

Network Manager IP Edition
4.2

Installation and Configuration Guide



Note

Before using this information and the product it supports, read the information in [“Notices” on page 211.](#)

This edition applies to version 4.2 of IBM Tivoli Network Manager IP Edition (product number 5724-S45) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2006, 2021.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this publication.....	vii
Publications.....	vii
Accessibility.....	viii
Tivoli technical training.....	ix
Support and community information.....	x
 Chapter 1. Downloading Network Manager.....	 1
 Chapter 2. Planning for installation.....	 3
Deployment of Network Manager.....	3
Deployment scenarios.....	3
Deployment considerations.....	14
Deployment examples.....	16
Checking system prerequisites.....	20
Network domains.....	20
Event collection using multiple domains per ObjectServer.....	21
Example visualization of topology from multiple domains.....	22
Hardware requirements.....	23
Processor selection guidelines.....	23
Requirements to run the installer.....	24
Requirements for the core components.....	24
Requirements for the GUI components.....	25
Requirements for the topology database server.....	26
Disk space for events and interfaces.....	27
Swap space requirements (UNIX).....	27
Discovery memory requirements.....	27
Software requirements.....	27
Compatibility requirements for other products.....	28
Supported topology databases.....	30
Supported operating systems.....	30
Supported browsers for Web applications.....	32
Operating system tools.....	32
UNIX user requirements.....	32
Installation directory requirements.....	33
File handle requirements.....	33
Password requirements.....	34
Network requirements.....	34
List of ports used by the product.....	34
DNS requirements.....	35
Bandwidth requirements for discovery.....	36
About DNCIM.....	36
FIPS 140-2 installations.....	36
 Chapter 3. Preparing to install.....	 39
Running installation and maintenance procedures as root or non-root.....	39
Configuring Red Hat Linux Enterprise Edition.....	39
Preinstallation tasks for AIX.....	39
Configuring SSH.....	40
Installation of a zip utility.....	40
Checking I/O Completion Port (IOCP) settings.....	40

Chapter 4. Installing Network Manager and related products.....	41
Checklist for installation.....	41
Installing and configuring IBM Installation Manager.....	44
Installing IBM Installation Manager by downloading the product files.....	44
Installing IBM Installation Manager by connecting directly to Passport Advantage.....	45
Installing and configuring a topology database.....	47
Installing and running the Network Manager database scripts.....	48
Setting up existing Db2 databases on UNIX.....	49
Installing and configuring Oracle databases on UNIX.....	50
Setting up NCIM to use multibyte characters.....	52
Installing and configuring Tivoli Netcool/OMNIBus.....	52
ConfigOMNI command-line options.....	54
Installing the Network Manager core components.....	55
Installing WebSphere Application Server.....	59
Installing Dashboard Application Services Hub.....	60
Installing Tivoli Netcool/OMNIBus Web GUI.....	63
Installing the Network Manager GUI components.....	64
Installing and configuring Cognos Analytics.....	66
Installing Network Manager reports.....	68
Installing the Network Health Dashboard (Netcool Operations Insight customers only).....	70
Installing and uninstalling fix packs.....	70
Post-installation tasks.....	70
Chapter 5. Uninstalling Network Manager.....	73
GUI applications.....	73
Reports.....	74
Network Manager core components and Tivoli Netcool/OMNIBus.....	75
WebSphere Application Server.....	76
Chapter 6. Installing and uninstalling fix packs.....	77
Installing fix packs.....	77
Applying schema updates.....	79
Checking schema updates.....	80
Uninstalling fix packs.....	80
Chapter 7. Integrating.....	83
Tivoli Netcool/OMNIBus.....	84
Configuring an ObjectServer for use with Network Manager core processes.....	84
Configuring the user repository.....	85
Configuring the Tivoli Netcool/OMNIBus Web GUI data source name.....	86
Configuring topology event types.....	86
Installing and configuring probes.....	87
Installing the Knowledge Library.....	87
Tivoli Netcool/OMNIBus integration reference.....	87
Netcool Configuration Manager.....	100
CCMDB, TADDM, and TBSM.....	101
Prerequisites.....	101
Configuring the DLA.....	102
Creating a Discovery Library book.....	108
Fine-tuning the data export.....	109
Loading Discovery Library books and enabling bidirectional launch.....	114
Configuring TADDM to start Network Manager.....	114
Configuring Network Manager to start TADDM.....	116
Importing TADDM GUIDs into the NCIM database.....	117
Integration with TBSM.....	118
Configuring the Dashboard Application Services Hub	118

IBM Tivoli Monitoring.....	118
IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.....	118
Installing and configuring.....	119
Accessing discovery data from dNCIM.....	126
Chapter 8. Upgrading and migrating.....	129
About upgrading.....	129
Upgrade paths and limitations.....	129
Default locations for different product versions.....	129
What data is migrated.....	130
Upgrading Network Manager.....	132
Preparing to upgrade.....	132
Updating the database.....	132
Migrating the core components.....	133
Migrating the GUI components.....	138
Migrating network topology.....	142
Chapter 9. Configuring.....	147
Configuring NCIM connection properties.....	147
Configuring encryption length and type.....	147
Configuring Network Manager for UNIX operating systems.....	148
Configuring root/non-root permissions.....	148
Loading updated MIB information.....	151
Configuring Cognos Analytics.....	152
Configuring reports for existing installations.....	152
Enabling historical polling.....	153
Enabling failover.....	153
About failover.....	153
About NCIM topology database high availability.....	154
Failover architectures.....	155
Failover operation.....	163
Limitations of failover.....	169
Configuring failover.....	170
Troubleshooting failover.....	187
Configuring security.....	192
Configuring cookies.....	192
Protecting against clickjacking.....	192
Changing the IP address and hostname of the Network Manager installation.....	193
For Network Manager.....	193
On the OMNIBus server.....	194
Updating Network Manager for a changed OMNIBus IP address.....	194
Updating DASH for a changed OMNIBus IP address.....	195
On the DASH server.....	195
Updating Network Manager for changed DASH hostname.....	196
Configuring Network Manager for a changed IP address of the Db2 NCIM server.....	196
Setting environment variables.....	197
Default directory structure.....	198
Configuring Juniper PE Devices.....	201
Configuring domains.....	202
Adding network domains.....	202
Binding a domain to a network interface controller (NIC).....	203
Configuring a dNCIM database on Linux on IBM z Systems.....	204
Configuring the SNMP Helper.....	205
Configuring SNMP Helper throttling.....	206
Configuring GetBulk support for SNMP v2 and v3.....	207
Configuring authentication.....	209
Changing the user authentication method.....	209

Configuring OQL Service Provider authentication.....	209
The IBM Support Assistant (ISA).....	210
Installing the IBM Support Assistant Lite collector.....	210
Notices.....	211
Trademarks.....	212

About this publication

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

Publications

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

Your Network Manager library

The following documents are available in the Network Manager library:

- The *IBM Tivoli Network Manager IP Edition Release Notes* give important and late-breaking information about Network Manager. This publication is for deployers and administrators, and should be read first.
- The *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide* describes how to install Network Manager. It also describes necessary and optional post-installation configuration tasks. This publication is for administrators who need to install and set up Network Manager.
- The *IBM Tivoli Network Manager IP Edition Administration Guide* describes administration tasks such as how to start and stop the product, discover the network, poll the network, manage events, administer processes, and query databases. This publication is for administrators who are responsible for the maintenance and availability of Network Manager.
- The *IBM Tivoli Network Manager Reference* contains reference information including the system languages, databases, and Perl API used by Network Manager. This publication is for advanced users who need to customize the operation of Network Manager.

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*

Includes installation and upgrade procedures 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*

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*

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*

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*

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 products, as they become available and whenever they are updated, to the IBM Knowledge Center Web site at:

<http://www.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 IBM publications online at the following Web site:

<http://www.ibm.com/e-business/linkweb/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 IBM publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to the following Web site:

<http://www.ibm.com/e-business/linkweb/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

Network Manager includes the following major accessibility features:

- Operations that use a screen reader.

Network Manager uses IBM Installation Manager to install the product. You can read about the accessibility features for IBM Installation Manager at https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

Network Manager uses the latest W3C Standard, <http://www.w3.org/TR/wai-aria/>, to ensure compliance to <http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards>, and <http://www.w3.org/TR/WCAG20/>. To take advantage of accessibility features, use the latest release of your screen reader in combination with the latest web browser that is supported by this product.

