disaster recovery (HADR) environment. Fix Pack 5 Similarly, you can also configure Network Manager core processes and the Network Manager GUI to operate in the Oracle Real Application Clusters (RAC) environment.

DB2 For guidance on best practices for implementing a high availability solution using DB2 HADR, see *IBM DB2 High Availability for Tivoli Netcool products - Best Practices* available at https://www.ibm.com/developerworks/community/wikis/home?lang=en#/wiki/Tivoli%20Netcool%20OMNIbus/page/Best%20Practices.

Note: If you implement failover, then you must ensure that both the primary and backup installations are using identical encryption keys. If the encryption keys are not identical, then the backup poller does not function correctly during failover. To ensure that both the primary and backup installations are using identical encryption keys, copy the following file from the primary server to the same location on the backup server: `$NCHOME/etc/security/keys/conf.key`. If you enter all SNMP community strings on the command line and do not encrypt them, you do not need to do this task. For more information on changing the encryption key, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Related concepts:

Fix Pack 4 “About NCIM topology database high availability” on page 276
Network Manager allows you to configure the Network Connectivity and Inventory Model (NCIM) topology database for high availability, minimizing the impact of computer or network failure. The following sections provide an overview of NCIM topology database high availability and explain how to configure it.

“Network Manager failover architecture (core processes)” on page 281
Failover of the Network Manager core processes can be implemented by setting up primary and backup Network Manager installations that run on different servers. Both installations can either connect to a single Tivoli Netcool/OMNIbus ObjectServer or to a virtual pair of ObjectServers.

Related information:

IBM DB2 Version 10.1 Information Center
For more information on DB2 10.1 HADR, search the IBM DB2 Version 10.1 Information Center. Suggested search terms include "high availability".

IBM DB2 Version 9.7 Information Center
For more information on DB2 9.7 HADR, search the IBM DB2 Version 9.7 Information Center. Suggested search terms include "high availability".

Oracle Database Online Documentation

Forcing Network Manager to use the DB2 catalog or an Oracle RAC service: Fix Pack 5

Use this information to force the Network Manager core processes to use the DB2 catalog or to connect to an Oracle RAC service name, depending on your database type.

DB2 For DB2 databases, the Network Manager core processes need to use the DB2 catalog to obtain information about the alternate DB2 server. To force the Network Manager core processes to use the DB2 catalog, edit two configuration files (`DbLogins.`*Domain*`.cfg` and `MibDbLogin.cfg`) and run the DB2 **`UPDATE ALTERNATE SERVER FOR DATABASE`** command.

Oracle Fix Pack 5 For Oracle databases, the Network Manager core processes need to connect to the service name used by Oracle RAC.

Oracle To configure the Network Manager core processes to use a service name instead of a SID, edit two configuration files (`DbLogins.`*Domain*`.cfg` and `MibDbLogin.cfg`).

The two configuration files — `DbLogins.`*Domain*`.cfg` and `MibDbLogin.cfg` — that you need to edit are part of the Network Manager core installation. Thus, these configuration files reside on the server on which Network Manager is installed. If you have Network Manager failover configured, then you would edit these configuration files on the primary and backup Network Manager servers.

1. On the Network Manager primary server, open the `$NCHOME/etc/precision/DbLogins.`*Domain*`.cfg` file and make the following changes depending on your database type:

Option	Description
DB2 **For DB2 databases**	1. Search for the attribute called `m_PortNum`. 2. Do not change the value of the `m_PortNum` attribute for `"DNCIM",`. Set the value of all the other `m_PortNum` attributes to 0 (zero). 3. Set the `m_DbName` attribute to the locally cataloged alias for the primary NCIM DB2 server. 4. Write and quit the configuration file. Perform the same steps on the Network Manager backup server, if necessary.

Option	Description
Oracle **For Oracle databases**	1. Search for the attribute called `m_OracleService` and add it after `m_PortNum` if it does not already exist. 2. Do not change the value of the `m_OracleService` attribute for `"DNCIM",`. Set the value of all the other `m_OracleService` attributes to 1. 3. Ensure `m_DbName` is set to the Oracle `SERVICE_NAME` as specified in `$ORACLE_HOME/network/admin/tnsnames.ora` 4. Ensure `m_Hostname` is set to the Oracle RAC SCAN host name. 5. Optionally, you can define your own custom Oracle RAC connection string using the attribute `m_ConnectionString`, as described here. This connection string can be used for connecting to an Oracle RAC cluster, or for other purposes. 6. Write and quit the configuration file. Perform the same steps on the Network Manager backup server, if necessary.

2. On the Network Manager primary server, open the `$NCHOME/etc/precision/MibDbLogin.cfg` file and make the following changes depending on your database type:

Option	Description
DB2 **For DB2 databases**	1. Search for the attribute called `m_PortNum`. 2. Set the value of `m_PortNum` attribute to 0 (zero). 3. Write and quit the configuration file. Perform the same steps on the Network Manager backup server, if necessary.

Option	Description
Oracle **For Oracle databases**	1. Search for the attribute called `m_OracleService` and add it after `m_PortNum` if it does not already exist. 2. Set the value of `m_OracleService` attribute to 1. 3. Ensure `m_DbName` is set to the Oracle `SERVICE_NAME` as specified in `$ORACLE_HOME/network/admin/tnsnames.ora` 4. Ensure `m_Hostname` is set to the Oracle RAC SCAN host name. 5. Optionally, you can define your own custom Oracle connection string using the attribute `m_ConnectionString`, as described here. This connection string can be used for connecting to an Oracle RAC cluster, or for other purposes. 6. Write and quit the configuration file. Perform the same steps on the Network Manager backup server, if necessary.

3. Oracle Fix Pack 5 For Oracle databases, you must also make the following change:
   a. Edit the `ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties` file.
   b. Add the following parameter to the file: .

      ```
      tnm.database.jdbc.url=jdbc.oracle:thin@SERVER_NAME:PORT_NUMBER:DATABASE_NAME
      ```

      Where:
      - *SERVER_NAME* is the name of the server where the Oracle RAC service is intalled.
      - *PORT_NUMBER* is the relevant port number on that server.
      - *DATABASE_NAME* is the name of the database, as defined in the tnm.database.dbname within the tnm.properties file.

   c. Save the tnm.properties file.
4. DB2 For DB2 databases, you also need to run the **UPDATE ALTERNATE SERVER FOR DATABASE** command from the primary and backup servers on which DB2 is installed. For details on this command, including the authorities required to run it, see Related information below for links to the DB2 Information Center.

   Run the **UPDATE ALTERNATE SERVER FOR DATABASE** command on the primary DB2 server to update the alternate DB2 server as follows:

   ```
   db2 update alternate server for database database-alias using hostname hostname
   port port-number
   ```

   where:
   - *database-alias* — Specifies the alias of the database where the alternate server is to be updated.
   - *hostname* — Specifies a fully qualified host name or the IP address of the node where the alternate server for the database resides.
   - *port* — Specifies the port number of the alternate server of the database manager instance.

Perform the same steps on the backup DB2 server.

The following example shows how to run the **UPDATE ALTERNATE SERVER FOR DATABASE** command on the primary DB2 server:

```
db2 update alternate server for database TAURUS using hostname co110002
port 50000
```

The following example shows how to run the **UPDATE ALTERNATE SERVER FOR DATABASE** command on the backup DB2 server:

```
db2 update alternate server for database TAURUS using hostname co110004
port 50000
```

Related tasks:

"Setting a custom connection URL to identify the DB2 or Oracle RAC servers" on page 318

Use this information to set a custom connection URL to identify the primary and backup DB2 servers, or to identify the Oracle 11 RAC service. This connection will allow the Network Manager GUI to work in the DB2 HADR or Oracle RAC environment, depending on your database type.

Related information:

IBM DB2 Version 10.1 Information Center

For more information on DB2 10.1 HADR, search the IBM DB2 Version 10.1 Information Center. Suggested search terms include "high availability".

IBM DB2 Version 9.7 Information Center

For more information on DB2 9.7 HADR, search the IBM DB2 Version 9.7 Information Center. Suggested search terms include "high availability".

Oracle Database Online Documentation

Custom Oracle connection string:

You can define a custom Oracle connection string. This connection string can be used for connecting to an Oracle RAC cluster, or for other purposes.