The Network Manager online product documentation in IBM Knowledge Center is enabled for accessibility. The accessibility features of IBM Knowledge Center are described at <https://www.ibm.com/support/knowledgecenter/v1/content/about/releasenotes.html#accessibility>.

Keyboard navigation

This product uses standard navigation keys.

Interface information

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:

- The Network Manager user interfaces do not have content that flashes more than two times in any one second period.

The Network Manager web user interface includes WAI-ARIA navigational landmarks that you can use to quickly navigate to functional areas in the application.

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 -**.

Related accessibility information

In addition to standard IBM help desk and support websites, IBM has established a TTY telephone service for use by deaf or hard of hearing customers to access sales and support services:

TTY service
800-IBM-3383 (800-426-3383)
(within North America)

IBM and accessibility

For more information about the commitment that IBM has to accessibility, see <https://www.ibm.com/able>.

Tivoli technical training

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

<https://www.ibm.com/training/search?query=tivoli>

Support and community information

Use IBM Support, Service Management Connect, and Tivoli user groups to connect with IBM and get the help and information you need.

IBM Support

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 <https://www.ibm.com/support/home/> 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 https://www.ibm.com/support/knowledgecenter/SLLVC/welcome/isa_welcome.html

Chapter 1. Downloading Network Manager

The procedure for downloading the product differs for General Availability (GA) releases and fix packs.

Before you begin

Note: If you use Network Manager as part of a solution, you must also check the compatibility of the versions of all component products in the solution documentation. For example, if you use Netcool Operations Insight, check the *product and component version matrix* for your version of Netcool Operations Insight at <https://www.ibm.com/support/knowledgecenter/en/SSTPTP>.

About this task

To download the product, locate your version in the following table:

Table 1. Download locations		
Product version	Download location	More information
4.2 Fix Pack 13	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm16440293
4.2 Fix Pack 12	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm16364949
4.2 Fix Pack 11	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm16257035
4.2 Fix Pack 10	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm16233900
4.2 Fix Pack 9	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm12984181
4.2 Fix Pack 8	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=ibm11099863
4.2 Fix Pack 7	Fix Central https://www.ibm.com/support/fixcentral/	http://www.ibm.com/support/docview.wss?uid=ibm10886151
4.2 Fix Pack 6	Fix Central https://www.ibm.com/support/fixcentral/	http://www.ibm.com/support/docview.wss?uid=ibm10794123

<i>Table 1. Download locations (continued)</i>		
Product version	Download location	More information
4.2 Fix Pack 5	Fix Central https://www.ibm.com/support/fixcentral/	http://www.ibm.com/support/docview.wss?uid=swg24044739
4.2 Fix Pack 4	Fix Central https://www.ibm.com/support/fixcentral/	http://www.ibm.com/support/docview.wss?uid=swg24044399
4.2 Fix Pack 3	Passport Advantage http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm	http://www.ibm.com/support/docview.wss?uid=swg24043360
4.2 Fix Pack 2	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=swg24042981
4.2 Fix Pack 1	Fix Central https://www.ibm.com/support/fixcentral/	https://www.ibm.com/support/docview.wss?uid=swg24042425
4.2	Passport Advantage http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm	http://www.ibm.com/support/docview.wss?uid=swg24041283

Chapter 2. Planning for installation

Read about deployment considerations and system requirements for Network Manager.

Before you begin

Check the planning documentation for all other products that you want to integrate with Network Manager. For example, if you are installing IBM Tivoli Netcool Configuration Manager, refer to the *IBM Tivoli Netcool Configuration Manager Integration Guide*.

Note: If you use Network Manager as part of a solution, you must also check the compatibility of the versions of all component products in the solution documentation. For example, if you use Netcool Operations Insight, check the *product and component version matrix* for your version of Netcool Operations Insight at <https://www.ibm.com/support/knowledgecenter/en/SSTPTP>.

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
- Large customer network
- Very large customer network

A further deployment scenario is the following: Telecommunications company or service provider 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.

<i>Table 2. Example customer networks compared</i>						
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	None	Netcool Operations Insight TADDM	Netcool Operations Insight TADDM	Netcool Operations Insight TADDM

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.

<i>Table 3. Example Network Manager deployments compared</i>						
Settings	Demo	Enterprise				Telco
		Small	Medium	Large	Very large	
Platform	Linux® x86	Any supported platform	Any supported platform	Linux	Linux	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	Db2® or Oracle RDBMS	Db2 or Oracle RDBMS	Db2 or Oracle RDBMS	Db2 or Oracle 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.

Tip:

If you are intending to run cross-domain discoveries in order to visualize links between the different domains, you must consider how the boundaries between domains affects cross-domain links. In particular, ensure that you choose domain boundaries with a minimum of cross-domain links.

Guidelines for number of network domains

If your network exceeds a certain size, you might need to break up the network into multiple domains. Use this information to work out the number of network domains needed for your deployment.

Depending on the operating system, a single Network Manager domain can support approximately 1,000,000 network entities that are created during a discovery operation. Network entities include ports, interfaces (including logical interface elements), cards, slots, and chassis. It is theoretically possible to include more network entities in a single domain, but discovery might take a long time to complete.

On 64-bit Linux, the maximum memory allowed for an individual Network Manager process is not arbitrarily limited but depends on how much memory is installed on the server.

Generally, the discovery process (ncp_disco) and the topology model process (ncp_model) use the most memory.

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 UNIX systems can support approximately 1 million 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 500,000 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 the following equation to determine the suggested number of network domains:

Number of domains required = (Number of network entities) / 1000,000

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: 60,000
- Average number of interfaces per device: 20

This customer network will produce approximately 2,400,000 network entities:

Number of network entities = $60,000 * 20 * 2 = 2,400,000$

Based on the following calculation, this network requires *three* network domains:

Number of domains required = $2,400,000 / 1,000,000 > 2$

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 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 = $84,000 / 1,000,000 < 1$

Related concepts

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.

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.

- System is an entry workstation class machine, with 8 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, 4 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.

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 16 GB of memory, quad-core processor, and multiple physical disks in RAID 5 configuration.
- Client system: single processor, 4 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 5,000 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.

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 more network domains are required, depending on the size of network.
- Single server deployment (up to 250 network devices and 5 to 10 concurrent users).
 - Four processors.
 - Up to 32 GB of memory.
 - Multiple physical disks in RAID 5 configuration.
- Two-server deployment (up to 5,000 network devices and 10 to 20 concurrent users).
 - Four processors for system with Network Manager.
 - Four processors for system with Tivoli Netcool/OMNIBus and Dashboard Application Services Hub.
 - Up to 32 GB of memory for each server.
 - Multiple physical disks in RAID 5 configuration.
- System may be any of the supported platforms.
- Client system: single processor, 4 GB of memory, supported JRE and Internet browser
- Db2 or Oracle RDBMS used for the NCIM database on server with 4 processors and 32Gb RAM.
- Number of polling engines:
 - Single-server deployment: 1
 - Two-server deployment: One poller for chassis pings, one or more pollers for SNMP polls.
- IPv6 dual stack support is required if workstations or network devices have IPv6.

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 Business Service Manager (TBSM)
 - IBM Tivoli Application Dependency Discovery Manager (TADDM)

Network Manager deployment

Deployment choices vary depending on the size of the network. For the 5000 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 two domains.
- Deployment of a dedicated database server.
- Each of the servers requires the following:
 - 8 processors.
 - Up to 128 GB of memory.
 - 3 disk, RAID 5 multiple disk array
- For the systems used, deploy as follows:
 - Server 1: Network Manager with 36 GB of memory.
 - Server 2: Tivoli Netcool/OMNIbus and Dashboard Application Services Hub with up to 12 GB of memory.
 - Server 3 a customer-selected RDBMS (Db2 or Oracle) with up to 84 GB of memory.
- Systems to be deployed on Linux or UNIX platform.
- Db2 or Oracle RDBMS used for the NCIM database.
- 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, 4 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.