To define a custom ORACLE connection string, edit the `$NCHOME/etc/precision/DbLogins.Domain.cfg` configuration file, and configure the insert within the file to include an `m_ConnectionString` field so that the insert looks something like this:

```
insert into config.dbserver
(
    m_DbId,
    m_Server,
    m_DbName,
    m_Schema,
    m_Hostname,
    m_Username,
    m_Password,
    m_PortNum,
    m_ConnectionString,
    m_EncryptedPwd
)
values
(
    "NCIM",
    "oracle",
    "ORATEST",
    "ncim",
    "server1.location1.acme.com",
    "ncim",
    "ncim",
    1521,
```

```
    "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=server1.location1.acme.com3)
(PORT=1521))(CONNECT_DATA=(SID=ORATEST)))",
    0
);
```

By using the m_ConnectionString attribute in this way you effectively replace the values of m_DbName, m_Hostname and m_PortNum. You should still provide these value; however, they will be overridden by the value specified in the attribute m_ConnectionString when connecting to the database.

Setting a custom connection URL to identify the DB2 or Oracle RAC servers:

Use this information to set a custom connection URL to identify the primary and backup DB2 servers, or to identify the Oracle 11 RAC service. This connection will allow the Network Manager GUI to work in the DB2 HADR or Oracle RAC environment, depending on your database type.

To set a custom connection URL to identify the primary and backup DB2 servers, or to identify the Oracle RAC servers, edit three properties files and specify the URL connection to the servers. Specify the same URL connection in each of the properties files.

The following two properties files are applicable to the Network Manager GUI:

- $NCHOME/precision/profiles/TIPProfile/etc/tnm/tnm.properties
- $NCHOME/precision/profiles/TIPProfile/etc/tnm/ncpolldata.properties

The following properties file is part of the Network Manager core installation:
$NCHOME/precision/platform/java/lib/ncp_topoviz/etc/tnm/tnm.properties

To set a custom connection URL:

1. Open the $NCHOME/precision/profiles/TIPProfile/etc/tnm/tnm.properties and the $NCHOME/precision/platform/java/lib/ncp_topoviz/etc/tnm/tnm.properties files for editing and make the following changes to both, depending on your database type:

Option	Description
DB2 **For DB2 databases**	Specify the URL connection to the primary and backup DB2 servers using the following syntax: `tnm.database.jdbc.url=jdbc:db2://`*`primary_db2_server`*`:`*`primary_db2_port_number`*`/`*`dbname`*`:clientRerouteAlternateServerName=`*`backup_db2_server`*`;clientRerouteAlternatePortNumber=`*`backup_db2_port`*`;` where: • *primary_db2_server* — Specifies the name of the primary server on which the DB2 database is running. • *primary_db2_port_number* — Specifies the port number of the primary server on which the DB2 database is running. • *dbname*: Specifies the name of the DB2 database. • *backup_db2_server* — Specifies the name of the backup server on which the DB2 database is running. • *backup_db2_port* — Specifies the port number of the backup server on which the DB2 database is running.
Oracle **For Oracle databases**	Specify the URL connection to the Oracle RAC servers using the following syntax: `tnm.database.jdbc.url=jdbc:oracle:thin:@`*`Oracle_RAC_SCAN_hostname`*`:`*`Oracle_RAC_port_number`*`/`*`Oracle_RAC_service_name`* where: • *Oracle_RAC_SCAN_hostname* — Specifies the Oracle Single Client Access Name (SCAN) address on which the Oracle RAC database is running. • *Oracle_RAC_port_number* — Specifies the port number on which the Oracle RAC database is running. • *Oracle_RAC_service_name* — Specifies the service name with which the Oracle RAC database is running.

2. Open the `$NCHOME/precision/profiles/TIPProfile/etc/tnm/ncpolldata.properties` file for editing and make the following changes depending on your database type:

Option	Description
DB2 **For DB2 databases**	Specify the URL connection to the primary and backup DB2 servers using the following syntax: `ncpolldata.database.jdbc.url=jdbc:db2://`*`primary_db2_server`*`:`*`primary_db2_port_number`*`/`*`dbname`*`:clientRerouteAlternateServerName=`*`backup_db2_server`*`;clientRerouteAlternatePortNumber=`*`backup_db2_port`*`;` where: • *primary_db2_server* — Specifies the name of the primary server on which the DB2 database is running. • *primary_db2_port_number* — Specifies the port number of the primary server on which the DB2 database is running. • *dbname*: Specifies the name of the DB2 database. • *backup_db2_server* — Specifies the name of the backup server on which the DB2 database is running. • *backup_db2_port* — Specifies the port number of the backup server on which the DB2 database is running.
Oracle **For Oracle databases**	Specify the URL connection to the Oracle RAC servers using the following syntax: `ncpolldata.database.jdbc.url=jdbc:oracle:thin:@`*`Oracle_RAC_SCAN_hostname`*`:`*`Oracle_RAC_port_number`*`/`*`Oracle_RAC_service_name`* where: • *Oracle_RAC_SCAN_hostname* — Specifies the Oracle Single Client Access Name (SCAN) address on which the Oracle RAC database is running. • *Oracle_RAC_port_number* — Specifies the port number on which the Oracle RAC database is running. • *Oracle_RAC_service_name* — Specifies the service name with which the Oracle RAC database is running.

Related tasks:

"Forcing Network Manager to use the DB2 catalog or an Oracle RAC service" on page 314
Use this information to force the Network Manager core processes to use the DB2 catalog or to connect to an Oracle RAC service name, depending on your database type.

Related information:

IBM DB2 Version 10.1 Information Center
For more information on DB2 10.1 HADR, search the IBM DB2 Version 10.1 Information Center. Suggested search terms include "high availability".

IBM DB2 Version 9.7 Information Center
For more information on DB2 9.7 HADR, search the IBM DB2 Version 9.7 Information Center. Suggested search terms include "high availability".

Oracle Database Online Documentation

Configuring parameters for health checks

If required, you can configure preferred conditions under which health check events are generated, by specifying identical OQL inserts to the Virtual Domain process schema file (`VirtualDomainSchema.cfg`) on both the primary and backup servers.

The Virtual Domain component uses two database tables (config and state) in the **`ncp_virtualdomain`** database to support Network Manager failover. The health check status records and filters are stored in these tables, which can be updated using the `VirtualDomainSchema.cfg` file. For further information about the config and state database tables, see the *IBM Tivoli Network Manager IP Edition Management Database Reference*.

To change the default settings for the health check parameters:

1. On the primary Network Manager server, edit the `$NCHOME/etc/precision/VirtualDomainSchema.cfg` file by specifying the following OQL inserts:
   - Update the column values in the config.defaults table to specify different time periods for the failover health checks.

     For example, you can use the m_HealthCheckPeriod column to change the time interval between each health check. Or you can use the m_FailoverTime column to change the interval after which failover is triggered by the backup domain, when the primary domain is deemed to be in poor health. The default settings are as follows:

     ```
     insert into config.defaults
     (
         m_HealthCheckPeriod,
         m_FailoverTime,
         m_AutoTopologyDownload
     )
     values
     ( 60, 300, 1 );
     ```

   - If required, update the state.filters table to define individual filters for each poller configured in the `$NCHOME/etc/precision/CtrlServices.cfg` file. For example, for an additionally configured poller, PingPoller:

     ```
     insert into state.filters
     (
         m_ServiceName,
         m_Filter,
         m_Description
     )
     values
     (
         "PingPoller",
         "m_ChangeTime > eval(time,'$TIME - 300') and m_CtrlState <> 7",
         "The Poller has been running within the last 300 seconds"
     );
     ```

2. Save and close the file.
3. Make identical changes to the `$NCHOME/etc/precision/VirtualDomainSchema.cfg` file on the backup server.

Related concepts:

"Health check events and failover" on page 287
Failover is governed by health checks, which are configured to run periodically to assess the health of the primary and backup Network Manager domains.

Configuring process dependencies for failover

When running Network Manager in failover mode, you must start the Network Manager processes by using the **ncp_ctrl** process. The order in which the processes start is important, and is defined by the process dependencies that are configured in the `$NCHOME/etc/precision/CtrlServices.cfg` file.

The Virtual Domain component (**ncp_virtualdomain**), which manages failover, depends on all the processes it is monitoring because it cannot correctly determine their health until the processes are running. In the `CtrlServices.cfg` file in both the primary and backup domains, the entry for the **ncp_virtualdomain** process has the following default configuration:

```
dependsOn=[ "ncp_poller(default)", "ncp_g_event" ];
```

No further configuration is needed to set the process dependencies for failover, provided this default setting is retained.

For further information about managing process dependencies, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Troubleshooting failover

Review this information for help in resolving issues you might encounter with failover.

Verifying the failover setup of the Tivoli Netcool/OMNIbus ObjectServers

If ObjectServer failover is configured, you might find it useful to verify the failover setup of the ObjectServers.

1. After starting both ObjectServers, check that events forwarded to the primary ObjectServer are being displayed in the Active Event List.
2. Stop the primary ObjectServer and check the ObjectServer log file (`$NCHOME/omnibus/log/`*`PRIMARY_NAME`*`.log`) for failover messages.
3. Check the Active Event List to confirm that events forwarded to the backup ObjectServer are being displayed.
4. Restore the primary ObjectServer to a running state and verify that failback has occurred by checking its log file.