Most 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 - 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 that are to be integrated with the system, other than the required Tivoli Netcool/OMNIBus:
 - IBM Tivoli Business Service Manager
 - IBM Tivoli Application Dependency Discovery Manager

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 you survey the network to be managed, break up the network into sections that can be managed, and then assign each of the sections 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 if the memory allocations and processor counts are acceptable.
 - Memory: 32-64 GB per domain
 - Processors: 4-8 per domain, depending on workloads
- Db2 or Oracle RDBMS used for the NCIM database.
- 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 you are using AIX®, enable large memory access.
- Client system: single processor, 4 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 600 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 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 (where Network Manager is installed): four processors, 32-64 GB of memory, two or more disks. Note that beyond four 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: (where the Dashboard Application Services Hub and Tivoli Netcool/OMNIbus are installed) four processors, 16 GB of memory, two or more disks
 - System 3: database server; 4 processors, 16 GB of memory
- Db2 or Oracle RDBMS used for the NCIM database.
- 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, 4 GB of memory, supported JRE and Internet browser
- IPv6 dual stack support is required if workstations or network devices have IPv6.

LTE 4G wireless telecommunications company network

This customer is a large wireless telecommunications company providing 4G wireless telephony services using their LTE (Long term Evolution) infrastructure. The purpose of this installation is to manage this customer network by alerting 24x7 network operations center staff to major failures.

The following sections provide suggestions for a Network Manager deployment to meet the needs of this network.

Description

The network to be managed has about 5000 eNodeBs, together with a further 3000 devices, which are either in the associated Evolved Packet Core (EPC) network or functioning as mobile backhaul router devices. The Network Manager entity count discovered for this network would typically be as follows:

- For the eNodeB devices: on the order of 20 to 25 entities per eNodeB.
- For the EPC network and backhaul equipment devices: on the order of 10 to 15 entities per device.

The LTE eNodeB and associated equipment is provided by multiple vendors which can vary in complexity and scale. These devices are distributed across many locations, as is typical in a 4G mobile network. All devices to be managed are connected using Fast Ethernet or Gigabit Ethernet. The topology and network inventory data discovered by Network Manager is received from vendor-specific EMS systems, and is processed by corresponding vendor-specific Network Manager collectors.

Within this environment the following conditions typically apply:

- Number of simultaneous active GUI clients: 5 to 20.
- Polling requirements: none, since topology data is received from the EMS, hence no polling of devices is assumed.

Network Manager deployment

A three-part deployment is needed for this type of environment.

1. Network Manager core components.
2. Dashboard Application Services Hub and Cognos Analytics.
3. NCIM topology database.

These three parts can be deployed on servers (single or multiple) or on virtual machines (single or multiple). A single domain is sufficient for this type of environment. Furthermore, the following deployment settings are appropriate:

- Network Manager core components
 - 4 to 6 processors.
 - Approximately 20 GB of memory.
 - 50 GB of disk space.
- Dashboard Application Services Hub and Cognos Analytics
 - 4 to 6 processors.
 - 6 to 8 GB of memory.
 - 20 GB of disk space.
- NCIM topology database
 - 4 processors.
 - 10 GB of memory.
 - 50 GB disk space minimum configured in a suitable RAID configuration, to provide required level of fault tolerance, reliability, and performance.
 - Db2, or other supported database platform.

In addition, the following GUI client system is appropriate:

- Single processor.
- 3 GB of memory.
- Supported JRE and Internet browser.

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 a number of Network Manager components' including the following:

Network Manager core components

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.

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.

Network Manager GUI components

This component includes the Dashboard Application Services Hub GUI framework, Web GUI components, Jazz for Service Management, and Java™.

Other components

Other components include Cognos Analytics and Network Manager reports.

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

Restriction: You must not use different versions of the same products or components together, unless advised otherwise by instructions in the IBM Knowledge Center or by IBM Support. If you need multiple instances of a product or component, you must install or upgrade them to the same version and fix pack. You must also ensure that the same set of test fixes, if any, are installed. For example, if you need multiple instances of the Network Manager GUI Components in one deployment, ensure that they are the same version, fix pack, and test fixes.

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.

Restriction: A limitation of a single-server deployment is that Tivoli Netcool/OMNIbus and Network Manager must be upgraded at the same time. All upgrades to major releases must be done at the same time to avoid compatibility issues. A major release is a release that has its own documentation set, for example, Tivoli Netcool/OMNIbus V8.1.0. Fixpacks can be applied at different times.

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, Tivoli Netcool/OMNIbus, and the NCIM database. The core components are the network discovery, polling, root cause analysis and event enrichment components.
- *Server 2:* Dashboard Application Services Hub with associated Network Manager web applications.

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:* Dashboard Application Services Hub 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:

- 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.

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 Dashboard Application Services Hub 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.

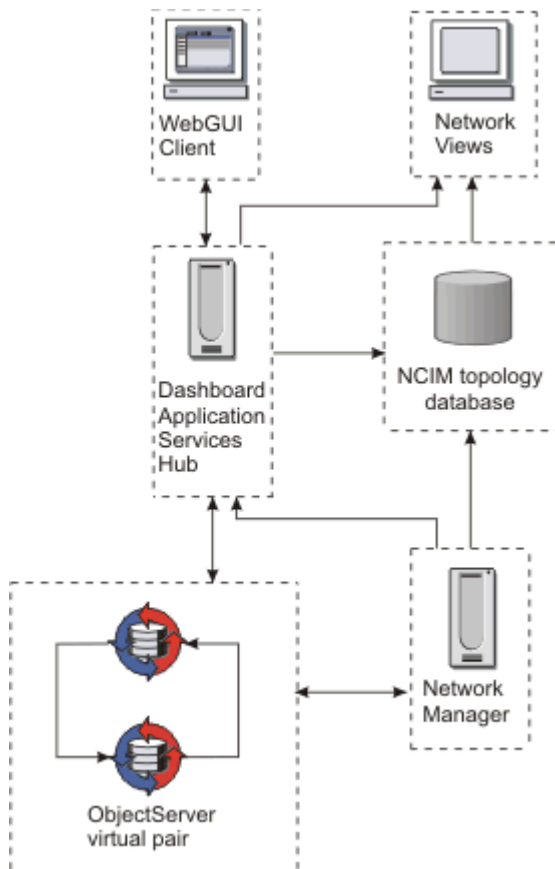


Figure 1. Simple deployment architecture

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.

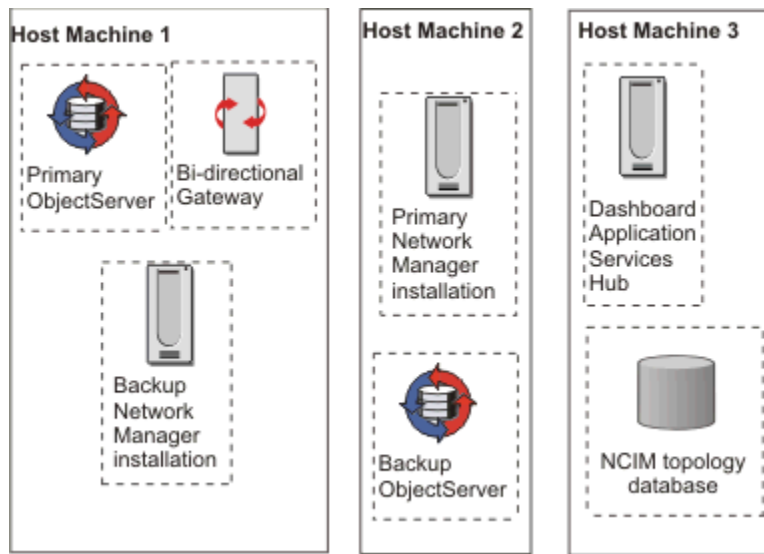


Figure 2. Simple deployment host machine allocation

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 GUI framework on host machine 3. The GUI framework includes the following software:

- WebSphere Application Server
- Dashboard Application Services Hub
- Network Manager GUI components
- Tivoli Netcool/OMNIBus Web GUI
- Cognos Analytics

Tip: If you install the Dashboard Application Services Hub on a machine with no other products, performance is likely to be better than if you install it on a machine with other products.

Note: The Network Manager core components must be installed before the Network Manager GUI framework.

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 Dashboard Application Services Hub installation in San Francisco. The ObjectServer in San Francisco consolidates the events from London and New York. The Dashboard Application Services Hub 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 Dashboard Application Services Hub server, and view topology from London and New York.

The following figure shows the architecture for this deployment.

Note: For a large deployment of this sort, network latency across the WAN should be taken into account. This is especially important if the poller is expected to store a lot of historical data. .

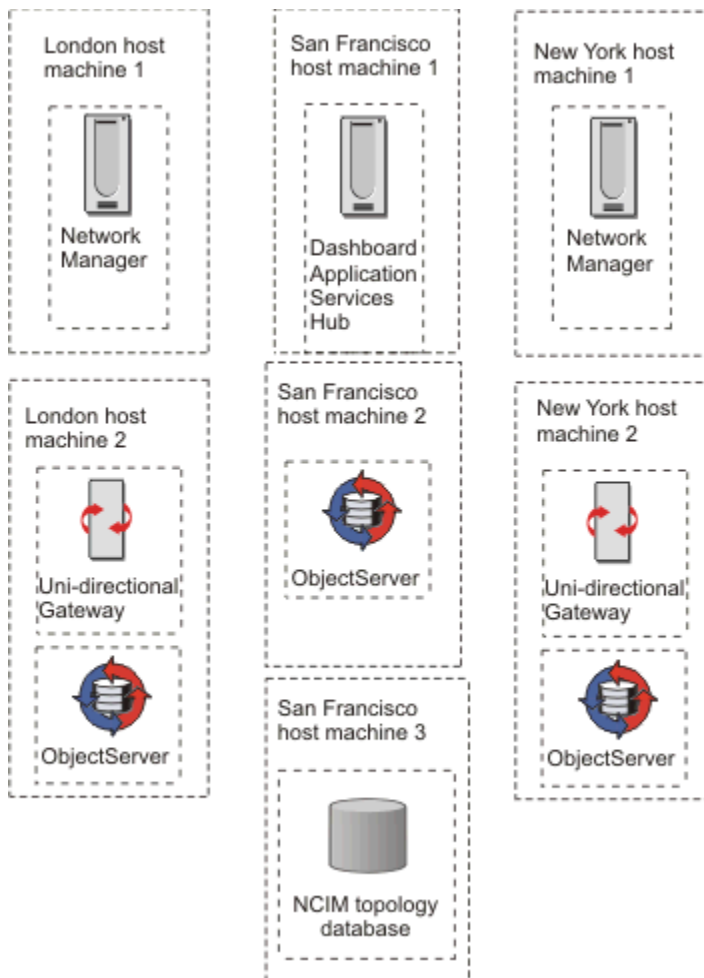


Figure 3. Large deployment architecture

Allocation of host workstations

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

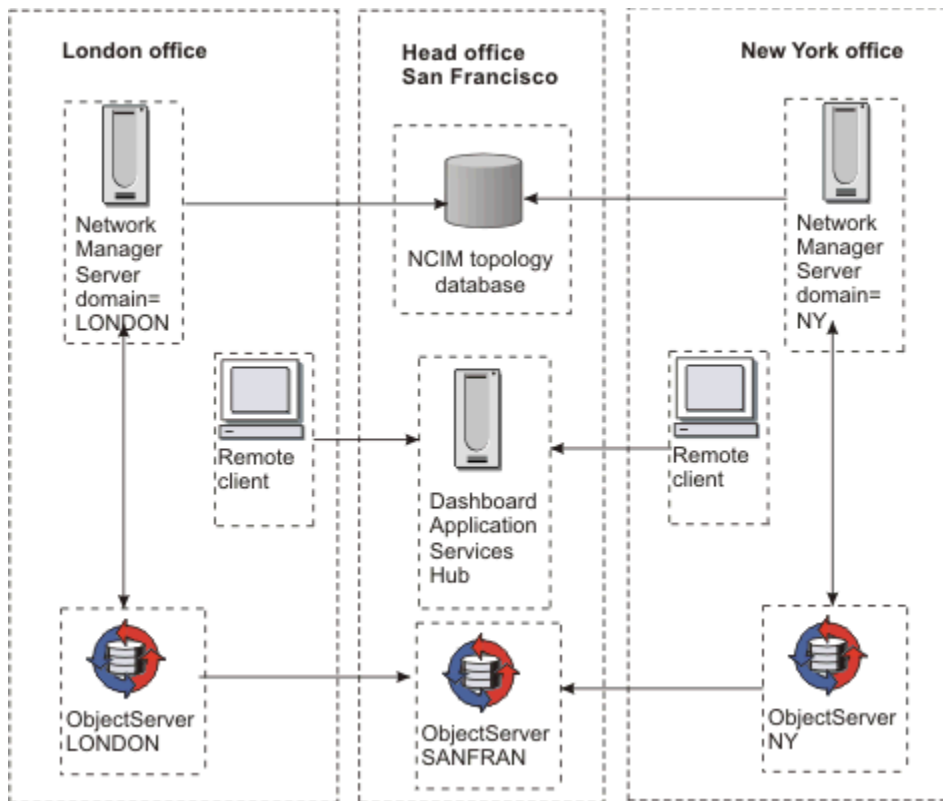


Figure 4. Large deployment host machine allocation

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. .

Note: If you are installing distributed Network Manager core component and Web application servers with different time zones, then you should set the same time zone on all servers which includes the database server as well as the core and GUI servers. This ensures that Network Manager is able to perform accurate timestamp comparisons from processes on different servers. You should also advise end users, such as network operators, that the system might display times that are different to the time in their location.

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. Install the Network Manager GUI framework on host machine 3. The GUI framework includes the following software:
 - WebSphere Application Server
 - Dashboard Application Services Hub
 - Network Manager GUI components
 - Tivoli Netcool/OMNIBUS Web GUI
 - Cognos Analytics

Tip: If you install the Dashboard Application Services Hub on a machine with no other products, performance is likely to be better than if you install it on a machine with other products.

Note: The Network Manager core components must be installed before the Network Manager GUI framework.

Checking system prerequisites

You must check system prerequisites before you install Network Manager or related products.

About this task

You can run a preliminary check of the hardware and software environment on the servers where you want to install Network Manager or related products without downloading those products. You can use IBM Prerequisite Scanner, a separate piece of software, to do this check. This initial check shows you whether you need to upgrade hardware or configure the operating system before you install your products.

In addition to the checks made by the IBM Prerequisite Scanner, the Network Manager installer runs its own checks when you attempt to install your products. The IBM Prerequisite Scanner can check for prerequisites of multiple products. The Network Manager installer checks only for the prerequisites of products that are selected for installation.

Important: The automated checks are not a substitute for understanding the hardware, software, and other prerequisites described in the documentation. Some prerequisites depend on your network or deployment and cannot be automated.

To check system prerequisites for Network Manager 4.2 core components and GUI components, you must download the scanner and the updated configuration file. Refer to the instructions at the following location: <https://www.ibm.com/support/pages/node/727673>

For instructions on using IBM Prerequisite Scanner with other products, refer to the installation documentation for other products.

Results

The results of the system prerequisites check are displayed, indicating whether the current server is suitable for installing your choice of components.

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 (_) for domain names. Any 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.
- If using multiple domains per ObjectServer, probes in each domain need to be configured 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.

Related concepts

[Guidelines for number of network domains](#)

If your network exceeds a certain size, you might need to break up the network into multiple domains. Use this information to work out the number of network domains needed for your deployment.

Related tasks

[Creating and configuring extra network domains](#)

To add more network domains, configure process control for the domains and register the domains with the NCIM topology database. Configurations and polls can be copied from existing domains. Configure or reconfigure network views to show devices on the new domains.

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 Administration 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.