For information about using the Tivoli Netcool/OMNIbus commands to start and stop the ObjectServer, see the Tivoli Netcool/OMNIbus documentation at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm. For information about starting and stopping the ObjectServer using Network Manager commands, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Tracking failover of the Network Manager core processes

You can perform a number of actions and checks to verify whether failover of the Network Manager core processes is operating as expected.

Tracking failover on startup

To ensure that the primary domain starts running as the active domain, start the primary domain and its Virtual Domain process before starting the backup domain. If the backup domain is started before the primary Virtual Domain process has started, the backup domain can become active, start polling the network, and raise health check problem events about the primary domain. This issue, however, resolves itself after the primary Virtual Domain starts and health check events are transmitted between the domains.

At startup, the topology and policies are copied from the primary domain to the backup domain. The backup domain, however, cannot become active (on failover) until it has initialized its topology. To verify that the topology has been initialized:

- Check for a non-zero size topology cache file (`Store.Cache.kernel.activeModel.domain`) in the `$NCHOME/var/precision` directory in the backup domain.
- If NCIM replication is configured, check that entities exist in the backup domain. There should be the same number of entities in the primary and backup ncim.entityData tables.

  Tip: It can take some time for the topology and policies to be copied from the primary to the backup domain, particularly for large topologies. Therefore, allow a reasonable time interval before checking for the topology cache file and entities in the backup domain.

Event generation for startup: Monitor the Active Event List for ItnmServiceState and ItnmFailoverConnection Network Manager events, to verify that the Virtual Domain processes are running, and that the TCP socket connection has been established:

- After each local **`ncp_virtualdomain`** process starts, the **`ncp_ctrl`** process generates an ItnmServiceState resolution event.
- When a TCP connection is established between the Virtual Domain processes, an ItnmFailoverConnection resolution event is generated.

Tracking failover when the system is in a steady state

Normal, *steady-state* failover behavior can be achieved only after the Virtual Domain processes in the primary and backup domains have started and connected. Steady-state behavior can be defined as follows:

- The primary domain is active, and operating as if it is the sole domain. The discovery process discovers the network, which is monitored by the poller, and events are enriched by the Event Gateway.
- The backup domain is in standby mode. Discovery is not initiated, and the poller keeps track of the policies configured in the primary domain, but does not poll any devices. The Event Gateway also does not update events in the ObjectServer.

You can run OQL queries on each domain to check on the status of processes:

- You can check the status of individual Network Manager processes by querying the database of the **`ncp_ctrl`** process. All processes that are running without

issue should have the setting `serviceState = 4` in the services.inTray database table, to indicate that the service is "alive and running".

- The **ncp_poller** and **ncp_g_event** processes each have an associated config.failover database table, which identifies their current failover state. When running successfully in a steady state, these processes have the setting `FailedOver = 0` in the config.failover OQL table in both domains. (The Virtual Domain process periodically updates the FailedOver field.)

  Tip: The config database schema is defined in the following files: `$NCHOME/etc/precision/NcPollerSchema.cfg` and `$NCHOME/etc/precision/EventGatewaySchema.cfg`.

  For further information about running OQL queries, see the *IBM Tivoli Network Manager IP Edition Language Reference*. For further information about how to identify which processes are running, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Event generation while in a steady state: Each domain generates events about its state, based on the filters in the `$NCHOME/etc/precision/VirtualDomainSchema.cfg` file. These events are generated at an interval configured in the m_HealthCheckInterval field. Monitor the Active Event List for ItnmHealthChk and ItnmDatabaseConnection Network Manager events to check whether the primary and backup domains are in good health:

- Each domain generates ItnmHealthChk resolution events while it is healthy.
- The primary domain generates an ItnmDatabaseConnection problem event if connection to the primary NCIM database is lost. If the connection is not re-established within the time interval defined for the NCIM state.filters entry in the `VirtualDomainSchema.cfg` file, the primary domain generates an ItnmHealthChk problem event, about the primary domain.
- If the backup domain does not receive an ItnmHealthChk resolution event from the primary domain within the configured m_FailoverTime interval, the backup domain generates a synthetic ItnmHealthChk problem event on behalf of the primary domain.

  If either the primary or backup domain generates an ItnmHealthChk problem event for the primary domain, failover is triggered, and the backup domain becomes active. If the primary domain is still running, it goes into standby mode.

  Tip: For health check events, the Node field identifies the domain for which the health check event is generated.

Tracking failover and failback

When failover occurs, the backup domain becomes active, the backup poller monitors the network, and the Event Gateway updates ObjectServer events. You can run OQL queries to check on the status of the **ncp_poller** and **ncp_g_event** processes. These processes each have an associated config.failover database table, which identifies their current failover state. When the backup domain is active, these processes have the setting `FailedOver = 1` in the config.failover table, to indicate that they are in a failover state. (If the primary domain is still running, the associated processes are also assigned the value of `FailedOver = 1`.)

When failback occurs, the backup domain goes into standby, and the primary domain becomes active again. This is analogous to startup.

Event generation on failover and failback: Monitor the Active Event List for ItnmHealthChk and ItnmFailover Network Manager events, to confirm failover and failback behavior:

- An ItnmHealthChk problem event about the primary domain indicates that failover has been triggered. A subsequent ItnmHealthChk resolution event about the primary domain indicates that failback has been triggered.
- ItnmFailover events are generated to indicate when a Network Manager domain fails over or fails back. The event description states whether the domain is the primary or backup, and whether it has become active or gone into standby mode.

Related reference:

"Network Manager status events" on page 163
Network Manager can generate events that show the status of various Network Manager processes. These events are known as Network Manager status events and have the alerts.status AlertGroup field value of `ITNM Status`.

Investigating why failover occurred

Because failover can be initiated by either the primary or the backup domain, it is important to identify which domain initiated failover.

Perform either of the following actions:

- Review the Virtual Domain log file (`$NCHOME/log/precision/ncp_virtualdomain.`*`DOMAIN`*`.log`) and the Event Gateway log file (`$NCHOME/log/precision/ncp_g_event.`*`DOMAIN`*`.log`).
- Review the ItnmHealthChk and ItnmFailover events in the Active Event List. (This is the simpler approach.)

If the primary domain initiated failover, this indicates a failure of one of the primary domain processes. You can check the status of the processes by querying the database of the **`ncp_ctrl`** process. The `serviceState` field in the services.inTray database table shows the current operational state for each of the processes. For further information about how to identify which processes are running, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

If the backup domain initiated failover, this indicates a failure to route health check events through the system due to one of the following reasons:

- The primary domain did not raise a health check event (for example, because the primary server was down).
- The Probe for Tivoli Netcool/OMNIbus or Event Gateway processes in both domains are not configured to access the same ObjectServer.
- The Event Gateway Failover plug-in is not enabled.
- The Probe for Tivoli Netcool/OMNIbus rules file has been modified such that the health check event does not contain the required information.
- The backup Event Gateway is not letting health check events through the nco2ncp filter.

  For further information about enabling the Failover plug-in and about event filters, see the *IBM Tivoli Network Manager IP Edition Event Management Guide*.

Also ensure that Virtual Domain is configured (in the `$NCHOME/etc/precision/CtrlServices.cfg` file) to have a dependency on all processes listed in the `$NCHOME/etc/precision/VirtualDomainSchema.cfg` file.

Related tasks:

"Configuring failover using the ConfigItnm.cfg file" on page 308
When you use the $NCHOME/etc/precision/ConfigItnm.*DOMAIN*.cfg file to configure failover, the Network Manager processes will read the file on startup to identify whether they are running in the primary or backup domain. Similarly, the **ncp_model** process will identify whether NCIM replication is in use, and run appropriately for that configuration.

Related reference:

"Network Manager status events" on page 163
Network Manager can generate events that show the status of various Network Manager processes. These events are known as Network Manager status events and have the alerts.status AlertGroup field value of ITNM Status.

Investigating TCP connection issues

A TCP socket connection is required between the Virtual Domain processes in the primary and backup domains so that the topology data and topology updates can be copied from the primary domain to the backup domain.

If the TCP connection is lost:

- Check that Virtual Domain is configured (in $NCHOME/etc/precision/CtrlServices.cfg) to have a dependency on all processes listed in the $NCHOME/etc/precision/VirtualDomainSchema.cfg file.
- Check that the **ncp_config** process is running. You can check the status of **ncp_config** by querying the database of the **ncp_ctrl** process. If running without issue, **ncp_config** should have the setting serviceState = 4 in the services.inTray database table. For further information about how to identify which processes are running, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

If the TCP connection is not being established:

- Check that the $NCHOME/etc/precision/ServiceData.cfg files in both domains have the same entry for the Virtual Domain process.
- Check that boundary firewalls between the domains allow the TCP connection on the defined server port.
- Check that the defined port is available for use on the primary domain.