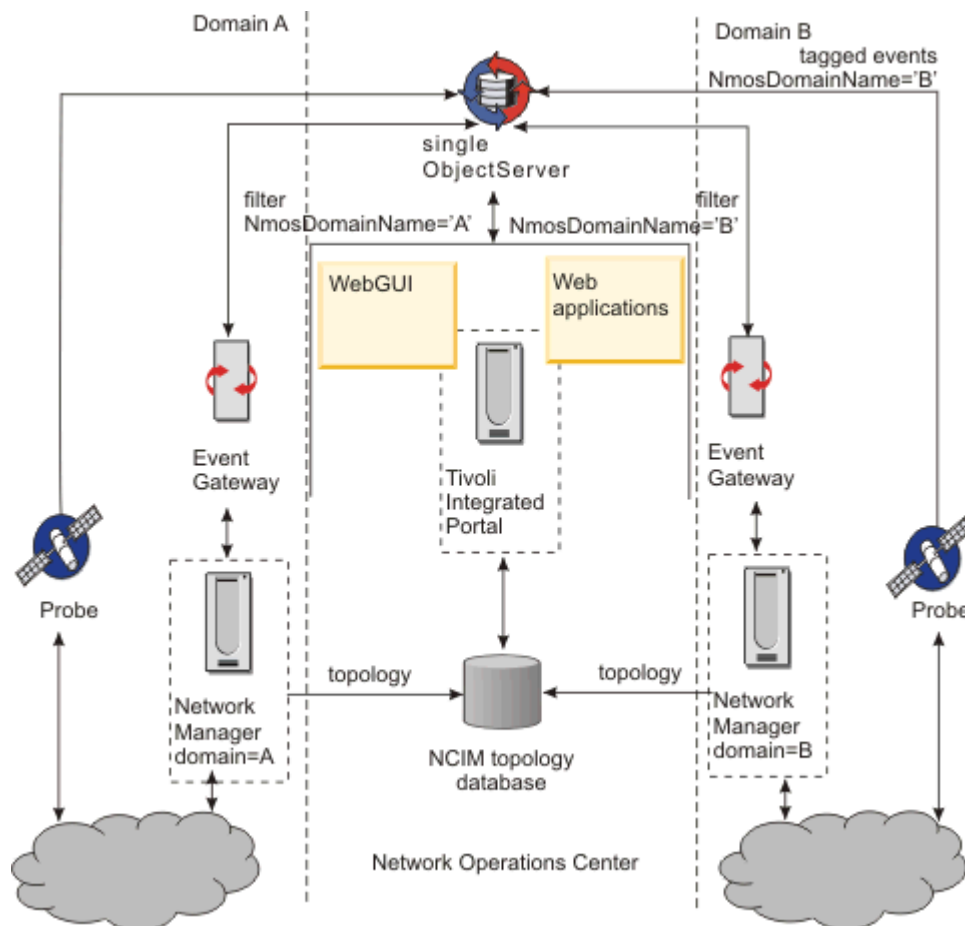


Figure 5. Managing event ownership: architecture for multiple-domain ObjectServer

Example visualization of topology from multiple domains

Web clients using a single Dashboard Application Services Hub can view topology from more than one Network Manager domain.

Multiple domains held in one topology database

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

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. All web clients connected to the Dashboard Application Services Hub can view topology maps in any of the domains by choosing a single domain from the domain menu.

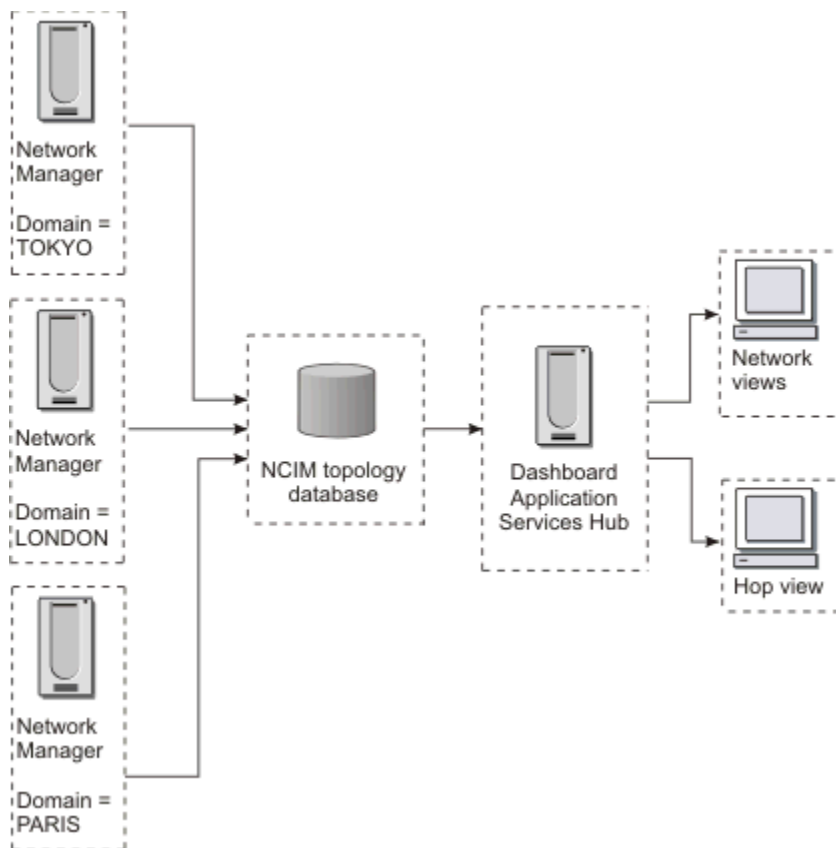


Figure 6. Viewing topology from multiple domains

If cross-domain discoveries have been run, an aggregated domain is created in the topology database, which includes device collections from all discovered domains. All web clients connected to the Dashboard Application Services Hub can view topology maps in all domains by choosing the AGGREGATION domain from the domain menu.

For more information on viewing topology, see the *Network Manager Topology Visualization Guide*.

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, 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 or more.

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 Linux on IBM z Systems 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 3.

Requirements to run the installer

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

In addition to these prerequisites, refer to the prerequisites for your version of IBM Installation Manager at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html.

Disk space requirements for installing as the root user

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. If you are installing Network Manager as the root user, you must observe the following requirements:

- At least 1 GB space in the /tmp directory on the GUI components server.
- At least 1GB space in the /var directory.
- If you install Network Manager into any location other than /opt, you must have at least 50 MB space in the /opt directory.
- At least 10GB space in the data location for IBM Installation Manager. You choose the data location during installation of IBM Installation Manager. This location is where packages are unpacked during installation and where packages are stored for rolling back.

Disk space requirements for installing as a non-root user

If you are installing Network Manager as the root user, you must observe the following requirements:

- At least 1 GB space in the /tmp directory on the GUI components server.
- At least 350 MB space free in your home directory.
- At least 10GB space in the data location for IBM Installation Manager. You choose the data location during installation of IBM Installation Manager. This location is where packages are unpacked during installation and where packages are stored for rolling back.

Requirements for the core components

To install and run 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 16 GB DRAM.
- For a distributed deployment, where only the Network Manager core components are installed on the server, you need a minimum of 8 GB DRAM.

These are minimum requirements, and the amount of memory required will vary depending on the size of the network to be managed and how you deploy Network Manager. For more information, see [“Deployment of Network Manager” on page 3](#).

Disk space requirements

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

- 5 GB hard disk space to store the software
- 4 GB hard disk space per domain 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).
- 50 GB free disk space to run Network Manager.

These are minimum values for guidance, and the amount of disk space required will vary depending on the size of the network to be managed and how you deploy Network Manager. For more information, see [“Deployment of Network Manager” on page 3](#).

Note:

For a production system that you intend to use for the long term, you must have enough additional disk space to store files that are generated by product operation, such as rollback files. If you install the Network Manager core components and Tivoli Netcool/OMNIBus, you need at least 400GB space on the partition where the products are installed.

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 36](#).

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 must meet the following hardware requirements.

Long-term disk space guidance for all GUI components and related products

For a production system that you intend to use for some time, you must have enough additional disk space to store files that are generated by product operation, such as rollback files. If you install the Network Manager GUI components, Dashboard Application Services Hub, Cognos Analytics, and Tivoli

Netcool/OMNIbus Web GUI, you need at least 100GB space on the partition where the products are installed.

Hardware requirements for installing Network Manager GUI components

To install the Network Manager GUI components, your server must meet the following 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 installing Cognos Analytics

To enable network management reports, you must have Cognos Analytics installed. Cognos Analytics is an optional component that needs to be installed separately to be able to use the reporting feature of Network Manager.

Review the hardware requirements for Cognos Analytics to make sure you meet your performance requirements.

Important: Ensure that you have at least 17GB of free space in the location where you want to install Cognos Analytics.

For detailed information, refer to the information about hardware requirements for your version of Cognos Analytics in the Cognos Analytics Knowledge Center at: <https://www.ibm.com/support/knowledgecenter/SSEP7J>.