Related tasks:

"Configuring process dependencies for failover" on page 322
When running Network Manager in failover mode, you must start the Network Manager processes by using the **ncp_ctrl** process. The order in which the processes start is important, and is defined by the process dependencies that are configured in the $NCHOME/etc/precision/CtrlServices.cfg file.

"Configuring the TCP socket connection between the domains" on page 310
A TCP socket connection is required between the Virtual Domain processes in the primary and backup domains so that the topology data and topology updates can be copied to the backup domain.

Sequence for restarting the server processes in a failover configuration

Use this information as a guide for restarting the server processes if your Network Manager failover environment requires a reboot of all the servers.

Start the processes in the following order:

1. Start the primary ObjectServer. Depending on your installation and configuration setup, you can use one of the following methods:
   - Tivoli Netcool/OMNIbus process control on UNIX, Linux, and Windows
   - Services on Windows
   - The Tivoli Netcool/OMNIbus **nco_objserv** command
   - The Network Manager **itnm_start** command

   For information about using the Tivoli Netcool/OMNIbus commands to start the ObjectServer, see the Tivoli Netcool/OMNIbus documentation at http://publib.boulder.ibm.com/infocenter/tivihelp/v8r1/topic/com.ibm.tivoli.nam.doc/welcome_ob.htm. For information about starting the ObjectServer using Network Manager commands, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.
2. Start the backup ObjectServer.
3. Start the topology database if not already running.
4. Start the primary Network Manager server on which the core processes are installed, by using the **itnm_start** command or by starting the master process controller, **ncp_ctrl**.

   Also verify that the Virtual Domain process in the primary domain has started, by running the **itnm_status** command in the `$NCHOME/precision/bin` directory.

   For information about starting the Network Manager server and processes, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.
5. Start the backup Network Manager server on which the core processes are installed.

Tip: The Tivoli Integrated Portal server, on which the Network Manager Web applications and the Tivoli Netcool/OMNIbus Web GUI are installed, starts automatically whenever the computer is started.

Changing the IP address and hostname of the Network Manager IP Edition installation

If you change the IP address and hostname of the server where any of the components of Network Manager IP Edition or integrated products are installed, you must configure Network Manager IP Edition and associated components and products.

Changing the IP address and hostname for Network Manager IP Edition

If you want to change the IP address and hostname for the server where the Network Manager IP Edition core components are installed, you must perform some configuration tasks.

Complete the following steps to change the IP address and hostname on the Network Manager IP Edition server.

1. Change to the following directory: NCHOME/etc/.
2. Edit the configuration file: `itnm.cfg`.
3. Change the following parameter: `ncp`. Update this to the new hostname of the Network Manager IP Edition server; for example: `ncp=myhost`
4. Save the `itnm.cfg` file.
5. Save the `itnm.cfg` file.
6. Change to the following directory: `NCHOME/etc/precision/`.
7. Edit the file: `ServiceData.cfg`.
8. Change the following line:

   ```
   SERVICE: ncp_config DOMAIN: NCOMS ADDRESS: Network_Manager_server_IP_address
   PORT: port_number SERVERNAME: Network_Manager_server_hostname DYNAMIC: NO
   ```

   Where:

   - *Network_Manager_server_IP_address* is the new IP address of the Network Manager IP Edition server.
   - *Network_Manager_server_hostname* is the new hostname of the Network Manager IP Edition server.
9. Save the `ServiceData.cfg` file.

Changing the IP address and hostname on the Tivoli Netcool/OMNIbus server

If you want to change the IP address and hostname on the Tivoli Netcool/OMNIbus server, you must perform some configuration tasks.

Complete the following steps to change the IP address and hostname on the Tivoli Netcool/OMNIbus server:

1. Change to the following directory: `NCHOME/etc/`.
2. Edit the file: `omni.dat`.
3. Look for lines containing the Tivoli Netcool/OMNIbus server. These lines might be similar to the following lines:

   ```
   [NCOMS]
   {
           Primary: OMNIbus_server_hostname 4100
   }
   [NCO_PA]
   {
           Primary: OMNIbus_server_hostname 4200
   }
   ```

   Where:

   - *OMNIbus_server_hostname* is the hostname of the Tivoli Netcool/OMNIbus server.

   Change the Tivoli Netcool/OMNIbus server hostname in each of these lines.

4. Run the NCHOME/bin/nco_igen utility to apply the changes.
5. Repeat the previous steps on each of the hosts that connect to the Tivoli Netcool/OMNIbus server; for example, make these changes on connected probes, gateways, and ObjectServers.

Updating Network Manager IP Edition for a new Tivoli Netcool/OMNIbus IP address and hostname

If you update the IP address and hostname for the Tivoli Netcool/OMNIbus server, you must configure Network Manager IP Edition to use the new IP address and hostname.

Complete the following steps to update Network Manager IP Edition to make it aware of the changes to the Tivoli Netcool/OMNIbus server hostname:

1. Update the Network Manager IP Edition core components by editing the configuration file: NCHOME/etc/precision/itnm.cfg.
2. Change the following parameter:nco. Update this to the new hostname of the Tivoli Netcool/OMNIbus server; for example:nco=omnihost.
3. Save the itnm.cfg file.
4. Update the Network Manager IP Edition GUI components by editing the file webgui_home_dir/etc/datasources, where webgui_home_dir is the installation directory for the Web GUI; for example, $NCHOME/omnibus_webgui.
5. Update the Network Manager IP Edition web applications to configure them to use the changed Tivoli Netcool/OMNIbus server hostname:
   a. Edit the following file:

      NCHOME/omnibus_webgui/etc/datasources/ncwDataSourceDefinitions.xml

   b. Change the host and port values in the following sections to match your updated configuration:
      - <ncwPrimaryServer>
      - <ncwBackUpServer>

        Note: Only change this section if a backup Tivoli Netcool/OMNIbus ObjectServer is configured.
   c. Save the modified ncwDataSourceDefinitions.xml file.
   d. Restart the Tivoli Integrated Portal server to apply the changes.

Updating the Tivoli Integrated Portal for a new Tivoli Netcool/OMNIbus IP address and hostname

If the Tivoli Integrated Portal server was originally configured to use the Tivoli Netcool/OMNIbus ObjectServer as its primary user repository, and you update the IP address and hostname for the Tivoli Netcool/OMNIbus server, you must configure the Tivoli Integrated Portal to use the new IP address and hostname.

Complete the following steps to configure the Tivoli Integrated Portal to use the new Tivoli Netcool/OMNIbus server hostname:

1. Edit the following file:

   TIPHOME/profiles/TIPProfile/config/cells/TIPCell/wim/config/
   wimconfig.xml

2. Change the host1 and port1 properties to match your updated configuration in the following file:

   config:repositories adapterClassName=
   "com.ibm.tivoli.tip.vmm4ncos.ObjectServerAdapter"

3. Save the modified wimconfig.xml file.
4. Restart the Tivoli Integrated Portal server to apply the changes.

Changing the IP address and hostname on the Tivoli Integrated Portal server

If you want to change the IP address and hostname of the Tivoli Integrated Portal, you must configure the Tivoli Integrated Portal.

Follow these steps to change the IP address and hostname on the Tivoli Integrated Portal server:

1. Change to the following directory: TIPHOME/profiles/TIPProfile/bin/.
2. Use the wsadmin command to change the Tivoli Integrated Portal server hostname and IP address:

   ```
   wsadmin.sh -user tipadmin -password password
   -c "\$AdminTask changeHostName -hostName new_hostname -nodeName new_node"
   -c "\$AdminConfig save"
   ```

   This provides output similar to the following:

   ```
   WASX7209I: Connected to process "server1" on node TIPNode
    using SOAP connector;The type of process is: UnManagedProcess
   WASX7029I: For help, enter: "$Help help"
   wsadmin>
   ```

   Note the value of the Tivoli Integrated Portal node name. In the foregoing example, this is TIPNode.
3. At the wsadmin> prompt, run the following command:

   ```
   $AdminTask changeHostName { -nodeName TIP_node_name
   -hostName TIP_server_hostname};
   ```

   Where:

   - *TIP_node_name* is the Tivoli Integrated Portal node name; for example TIPNode in the example given earlier in this procedure.
   - *TIP_server_hostname* is the new hostname of the Tivoli Integrated Portal server.

     For example:

     ```
     wsadmin>$AdminTask changeHostName { -nodeName TIPNode
     -hostName myhost };
     ```
4. At the wsadmin> prompt, run the following commands to save the file and then to exit.