Requirements for the topology database server

Read about Network Manager topology database requirements.

Disk space requirements

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

- 3 to 5 GB for Db2.
- 3 to 5 GB for 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.

For a large network contained within a single domain you should have 5 GB for the topology data, and a total of 50 GB to cover storage of data as well. For more information about planning the Network Manager deployment for your network including considerations for size and domains, see [“Deployment of Network Manager” on page 3](#).

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:

$$3000 * 30 * 4 \text{ KB} = 360 \text{ MB}$$

The total disk space required is therefore:

$$512 \text{ MB} + 512 \text{ MB cache} + 360 \text{ MB} + (4 \text{ KB} * 5000) = 1.4\text{GB}$$

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.

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.

Related concepts

Guidelines for number of network domains

If your network exceeds a certain size, you might need to break up the network into multiple domains. Use this information to work out the number of network domains needed for your deployment.

Software requirements

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

Compatibility requirements for other products

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

Products required by Network Manager

The following products and components are required by Network Manager. Network Manager requires specific versions of these products.

Note: If you use Network Manager as part of a solution, you must also check the compatibility of the versions of all component products in the solution documentation. For example, if you use Netcool Operations Insight, check the *product and component version matrix* for your version of Netcool Operations Insight at <https://www.ibm.com/support/knowledgecenter/en/SSTPTP>.

Java Runtime Environment (JRE)

Network Manager does not install a JRE. It uses the JRE that is installed by other products, such as WebSphere Application Server. You must use the appropriate JRE for the combination of products or components that are installed on any one server.

Network Manager itself, requires Java 8 or later, for version 4.2 Fix Packs 8 and 9. It changes the default Java used by WebSphere Application Server to Java 8. For Network Manager version 4.2 Fix Pack 10 or later, the necessary Java Development Kit is available in the package to use WebSphere Application Server.

If you do not have the correct version of Java, you might see an error message similar to the following:

```
ERROR: IBM WebSphere SDK Java Technology Edition is not installed or selected to be installed.
```

Before installing Network Manager Fix Pack 8 or 9, ensure that Java 8 is installed in WebSphere. List the available Java Development Kits by running the following command:

```
/opt/IBM/WebSphere/AppServer/bin/managesdk.sh -listAvailable
```

If the command output does not include a line similar to the following: CWSKD1005I: SDK name: 1.8_64, download Java 8 here: <https://www.ibm.com/support/pages/ibm-websphere-java-sdks-websphere-application-server-v85514#SDK80>, add the zip file as a repository to IBM Installation Manager, and use the **Install** option to install the new JDK version.

Tivoli Netcool/OMNIbus

Network Manager requires Tivoli Netcool/OMNIbus. It supports the following versions of Tivoli Netcool/OMNIbus:

- V7.4
- V8.1 Fix Pack 24 or later

Tivoli Netcool/OMNIbus Web GUI

Network Manager supports Tivoli Netcool/OMNIbus Web GUI V8.1 **Fix Pack 11** Fix Pack 20, or later.

Dashboard Application Services Hub

Network Manager requires Dashboard Application Services Hub Version 3.1.3.9 or later.

IBM Websphere Application Server

Network Manager requires IBM Websphere Application Server Version 8.5.5.18 (version 8) or 9.0.5.6 (version 9).

Note: If you want to use WebSphere Application Server version 9, you must have new installation of WebSphere Application Server version 9, Network Manager Fix Pack 11 and Tivoli Netcool/OMNIbus Web GUI Version 8.1.0.20 or later. This is because the upgrade path is not available for WebSphere Application Server from version 8 to version 9.

IBM Websphere SDK

Network Manager requires IBM Websphere SDK Java Technology Edition Version 8.

IBM Installation Manager

Network Manager requires IBM Installation Manager V1.9.1.4 or later. On SuSE Linux V11 and V12 for System z, only the 32-bit version of IBM Installation Manager is supported.

Jazz for Service Management

Network Manager requires Jazz for Service Management V1.1.3.9 or later.

Previous versions of Network Manager

Install Network Manager 4.2 in a different directory to Network Manager V4.1.1 or earlier.

Requirements for products that are compatible with Network Manager

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.

Cognos Analytics

If you want to run reports, and you install Network Manager Reports, you also require Cognos Analytics V11.

- **Fix Pack 11** As of 4.2 Fix Pack 11, Tivoli Common Reporting is not supported. You must use Cognos Analytics.
- **Fix Pack 1** For 4.2 Fix Pack 1, Tivoli Common Reporting V3.1.3.0. Jazz for Service Management V1.1.3.0 contains Tivoli Common Reporting V3.1.3.0.
- For the 4.2 GA version, Tivoli Common Reporting V3.1.2 Fix Pack 1. Jazz for Service Management V1.1.2.1 contains Tivoli Common Reporting V3.1.2.

Important: Ensure that you have at least 17GB of free space in the location where you want to install Cognos Analytics.

IBM Tivoli Netcool Configuration Manager

Network Manager supports IBM Tivoli Netcool Configuration Manager 6.4.2 or later.

IBM Tivoli Monitoring

Network Manager is compatible with IBM Tivoli Monitoring version 6.3 FP 2 or later on AIX, Linux, or Windows. The Agent itself (IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition) only runs on Linux and AIX, because Windows is not a supported platform for Network Manager 4.2.

Note: IBM Tivoli Monitoring version 6.3 Fix Pack 2 is included in the Network Manager V4.2 package.

IBM Tivoli Business Service Manager

Network Manager supports IBM Tivoli Business Service Manager 6.1.1.

IBM Tivoli Application Dependency Discovery Manager and IBM Tivoli Change and Configuration Management Database

Network Manager supports IBM Tivoli Application Dependency Discovery Manager and IBM Tivoli Change and Configuration Management Database 7.2.1 or later.

Related tasks

[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.

Supported topology databases

The default topology database for Network Manager is IBM Db2 10.5 Enterprise Server Edition.

Network Manager supports the following topology databases:

- IBM Db2 version 10.1 Enterprise Server Edition
- IBM Db2 version 10.5 Workgroup Server Edition
- IBM Db2 version 10.5 Enterprise Server Edition
- IBM Db2 version 11.1 Enterprise Server Edition
- IBM Db2 version 11.5 Enterprise Server Edition
- **Fix Pack 3** IBM Db2 version 11.1 Advance Enterprise Server Edition
- Oracle Database version 11g, Enterprise Edition with Partitioning option (Support added in Network Manager 4.2 Interim Fix 2)
- Oracle Database version 12c, Enterprise Edition with Partitioning option
- Oracle Database version 19c, Enterprise Edition with Partitioning option

Important: All of the database systems cited above include table partitioning capability. The Oracle database systems require the Partitioning option to be included. Table partitioning is required for Network Manager to function properly.

When setting up failover, you can configure Network Manager to operate in the Db2 High Availability Disaster Recovery (HADR), or in the Oracle Real Application Clusters (RAC) environment, depending on your database. For more information, see [“Configuring failover” on page 170](#).

For a matrix of supported operating systems and databases, see the detailed system requirements document at:

<https://www.ibm.com/software/reports/compatibility/clarity/>

Important: Ensure that your database has all the recommended patches applied, including the latest patch levels.

Related tasks

[Installing and configuring a topology database](#)

Your database administrator must install and configure a supported topology database before you can install Network Manager.

Supported operating systems

Network Manager is supported on the following operating systems.

For the most current information about supported operating systems, see the detailed system requirements document at:

<https://www.ibm.com/software/reports/compatibility/clarity/>

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

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

- AIX 6.1 iSeries and pSeries
- AIX 7.1 iSeries and pSeries
- AIX 7.2 iSeries and pSeries

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

- Red Hat Enterprise Linux Server 6 (x86-64)
- Red Hat Enterprise Linux Server 7 (x86-64)
- **Fix Pack 11** Red Hat Enterprise Linux Server 8 (x86-64)
- SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 and SP3
- **Fix Pack 3** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)
- **Fix Pack 10** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP4
- **Fix Pack 11** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP5

Fix Pack 3 From Fix Pack 3 to Fix Pack 5, on Linux on IBM z Systems, the following versions are supported:

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP1 on IBM z Systems (s390x, 64 bit)

Fix Pack 6 From Fix Pack 6 onwards, on Linux on IBM z Systems, the following versions are supported:

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP2 and SP3 on IBM z Systems (s390x, 64 bit)

Fix Pack 10 From Fix Pack 10 onwards, on Linux on IBM z Systems, the following versions are supported:

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP5 on IBM z Systems (s390x, 64 bit)

The following hypervisor and operating system combinations are supported:

- VMware ESX 5.0, 5.5, 6.0:
 - Red Hat Enterprise Linux Server 7 (x86-64)
 - SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 and SP3
 - **Fix Pack 3** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)

Additional requirements for AIX

AIX

Ensure that you have either the unzip or GNU tar utilities installed so that you can uncompress the installation file. To install these utilities, go to: <http://www-03.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html>.