   ```
   wsadmin>$AdminConfig save
   wsadmin>exit
   ```
5. Restart the Tivoli Integrated Portal server.

Updating Network Manager for changed hostname of the Tivoli Integrated Portal server

If you change the hostname of the Tivoli Integrated Portal server, you must configure Network Manager IP Edition to use the new hostname.

To configure Network Manager IP Edition to use the new hostname, complete the following steps:

1. Update the Network Manager IP Edition core components by editing the configuration file: NCHOME/etc/itnm.cfg.
2. Change the following parameter:

```
tip
```

Update this to the new hostname of the Tivoli Integrated Portal server; for example:

```
tip=tiphost
```

3. Save the `itnm.cfg` file.

Changing the IP address and hostname on the Deployment Engine server

If you have changed the IP address and hostname on servers where components of Network Manager IP Edition are installed, you must configure the IP address and hostname for the IBM Deployment Engine.

Follow these steps to change the IP address and hostname for IBM Autonomic Deployment Engine (DE):

1. Change to the following directory: `$DE_HOME/bin/`, where `DE_HOME` is as follows:
   - `/usr/ibm/common/acsi/` for a root installation.
   - `$HOME/.acsi_$LOGNAME/` for a non-root installation.
2. Use the `de_chghostname` command to change the DE server hostname:

   ```
   ./de_chghostname.sh -name DE_server_hostname
   ```

   Where *DE_server_hostname* is the new hostname of the DE server.

Changing the IP address for Tivoli Common Reporting

If you want to change the IP address and hostname on the Tivoli Common Reporting server, you must perform some configuration tasks.

Follow these steps to change the IP address and hostname on the Tivoli Common Reporting server:

1. On the server where Tivoli Common Reporting is installed, Export the Tivoli Common Reporting configuration using the following command:

   ```
   $TCR_HOME/cognos/bin/tcr_cogconfig -e cogstartup.xml.exported
   ```

2. Update the file `cogstartup.xml.exported` by changing all instances of the old hostname with new hostname.
3. Replace the original `$TCR_HOME/cognos/configuration/cogstartup.xml` file with the `cogstartup.xml.exported` file.
4. Update the file `$TCR_HOME/cognos/configuration/cogconfig.prefs` by changing all instances of old hostname with new hostname.
5. Update the connection string by first changing to the directory `/opt/IBM/tivoli/tipv2Components/TCRComponent/bin/` and then issuing the following command:

   ```
   ./trcmd.sh -user user -password password -datasource
   -add servletInventory -connectionName servletInventory
   -dbType database_type -connectionString connection_string -force
   ```

   Where:

   - *user* is the database user name.
   - *password* is the database user password
   - *database_type* is the database type.
   - *connection_string* is the connection string to use, including the new hostname.

   For example:

```
./trcmd.sh -user tipadmin -password passw0rd -datasource
-add servletInventory -connectionName servletInventory -dbType XML
-connectionString "http://abc.xyz.com:16310/tarf/servlet/inventory#'?search=%2f
%2f%2a'
+ '&CAMpassport=' + CAMPassport() #" -force
```

6. Restart the Tivoli Integrated Portal server and the Tivoli Common Reporting server.

Configuring Network Manager IP Edition for a changed IP address of the DB2 NCIM server

If you change the IP address or hostname of the DB2 server hosting the NCIM topology database, you must configure Network Manager IP Edition to use the new details.

1. On the server where the Network Manager IP Edition are installed, edit the following file:

   `NCHOME/etc/precision/DbLogins.DOMAIN.cfg`
2. Change the hostname settings in this file and save the file.
3. Edit the following file:

   `NCHOME/etc/precision/MibDbLogin.cfg`
4. Change the hostname settings in this file and save the file.
5. On the server where the Network Manager IP Edition web applications are installed, edit the following file:

   `NCHOME/precision/profiles/TIPProfile/etc/tnm/tnm.properties`
6. Change the hostname settings in this file and save the file.
7. Edit the following file:

   `NCHOME/precision/profiles/TIPProfile/etc/tnm/ncpolldata.properties`
8. Change the hostname settings in this file and save the file.

Setting environment variables

Before starting any components or working with any configuration files, set the Network Manager environment variables by sourcing the environment variables 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, source the appropriate script for your operating system.

- UNIX Run the *Installation directory*`/netcool/env.sh` script. On Bash and Korn shells, source the env.sh script using a command similar to the following:
  `./opt/IBM/tivoli/netcool/env.sh`
- 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.

Default directory structure

Use this information to understand the Network Manager directory structure.

Top level directory structure

Within the directory that Network Manager is installed into, the following subdirectories are created: `netcool`, `tipv2`, and `tipv2Components`.

- The `netcool` directory contains Network Manager configuration files.
- The `tipv2` directory contains WebSphere Application Server and Tivoli Integrated Portal customizations. The `tipv2` directory is the default directory suggested by the installer for the Tivoli Integrated Portal and can be set independently to the Network Manager installation directory. If you are installing Network Manager into an existing installation of the Tivoli Integrated Portal, the Tivoli Integrated Portal files are installed into the existing Tivoli Integrated Portal directory.
- The `tipv2Components` directory contains Enterprise Storage Server (ESS) server, Business Intelligence and Reporting Tools (BIRT) extensions, and Tivoli Common Reporting files.

For information about the installation directories for Tivoli Netcool/OMNIbus and Tivoli Netcool/OMNIbus Web GUI, see the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*.

Directories used by the installer

The installer installs files in NCHOME, TIPHOME, and in other directories, depending on the operating system being installed on and the user performing the installation. The following table lists the extra directories used by the installer.

Table 28. Directories used by the installer

Installation	Directories used for installation files
UNIX UNIX operating systems, root user	/usr/ibm/common/acsi
	/var/ibm/common/acsi
UNIX UNIX operating systems, non-root user	~/.acsi_$HOSTNAME
	~/tivoli
	~/.cit (that is, in the user's home directory)
Windows 64 bit Windows	C:\Program Files (x86)\IBM\Common\acsi
Windows 32 bit Windows	C:\Program Files\IBM\Common\acsi

Contents of the netcool directory

The following table describes the contents of the netcool directory. All paths are shown relative to NCHOME. In this table, *arch* denotes an operating system directory. The name of this directory varies according to the operating system on which the software is installed:

- Solaris – solaris2
- Linux – linux2x86
- AIX – aix5
- Windows – win32
- zLinux - linux2s390

If you have installed other IBM Tivoli products, such as IBM Tivoli Business Service Manager, on the same server as Network Manager, there might be extra directories and files present. See the documentation for any other products you have installed for more information on their directories and files.

Table 29. Directories in NCHOME

Directory	Description
bin	Contains wrapper scripts that set the environment and execute/run the binary files for product or components supplied with Network Manager.
etc	Contains configuration files for products or components supplied with Network Manager.
etc/precision	Configuration files for all the Network Manager components.
ini	Only on Windows operating systems. Contains files specific to IBM Tivoli Netcool/OMNIbus.
install	Contains files used by the installation process. You should not need to alter the contents of this directory.
license	Contains the text of the product license agreement in various languages.
locales	Only on Windows operating systems. Contains lookup files for internationalization of various components.
log	Contains log files.
log/install	Contains log files for the installation.

Table 29. Directories in NCHOME (continued)

Directory	Description
log/precision	Contains log files created by Network Manager processes.
omnibus	If present, contains IBM Tivoli Netcool/OMNIbus files.
omnibus_webgui	If present, contains Tivoli Netcool/OMNIbus Web GUI files.
PD/precision	Contains FFDC scripts.
platform/*arch*	Contains the Java Development Kit (JDK) and Java Runtime Environment (JRE) used by the Tivoli Integrated Portal.
precision	Contains files for Network Manager. See later in this topic.
probes	Contains files for the Probe for IBM Tivoli Netcool/OMNIbus, the nco_p_ncpmonitor process.
_uninst	Contains files for uninstallation.
var	Contains persistent application data.
var/install	Contains database files for the installation process.
var/precision	Used by the ncp_store process to hold cached information that can be used to restore the databases should a process terminate unexpectedly.

Contents of the precision directory

The following table describes the contents of the NCHOME/precision directory. All paths are shown relative to NCHOME/precision.

In this table, *arch* denotes an operating system directory. The name of this directory varies according to the operating system on which the software is installed:

- Solaris – solaris2
- Linux – linux2x86
- AIX – aix5
- Windows – win32
- zLinux - linux2s390

Note: NCHOME/precision is the path set by default for PRECISION_HOME and ITNMHOME.

Table 30. Directories in NCHOME/precision

Directory	Description
adapters/ncp_dla	Contains files for the library adapter used for integration with products such as IBM Tivoli Application Dependency Discovery Manager.
adapters/ itnm_systemsDirector LiC	Contains files for integration with IBM Systems Director.
aoc	Contains the Active Object Class (AOC) files used by the dynamic class management and distribution system, CLASS.
bin	Contains wrapper scripts for all executable files. The executable files are held at the following location:platform/*arch*/bin
collectors/ perlCollectors	Contains files for Element Management System integrations.

Table 30. Directories in NCHOME/precision (continued)

Directory	Description
contrib	Contains unsupported utilities for managing Network Manager. Also used by the Netcool for Asset Management solution to contain example SQL*Plus reports.
cshrc	Only on UNIX operating systems. Used for setting up the environment for your C shell.
disco	Contains files used by DISCO. Contains the agent definition files, discovery agents, finder, helper files, and the stitchers.
eventGateway	Contains stitchers for event gateway and RCA.
integration	Contains files for component GUI integration.
install	Contains files used by the installation process.
java_api	Contains the JAVA API for developing Java applications that integrate with Network Manager components.
locales	Only on Windows operating systems. Contains lookup files for internationalization of various components.
mibs	Contains Management Information Base (MIB) files.
PD	Any core files generated by Network Manager are written into subdirectories of the PD directory. The core files can be used to help diagnose the cause of a problem.
perl	Contains perl files used in Network Manager.
platform/*arch*	Contains subdirectories particular to the operating system on which you installed Network Manager.
platform/*arch*/bin	Contains executable files for the Network Manager components. The files are appended to your PATH environment. Wrapper scripts for all of these executable files are held in the following location: NCHOME/precision/bin.
platform/*arch*/jre	Contains the JAVA Run-Time Environment used by Network Manager.
platform/*arch*/lib	Contains the object libraries used by all Network Manager components.
platform/java/lib	The Monitor Configuration GUI installation. The User Configuration Tool installation.
products	Contains GUI files for integrated products.
profile	Only on UNIX operating systems. Used for setting up the environment for your Bash shell.
profiles	Contains GUI-related files. **Note:** All Network Manager-specific files previously located in TIPHOME/profiles are now located in ITNMHOME/profiles.
scripts	Contains scripts supplied with the Network Manager products. It is advisable to keep any user-defined scripts in this directory so that they can easily be managed.
system	Contains files for product operation.
systemApps	Contains files for Web applications.

Related reference:

"Installation directory requirements" on page 47
The directory where you install Network Manager must fulfill certain

requirements.

Configuring Juniper PE Devices

One of the device polls enabled by default is the Juniper Remote Ping poll. To ensure that this poll is able to retrieve data, you must configure each Juniper PE device to provide access to certain tables within the device.

Remote ping poll operations on Juniper devices require access to the `pingCtlTable` and `jnxPingCtlTable` tables in the Juniper PE devices. This is achieved using the SNMP View-Based Access Control Model (VACM) for view `PrecisionIP`.

Make sure you set up each Juniper PE device to provide access to these tables for view `PrecisionIP` before enabling the Juniper Remote Ping poll policy.

The following example shows how a Juniper PE device can be configured to provide access for view `PrecisionIP` to the tables required for remote ping polling.

Setting Up Access using VACM

To provide access to the `pingCtlTable` and `jnxPingCtlTable` tables for view `PrecisionIP` on a Juniper PE device, do the following:

1. Use the `telnet` command to log into the PE device.
2. Enter `configure` to launch the editing command line.
3. Type `edit snmp` and press **Enter**.
4. Type `edit view PrecisionIP` and press **Enter**.
5. Type `set oid 1.3.6.1.2.1.80 include` and press **Enter**.
6. Type `set oid 1.3.6.1.4.1.2636.3.7` include and press **Enter**.
7. Type `up` and press **Enter**.
8. Type `edit community watermelon` and press **Enter**, where `watermelon` is the new write community string.
9. Type `set view PrecisionIP` and press **Enter**.
10. Type `set authorization read-write` and press **Enter**.
11. Type `commit` and press **Enter**.
12. Type `exit` and press **Enter**. New entries are created for view `PrecisionIP` in the `vacmViewTreeFamilyTable` MIB table on the PE device.

    To view the summary of the inserted section, you can type `show configuration snmp` and press **Enter**. The following screen is displayed:

    ```
    view PrecisionIP {
    oid 1.3.6.1.2.1.80 include;
    oid 1.3.6.1.4.1.2636.3.7 include;
    }
    community watermelon {
    view PrecisionIP;
    authorization read-write;
    }
    ```

    The settings above provide access to the tables required for remote ping poll operations using the community string `watermelon`.

Upgrading Oracle client libraries

Network Manager uses Oracle 10 and Oracle 11 client libraries. If you installed Network Manager with the Oracle 10 client libraries, you can upgrade to the Oracle 11 client libraries.

To upgrade from Oracle 10 to Oracle 11 client libraries:

1. Edit the `DbLogins.cfg` file and change the `m_Server` parameter to a value of `Oracle11`. The `DbLogins.cfg` file can be found at the following location:
   - UNIX `UNIX:$NCHOME/etc/precision/DbLogins.cfg`
   - Windows `Windows:%NCHOME%\etc\precision\DbLogins.cfg`
2. On AIX only perform the following steps:
   a. Edit the `$NCHOME/precision/bin/ncp_common` wrapper script.
   b. Find the following code snippet in this file:

```
if [ "ncp_perl" = "$BINARYNAME" ]; then
        #
        # ncp_perl can only use the Oracle 10 client it was compiled against
        #
        DIRLIST=${PRECISION_HOME}/platform/$1/lib:${ORACLE10_CLIENT}:
${NCHOME}/platform/$1/lib
    else
        #
        # To use the Oracle 11 client libraries change the line below
to use ORACLE11_CLIENT:
        #
        DIRLIST=${PRECISION_HOME}/platform/$1/lib:${ORACLE10_CLIENT}:
${NCHOME}/platform/$1/lib
    fi
```

3. In the second line beginning with `DIRLIST=`, change the variable `ORACLE10_CLIENT` (highlighted in boldface) to `ORACLE11_CLIENT`.

Configuring Informix disk space on Windows

If you are using Network Manager with Informix on Windows operating systems, set up disk space management for Informix after completing a successful installation.

After completing a successful Network Manager installation on Windows systems, perform the following steps to configure the following if you are using Informix:

- Set Informix to automatically check the amount of available free database space every 5 minutes, and set it to create additional space if more than 90% full.
- Set the Informix scheduler to run update statistics once a day.

1. Log out of Windows and log back in as the Informix user.
2. Go to **Start** > **All Programs** > **IBM Informix Dynamic Server** > **ITNM**.
3. Enter the following command: `SET NCHOME=`*`location of Network Manager installation`*
4. Enter the following command: `%ITNMHOME%\install\scripts\ids_post_install_sysadmin.bat`

Providing support for legacy devices in a FIPS 140-2 installation

If you have installed a FIPS 140-2 installation, you can still install non-FIPS 140–2 compliant algorithms such as DES and MD5 to enable you to access legacy equipment on your network.

1. Go to the directory where you extracted the Network Manager installation package.
2. Change to the following subdirectory of the extracted installation package: `COI/PackageSteps/Non-FIPS_back_end/FILES`
3. Depending on your operating system, verify that the following file is present:
   - UNIX `Non-FIPS_back_end-`*`arch-v.r.f.m`*`.tar.gz`
   - Windows `Non-FIPS_back_end-`*`arch-v.r.f.m`*`.zip`

   where:
   - *v.r.f.m* is the version number.
   - *arch* is the name of the operating system architecture on which the product is installed, for example, `solaris2`.
4. Depending on your operating system, perform the following step:
   - UNIX On UNIX systems, run the following command: `tar -xzvf Non-FIPS_back_end-`*`arch-v.r.f.m`*`.tar.gz -C $NCHOME *libNCP*`
   - Windows On Windows systems, extract the zip file and use Windows Explorer to copy the `libNcp*` dll libraries from `COI\PackageSteps\Non-FIPS_back_end\FILES\precision\platform\win32\bin` to `%NCHOME%\precision\platform\win32\bin`

   As a result, you should have the two shared libraries in the right location, for example:
   - UNIX On UNIX systems:
     - `$NCHOME/precision/platform/solaris2/lib/libNcpSnmpPrivDES.so`
     - `$NCHOME/precision/platform/solaris2/lib/libNcpSnmpAuthMD5.so`
   - Windows On Windows systems:
     - `%NCHOME%\precision\platform\win32\bin\libNcpSnmpPrivDES.so`
     - `%NCHOME%\precision\platform\win32\bin\libNcpSnmpAuthMD5.so`

   These libraries allow the Network Manager Polling engine, ncp_poller, to use the DES and MD5 encryption algorithms.
5. Edit the following configuration file: `ITNMHOME/profiles/TIPProfile/etc/tnm/tnm.properties`
6. Change the following property to false: `tnm.fips.mode=false` This allows configuration of the DES and MD5 encryption algorithms for SNMPv3 using the Discovery Configuration GUI.