Ensure that GTK2 is installed. To install GTK2, see the following technote: <http://www.ibm.com/support/docview.wss?uid=swg21631478>.

Library requirements for Linux systems

Linux

Network Manager components require the following libraries and any dependencies of these packages. Ensure you have these libraries on the system where you want to install Network Manager, or install the appropriate packages to obtain the required libraries.

In addition to the libraries below, ensure that you have all required libraries for the appropriate versions of any integrated products. Specifically, check the requirements for your version of Jazz for Service Management in the Jazz for Service Management documentation at: <https://www.ibm.com/support/knowledgecenter/SSEKCU>, and for Cognos Analytics in the Cognos Analytics Knowledge Center at <https://www.ibm.com/support/knowledgecenter/SSEP7J>.

Table 4. Library requirements for Linux systems			
Library	Red Hat package	SuSE package	Required by component
libstdc++.so.6 (64-bit)	libstdc++-4.4.4-13+ libstdc++-4.8.2+	libstdc++46-4.6.1+	Network Manager Core
libpam.so.0 (64-bit)	pam-1.1.1	pam-64bit	Tivoli Netcool/OMNIBus

Supported browsers for Web applications

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

The minimum screen resolution for using the Web applications is 1536 x 864.

The following Web browsers are supported:

- **Fix Pack 7** Google Chrome
- Internet Explorer 10, 11
- Mozilla Firefox 38 Extended Support Release (ESR)
- **Fix Pack 1** Mozilla Firefox 45 Extended Support Release (ESR)
- **Fix Pack 4** Mozilla Firefox 52 Extended Support Release (ESR)

Operating system tools

Ensure that you have the correct versions of any required operating system tools available.

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).

On Linux, Network Manager requires Python 2 (not Python 3), version 2.6.6 or later, to be installed on the server where the core components are installed. On AIX, Network Manager requires Python 2 (not Python 3), version 2.7.5 or later.

Ensure that the bash shell is installed on the server where the Network Manager core components are to be installed.

UNIX user requirements

On UNIX operating systems, ensure that you meet all the requirements connected with required operating system users, and root and non-root installations.

User for poller aggregation

If you are installing Network Manager as a root user, you must create a non-root user before installing Network Manager to run the poller aggregation engine. This operating system user must have write permissions to the installation directory. If you install Network Manager as a non-root user, the installing user will be used to run the poller aggregation engine.

Root and non-root user restrictions

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.

Note: You must always use the same user to install, start, or stop all products that were installed by using IBM Installation Manager. You cannot use a different user, even if the products were installed in group mode. This user must be an administrative user for all products installed on that server.

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 UNIX, if you installed Network Manager as a non-root user, you must perform additional configuration.

Installation directory requirements

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

Requirements on all operating systems

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 the /opt, /var, and /tmp directories.

Related reference

[Default directory structure](#)

Use this information to understand the Network Manager directory structure.

File handle requirements

On UNIX and Linux operating systems, ensure that there are enough file handles 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`

Also, ensure that you have the number of processes per user set to a minimum of 16384. You can check this value by using the following command: `ulimit -u`. The 16384 value is a minimum one and this value might need to be adjusted for your environment based on your needs.

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

Note:

If you are using log file rotation with a set pool size, bear in mind that the number of open files can increase significantly. Enabling a logging pool adds an extra number of open files equivalent to the number of Network Manager processes running multiplied by the number of log files in the pool. Ensure that the limit on open files is high enough so that processes do not encounter problems opening log files.

Changing the values on Linux

Linux

To change the `ulimit`, modify the `/etc/security/limits.conf` file. As a system administrator (root user) you can add the following lines at the end of the `/etc/security/limits.conf` file:

*	soft	nproc	16384
*	hard	nproc	16384

*	soft	nofile	8192
*	hard	nofile	8192

Changing the values on AIX

AIX

The current values are listed in the `/etc/security/limits` file, in the lines that contain the parameters `nofiles` and `nproc`. As a system administrator (root user) you can use the `ulimit` command to change these values. For more information, search for information on the `ulimit` command at https://www-01.ibm.com/support/knowledgecenter/ssw_aix/welcome.

Password requirements

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

Network requirements

Ensure that your network meets the requirements before installing Network Manager.

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

List of ports used by the product

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

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

Table 5. Default ports used by Network Manager		
Port	Protocol	Description
22	SSH over TCP/IP	If SSH support is enabled, the Telnet Helper uses this port to communicate with network devices.
23	Telnet over TCP/IP	If SSH support is not enabled, the Telnet Helper uses this port to communicate with network devices.
161	SNMP	Port 161 is the default port on network devices to which SNMP queries are sent during the discovery and monitoring processes. Defined in the column <code>m_SnmpPort</code> in the database table <code>snmpStack.verSecurityTable</code> .
162	UDP	Default trap port. Used by the Trap polling agent. If more than one application/process needs access to this port, <code>ncp_trapmux</code> , the SNMP trap multiplexer, can be used to forward traps. The SNMP trap multiplexer, the Trap discovery agent, and the Trap polling agent can all be configured to use a different port.
1883	Message Queuing Telemetry Transport (MQTT)	Default port used by Really Small Message Broker for inter-process communication.
4100	TCP/IP	Default ObjectServer port. This must be entered at install time. Defined in <code>interfaces.Arch</code> on the ObjectServer workstation. This port is used by the <code>ncp_g_event</code> process to communicate with the ObjectServer.

Table 5. Default ports used by Network Manager (continued)		
Port	Protocol	Description
7968	TCP/IP	Default port for access to the Network Manager server from Dashboard Application Services Hub. This is used by the Discovery Configuration GUI and it is defined in the <code>ServiceData.cfg</code> configuration file. If you want to change this port, edit the <code>ServiceData.cfg</code> configuration file and restart the <code>ncp_model</code> process and the <code>ncp_config</code> process using CTRL.
16310	HTTP	Default port for the Dashboard Application Services Hub. The Dashboard Application Services Hub allocates the next thirteen ports up from the port specified for the Dashboard Application Services Hub during the installation for its own use. By default, this port redirects to 16316.
16311	HTTPS	Default secure port for the Dashboard Application Services Hub.
33000	TCP/IP	By default, the multicast IP address 225.13.13.13 and port 33000 are used to enable the discovery helpers and discovery agents to locate the Helper server. This multicast address is specified in the file <code>\$NCHOME/etc/precision/ServiceData.cfg</code> . Once a process has located the Helper server, a TCP connection is established on a port assigned by the operating system.
50000	TCP/IP	Default Db2 database port.
OS-assigned	TCP/IP	TCP ports are assigned by the operating system for TCP communication between processes, for example, the communication between discovery agents and the helper server. If this is an issue, you must ensure that your firewall is external to the Network Manager server, and that all discovery processes are run on the same host.
1521	TCP/IP	Default Oracle database port.

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.

On UNIX platforms, the host name is defined in the `/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 Dashboard Application Services Hub to fail.

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 Administration Guide*.

About DNCIM

The discovery engine, **ncp_disco**, uses an embedded relational database, known as Discovery NCIM (DNCIM).

During the discovery process, data is collected from the network, and the network topology is created using this data. During data collection and processing into a network topology, the network topology data is stored in different databases. Once the final network model, including connectivity and containment, is built the network topology data is stored in DNCIM. DNCIM has the same structure as the NCIM topology database.

For more information about DNCIM, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

FIPS 140-2 installations

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

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 way that has been designed with FIPS 140–2 specifications taken into consideration.