Related tasks:

"Uncompressing the installation file" on page 55
If you have downloaded the installation file, you must uncompress the installation package before installing the product.

Configuring OQL Service Provider authentication

Queries against Network Manager component databases can be run from the command line using the OQL Service Provider process, ncp_oql. You can configure ncp_oql to authenticate against the NCIM database or against the Tivoli Netcool/OMNIbus ObjectServer. Alternatively you can configure ncp_oql to allow queries to run without authentication.

The OQL Service Provider authentication engine, ncp_auth is no longer used in V3.9. By default, there is no authentication for ncp_oql queries from the command line. You can configure the OQL Service Provider to authenticate against the NCIM database or against the ObjectServer, as follows:

- *Authentication against the NCIM database*: this forces the OQL Service Provider to authenticate using the username and password of the NCIM database, as specified at installation time and configured in the DbLogins.cfg configuration file.
- *Authentication against the ObjectServer*: this forces the OQL Service Provider to authenticate using the administrator account name and password of Tivoli Netcool/OMNIbus, as specified at installation time.

OQL Service Provider authentication is controlled by the value of the `m_OQLAuthenticationMode` within the config.settings table. The field takes the following values:

- 0: No authentication. Username and password are not required, and if specified in the command line, are ignored.
- 1: Authentication against NCIM database.
- 2: Authentication against the Tivoli Netcool/OMNIbus ObjectServer.

To set up OQL Service Provider authentication:

1. Edit the **ncp_config** configuration file, `$NCHOME/etc/precision/ConfigSchema.cfg`.
2. Configure one of the following inserts to the config.settings table:
   - Configure authentication against the NCIM database.

     ```
     insert into config.settings
     (
             m_OQLAuthenticationMode,
     )
     values
     (
             1,
     );
     ```

   - Configure authentication against the ObjectServer.

     ```
     insert into config.settings
     (
             m_OQLAuthenticationMode,
     )
     values
     (
             2,
     );
     ```

Configuring the SNMP Helper

The SNMP Helper is used by discovery and polling to issue SNMP requests to network devices. You can configure how the SNMP Helper issues SNMP requests and how it processes the results of SNMP requests.

For information on where the SNMP Helper is used in discovery and polling, see the following guides:

- For discovery, see the *IBM Tivoli Network Manager IP Edition Discovery Guide*.
- For polling, see the *IBM Tivoli Network Manager IP Edition Event Management Guide*.

Configuring SNMP Helper throttling

You can activate throttling in the SNMP Helper. Activating throttling increases the delay between Network Manager SNMP requests to a network device. This decreases the load on the network device. By default, throttling is switched off in the SNMP Helper.

About SNMP Helper throttling

Throttling the SNMP Helper establishes a delay between SNMP requests sent by the SNMP Helper using a formula that uses the GeneralSlowdown, GetNextBoundary, and GetNextSlowdown parameters.

Here is how the SNMP Helper sends requests without throttling (default) and with throttling:

- When throttling is inactivate, then SNMP GetNext operations work as follows: the SNMP Helper sends the first SNMP Get request and once Network Manager obtains a response then the SNMP Helper immediately sends the GetNext request.
- When throttling is activated, a delay is introduced between GetNext requests. The delay can be a shorter, generally defined delay or a longer delay. The system keeps track of the number of GetNext requests being sent to a network device and once that number exceeds a certain value, then the longer delay is applied; otherwise the shorter delay is applied. The system uses the `GeneralSlowdown`, `GetNextBoundary`, and `GetNextSlowdown` parameters defined in the snmpStack.accessParameters database table to determine which delay to apply. For more information on the snmpStack.accessParameters database table, see the *IBM Tivoli Network Manager IP Edition Discovery Guide*.

Activating SNMP Helper throttling

You can activate SNMP Helper throttling.

To activate SNMP Helper throttling, perform the following steps:

1. Edit the following configuration file: `NCHOME/etc/precision/NcPollerSchema.cfg`.

   Note: You can make the NcPollerSchema.cfg file domain specific by copying it to `NCHOME/etc/precision/NcPollerSchema.`*`DOMAIN_NAME`*`.cfg`, where *DOMAIN_NAME* is the name of the domain.
2. Add the following line at the end of the file:

   ```
   update config.properties set EnableThrottling = 1;
   ```
3. Save the file `NCHOME/etc/precision/NcPollerSchema.cfg`.
4. Activate the changes by performing one or both of the following:

- Start or schedule a new full discovery. Discovery will now make use of throttling.
- Restart the Polling engine, ncp_poller, with the `-readsnmpconfig` command-line option specified.

Configuring GetBulk support for SNMP v2 and v3

You can configure the SNMP Helper to use the GetBulk operation when SNMP v2 or v3 is used. Use of the GetBulk operation improves discovery speed and polling efficiency. By default, the SNMP helper does not use GetBulk.

About GetBulk

The SNMP v2 and SNMP v3 GetBulk command enables more efficient data transfer. When the SNMP Helper is enabled to use GetBulk, this decreases the time taken for the discovery data collection phases. Use of GetBulk also increases polling efficiency.

Configuring the SNMP Helper to use GetBulk reduces the resource footprint of Network Manager in the following ways:

- It reduces the impact on management network because fewer SNMP packets are exchanged.
- It reduces the impact on managed devices because fewer SNMP packets are processed.
- It reduces the CPU time required by the Network Manager processes such as the Discovery engine, ncp_disco, and the Polling engine, ncp_poller, due to reduced overheads.

Use of GetBulk decreases the time taken for the discovery data collection phases as a large percentage of the time required for data collection is taken up waiting for packets to traverse the network. This usage significantly reduces the time taken to collect data for large tables, such as interface and routing tables.

Configuring Network Manager to use GetBulk

You can configure the SNMP Helper to use GetBulk. You can also exclude specific devices from GetBulk support.

If you configure the SNMP Helper to use GetBulk, then this will apply to all pollers in the current domain. The SNMP Helper will also use GetBulk for all devices in the domain accessed using SNMP v2 or SNMP v3, unless you exclude specific devices as described in the following steps.

Note: When GetBulk is enabled, then for each GetBulk-capable device, a GetBulk request is always sent instead of a GetNext request.

To configure the SNMP Helper to use GetBulk, perform the following steps.

1. Edit the following configuration file: `NCHOME/etc/precision/NcPollerSchema.cfg`.

   Note: You can make the NcPollerSchema.cfg file domain specific by copying it to `NCHOME/etc/precision/NcPollerSchema.`*`DOMAIN_NAME`*`.cfg`, where *DOMAIN_NAME* is the name of the domain.
2. Find the insert into the `config.properties` database and set the value for the `UseGetBulk` property to `1`.
3. Save the file `NCHOME/etc/precision/NcPollerSchema.cfg`.

4. Optional: If you have network devices that do not support GetBulk, then you can exclude these network devices on a device-by-device basis by performing the following steps:
   a. Edit the following configuration file: NCHOME/etc/precision/ SnmpStackSecurityInfo.cfg.

      Note: You can make the SnmpStackSecurityInfo.cfg file domain-specific by copying it to NCHOME/etc/precision/ SnmpStackSecurityInfo.*DOMAIN_NAME*.cfg, where *DOMAIN_NAME* is the name of the domain.
   b. For each device that you want to exclude from GetBulk support, add an insert into the SnmpStackSecurityInfo.cfg configuration file, similar to the following example. The following example insert excludes the device 10.0.13.74 from GetBulk support.

```
insert into snmpStack.accessParameters
    ( m_NetAddress, m_UseGetBulk )
values
    ( '10.0.13.74', 0 );
```

   c. Once you have added inserts for each of the devices to exclude, save the file NCHOME/etc/precision/ SnmpStackSecurityInfo.cfg.
5. Activate the changes by performing one or both of the following:
   - Start or schedule a new full discovery. Discovery will now make use of GetBulk.
   - Restart the Polling engine, ncp_poller, with the -readsnmpconfig command-line option specified.

Configuring maximum number of repetitions for GetBulk requests

The GetBulk command is used to retrieve all the rows of a table from a network resource, for example, to retrieve all the rows in a routing table from a router. The max-repetitions parameter indicates how many rows of the table are to be retrieved in a single GetBulk operation. You can adjust the GetBulk configuration settings to minimize the number of packets exchanged as part of the GetBulk operation.

The SNMP Helper determines the value of the maximum number of repetitions for GetBulk requests (the max-repetitions parameter) based on the following calculation:

max-repetitions = DefaultGetBulkMaxReps / #varbinds

Where:

- The *DefaultGetBulkMaxReps* property is defined in the $NCHOME/etc/precision/ NcPollerSchema.cfg file. The default value is 20. This property defines the number assigned to the max-repetitions field in GetBulk requests issued by Network Manager processes. The value 20 is used when the GetBulk request contains a single varbind. If multiple varbinds are included, then the value is adjusted accordingly (divided by the number of varbinds), so that responses always contain a similar number of varbinds.
- *#varbinds* is the number of variable bindings being requested. In the SNMP Helper, this value is usually 1. However, the value can vary depending on where the SNMP Helper is being deployed and on the following factors:
  – In the Discovery engine, ncp_disco, the *#varbinds* value can vary depending on the code in the discovery agent.

– In the Polling engine, ncp_poller, the *#varbinds* value can vary depending on which MIB objects are included in the poll definition.

1. Edit the following configuration file: `$NCHOME/etc/precision/NcPollerSchema.cfg`.

   Note: You can make the NcPollerSchema.cfg file domain specific by copying it to `$NCHOME/etc/precision/NcPollerSchema.`*`DOMAIN_NAME`*`.cfg`, where *DOMAIN_NAME* is the name of the domain.
2. Find the line that defines the value of the *DefaultGetBulkMaxReps* property.
3. Change the value assignment for the *DefaultGetBulkMaxReps* property.
4. Save the file `$NCHOME/etc/precision/NcPollerSchema.cfg`.
5. Restart the Polling engine, ncp_poller to activate the configuration changes.

Configuring SSO between Charting and Tivoli Monitoring

The instructions below describe how to configure IBM Tivoli Monitoring and Charting for single sign on (SSO) using the `ITMWebService`. At the bottom are also instructions for how to configure Tivoli Integrated Portal to communicate with a remote Tivoli Monitoring Web Service, which only works in an SSO environment.

- Install Tivoli Monitoring 6.2.2. You must configure Tivoli Monitoring Tivoli Enterprise Portal Server to use LDAP and SSO during the configuration step. Refer to Tivoli Monitoring documentation, but essentially you need to do the following:
  – During the Tivoli Enterprise Portal Server configuration, check the LDAP and SSO check boxes. Enter the information to connect to LDAP.
  – When the SSO configuration is displayed, enter `TIPRealm` for the realm name and your network domain for your domain name (for example, `raleigh.ibm.com`).
  – Export the LTPA keys to disk. For more information, see: http://www-01.ibm.com/support/knowledgecenter/SS7JFU_7.0.0/com.ibm.websphere.express.doc/info/exp/ae/tsec_altpaexp.html?cp=SS7JFU_7.0.0%2F1-3-0-0-2-1.
  – Take a note of the password.
  – Copy the `\ibm\itm\cnps\sqllib\kfwtipewas.properties` file to the `\ibm\itm\cnps` directory and run `reconfigure` for the Tivoli Enterprise Portal Server. Once the `reconfigure` is complete, the web service feature is activated.
- Install and configure Tivoli Integrated Portal to include the charting component.

To configure SSO for the charting component and Tivoli Monitoring:

1. Configure Lightweight Directory Access Protocol (LDAP) security in Tivoli Integrated Portal:
   a. Add and configure an LDAP repository.
   b. Configure Tivoli Integrated Portal to allow you to manage LDAP users in the portal.
2. Configure Tivoli Integrated Portal for SSO. Make sure both Tivoli Monitoring and the embedded application server for Tivoli Integrated Portal use the same LTPA keys (import the LTPA keys you exported from Tivoli Monitoring), Realm names, and exchange SSL certificates. For more information, see: http://www-01.ibm.com/support/knowledgecenter/SS7JFU_7.0.0/com.ibm.websphere.express.doc/info/exp/ae/tsec_altpaimp.html?cp=SS7JFU_7.0.0%2F1-3-0-0-2-2

3. On the Tivoli Integrated Portal Server, change to *tip_home_dir*/profiles/TIPProfile/bin and run the following command to configure Tivoli Integrated Portal to use SSO when communication with Tivoli Monitoring:

   Windows `tipcli.bat ITMLogin -hostname <TEPS_hostname> -port 1920`

   Linux UNIX `tipcli.sh ITMLogin -hostname <TEPS_hostname> -port 1920`

4. 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`
5. Create the users in Tivoli Integrated Portal and assign them to a role that has privileges to view the charts from Tivoli Monitoring, such as `chartAdministrator`.
6. Associate the same users that you created with a Tivoli Enterprise Portal user.
   a. Log into the Tivoli Enterprise Portal and associate that same user from LDAP with a Tivoli Enterprise Portal user.
   b. In Tivoli Enterprise Portal, select **Edit --> Manage Users**.
   c. Click the button to create a new user and enterr the user ID and user name. To be consistent, you can use the same user ID as in Tivoli Integrated Portal.
   d. Enter the distinguised name. You can get this from the Tivoli Integrated Portal Manage Users panel. You may be able to find it using the **Find** button in the Tivoli Enterprise Portal. If you do not locate it with the **Find** button, copy and paste it from the Tivoli Integrated Portal Manage Users panel. It should look like this: `uid=`*`userID`*`,o=IBM,c=US`
   e. Give the user `Workspace Administration Mode` permission.

   Note: When you log into the Tivoli Integrated Portal, you cannot use `sysadmin` which is the default Tivoli Monitoring user or `tipadmin` which is the default Tivoli Integrated Portal user because neither of these users are in stored in the LDAP.
7. When you have finished, follow these steps to test the configuration:
   a. Log into he Tivoli Integrated Portal as one of the users that you created with chart access.
   b. Create a new page using **Settings** > **Page Management** > **New Page**.
   c. Select the Charting portlet and click **OK**.
   d. Give the page a name and save it.
   e. Navigate to the charting portlet and select **Tivoli Charts**.
   f. In the table toolbar, click **New** to create a new connection and provide the necessary information to connect to the remote Tivoli Monitoring web service and click **OK**. For example:

- Name: `ITM`
- Protocol: `http`. This can be later changed to `https` if required but for testing purposes `http` is sufficient.
- Hostname: *`TEPS_server_name`*`.raleigh.ibm.com`. This is the hostname of the Tivoli Enterprise Portal server, for example, `tiv-isc09.ibm.com`.
- Port: `15200`. If you use `https`, the default port is `15201`.
- Service name: `TIPWebServiceHttpRouter`.

g. Select one of these groups. It will populate the table with the charts and tables from that Tivoli Monitoring workspace.

h. Select a chart and click **Finish**.

The chart is imported, which can take some time initially. When processing is complete, the chart is rendered in the portlet. If you do not see the chart, review any error messages and make sure you followed these steps correctly.

Related tasks:

"Configuring single sign-on" on page 204
Use these instructions to establish single sign-on support and configure a federated repository.

"Adding an external LDAP repository" on page 198
After installation, you can add an IBM Tivoli Directory Server or Active Directory Microsoft Active Directory Server as an LDAP repository for Network Manager.

"Configuring an external LDAP repository" on page 199
You can configure the Tivoli Integrated Portal Server to communicate with an external LDAP repository.

"Managing LDAP users in the console" on page 200
To create or manage users in the portal that are defined in your LDAP repository, in the WebSphere Application Server administrative console specify the supported entity types.

The IBM Support Assistant (ISA)

The IBM Support Assistant is a tool which helps you to search and find product support and education information.

If a Problem Management Record (PMR) needs to be opened, IBM Support Assistant can save you time by automatically gathering support information. The IBM Support Assistant provides the following services:

- Improved access to IBM support information, IBM newsgroups, and other resources through a federated search interface (one search across multiple resources)
- Easy access to IBM educational materials and product education roadmaps
- Easy access to IBM product home pages, product support pages, and product forums or newsgroups through convenient links
- Improved PMR time to resolution by collecting key system information and sending the data to IBM through electronic creation of a PMR

A Network Manager plug-in is available for the IBM Support Assistant. The plug-in is needed by the IBM Support Assistant so that it can diagnose Network Manager problems.

For more information about the IBM Support Assistant, refer to the following IBM Web site: http://www.ibm.com/software/support/isa

Installing the IBM Support Assistant Lite collector

The IBM Support Assistant (ISA) Lite collector for Network Manager provides automated data collection on systems where Network Manager is installed. It can collect the information about logs, rules files, configuration data, and so on.

To install the ISA Lite collector, perform the following steps:

1. Install Network Manager.
2. Open the following technote: http://www-01.ibm.com/support/docview.wss?uid=swg27015867
3. Follow the steps in the technote to set up and use the ISA Lite collector for Network Manager.

Appendix. 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 character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 31 are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Table 31. 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.

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

This Software Offering does not use cookies or other technologies to collect personally identifiable information.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's privacy policy at http://www.ibm.com/privacy.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Printed in the Republic of Ireland