Restriction: If FIPS 140–2 compliance is important to you, you must install Network Manager with a restricted set of cryptographic algorithms by clearing the **Additional cryptographic routines** feature in the installer. If you install these additional routines, then your installation uses non-FIPS 140-2 compliant cryptographic routines.

If your requirements change, or you make an error during installation, you can install or uninstall the **Additional cryptographic routines** feature after installation by running the installer again and selecting **Modify**.

Integrating with other products

If FIPS 140–2 compliance is important to you, you must also ensure that all products that integrate with Network Manager, such as IBM Tivoli Netcool/OMNIbus, have a FIPS mode. You must also configure the products if necessary. You must also check that your operating system uses only FIPS 140–2 compliant modules.

Differences in a FIPS 140–2 installation of Network Manager

An installation with restricted cryptographic routines that is intended for use in a FIPS 140-2 compliant environment differs from a normal installation in the following ways:

- The Telnet discovery agents do not use SSHv1 to interrogate devices. This usage might result in a failure to connect securely to a device if the device supports only SSHv1, or if the device supports only non-FIPS 140-2 compliant SSHv2 algorithms.
- The SNMP Helper and the MIB browser cannot be configured to use MD5 or DES encryption. The SNMP Helper and the MIB browser support SHA and SHA1 algorithms for message digest, and 3-DES and AES 128 for encryption.

Chapter 3. Preparing to install

Before you begin installing Network Manager, you must complete additional tasks, depending on your environment.

Running installation and maintenance procedures as root or non-root

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.

Note: You must always use the same user to install, start, or stop all products that were installed by using IBM Installation Manager. You cannot use a different user, even if the products were installed in group mode. This user must be an administrative user for all products installed on that server.

Related concepts

[Root and non-root installation](#)

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 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.

Configuring Red Hat Linux Enterprise Edition

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

About this task

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

Procedure

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.

Preinstallation tasks for AIX

To install Network Manager on AIX operating systems, you must perform additional tasks to make your servers ready for installation.

About this task

These tasks are not necessary if you are using other operating systems.

Configuring Secure Shell (SSH) for AIX

If you are planning to install as a non-root user on AIX, and use SSH to access your AIX server, you must perform extra configuration steps before you access the AIX server.

About this task

Tip: If you use rlogin or telnet to access your AIX server, you do not need to perform the following steps.

To ensure that the installation will work, perform the following steps:

Procedure

1. Open the `/etc/ssh/sshd_config` file on the AIX server where you want to install Network Manager.
2. Ensure that the file contains the following line:

```
UseLogin yes
```

3. Save and close the file.
4. You can now use SSH to access the server and install Network Manager.

Installation of a zip utility

Installation of a zip utility for file compression is needed to export GUI customizations with the `nmGuiExport` script.

Before you export GUI customization data by using the `nmGuiExport` script, make sure that you install a zip utility on every server where GUI components of your previous system are installed. If a zip utility is not installed on the server of your previous system, then the `nmGuiExport` script fails, the `upgradeData.zip` archive is not created, and the script displays an error message.

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.

About this task

You must perform the following steps as the root user.

Procedure

1. Issue the following command

```
/usr/sbin/lssdev -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.

Chapter 4. Installing Network Manager and related products

Install the prerequisites, associated products, and components of Network Manager in the order that they are presented here.

Before you begin

Before you install any products, review all the prerequisites and requirements in [Chapter 2, “Planning for installation,”](#) on page 3 and complete any necessary pre-installation tasks in [Chapter 3, “Preparing to install,”](#) on page 39.

About this task

The instructions that follow are for installing one component at a time. To install two or more components in a certain order on the same server, select them to be installed at the same time, and IBM Installation Manager installs them in the correct order.

Checklist for installation

Before you start the installation, check that you have all the required information ready. During the installation, note down information that you need later.

Information to collect before installation

Collect all the information below that is relevant to your deployment before you start the installation. You can print out this checklist.

IBM Installation Manager information

☐ Installation location: _____ Where you plan to install IBM Installation Manager. For example, `/opt/IBM/netcool/im/`. You must start IBM Installation Manager from this location after it is installed.

☐ Data location: _____ The location where IBM Installation Manager unpacks packages and stores packages for rolling back. Ensure that this location has at least 10GB free space. This directory must not contain or be contained by the `eclipseIM` subfolder or the IBM Installation Manager share location. An example location for the data location is `/opt/IBM/netcool/IBMIMData`.

☐ Share location: _____ You are asked for this location when you install the first product into IBM Installation Manager, not during the installation of IBM Installation Manager itself. This directory must not contain or be contained by the `eclipseIM` subfolder or the IBM Installation Manager data location. An example location for the share location is `/opt/IBM/netcool/IBMIMShare`.

Db2 or Oracle information

Collect the following information for your choice of database before installing Network Manager.

☐ The directory where Db2 or Oracle is installed: _____

☐ If using Db2, the user name of an operating system and Db2 user to use to connect to the Db2 database: _____

- ☐ If using Oracle, ensure that you have entitlement to use the Partitioning feature.
- ☐ The Db2 database name or Oracle Service Name: _____
- ☐ The host name of the server where the database is installed: _____

ObjectServer information

If you want to use an existing ObjectServer for Network Manager event data, note its details here. You need these details when you install the Network Manager core components.

- ☐ Name of the ObjectServer: _____
- ☐ Host name where this ObjectServer is installed: _____
- ☐ Port configured for connections to this ObjectServer: _____
- ☐ Super user ID for this ObjectServer: _____
- ☐ Password for this user: _____

Network Manager core components information

Collect the following information for the core components before installing Network Manager.

- ☐ Python path: _____ The full path to a compatible version of Python is needed to install the Network Manager core components.
- ☐ Poller aggregation user: _____ If you are installing Network Manager as the root user, you need a non-root user to run the poller aggregation engine. This operating system user must exist and must have write permissions to the installation directory.
- ☐ Poller aggregation group: _____ The group to which the poller aggregation user belongs. The user poller aggregation must exist as a member of this group before poller aggregation can occur.

Information to collect during installation

During installation, you must define various configuration parameters. Some of these configuration parameters are needed later in the installation. Note down the following information as you install Network Manager and related components.

ObjectServer information

If you create an ObjectServer during the installation of the Network Manager core components, note its details here.

- ☐ Name of the ObjectServer created for use with Network Manager: _____
- ☐ Host name where this ObjectServer is installed: _____
- ☐ Port configured for connections to this ObjectServer: _____

☐ Super user ID for this ObjectServer: _____

☐ Password for this user: _____

Other Network Manager core components information

☐ The name of the user that runs the Network Manager installer: _____
This user must also run the upgrade scripts when you migrate to a new version.

☐ Password for the default Network Manager users `itnadmin` and `itnmuser`:

☐ Network domain name: _____ This is the name that you chose during installation of the Network Manager core components.

WebSphere Application Server information

Collect the following information as you install WebSphere Application Server:

☐ WebSphere Application Server install location: _____

☐ WebSphere Application Server server name: _____

☐ WebSphere Application Server user name: _____

☐ WebSphere Application Server password: _____

☐ HTTP transport port: _____

☐ HTTPS secure transport port: _____

☐ Administrative console port: _____

☐ Administrative console secure port: _____

☐ Context root: _____

Dashboard Application Services Hub information

Collect the following information as you install Dashboard Application Services Hub.

☐ Dashboard Application Services Hub install directory: _____

Network Manager GUI components information

Collect the following information as you install the Network Manager GUI components.

☐ Passwords for Network Manager users: _____ The password for the users `itnadmin` and `itnmuser`.

Installing and configuring IBM Installation Manager

Before you install or update Tivoli Netcool/OMNIBus, Network Manager, or any other IBM products, install or update IBM Installation Manager and configure it for use.

About this task

You have two options to obtain the IBM Installation Manager and Network Manager software.

- Download IBM Installation Manager to the target server and connect IBM Installation Manager to ibm.com® or a local repository. IBM Installation Manager can download other products.
- Download a compressed software package containing IBM Installation Manager and Network Manager and copy it to the target server.

Installing IBM Installation Manager by downloading the product files

If you want to install IBM Installation Manager and Network Manager on a server that is not connected to the internet, download the software to another server from Passport Advantage®. Then, copy it to the server where you want to install the software.

Before you begin

Create an IBM ID at <http://www.ibm.com>. You need an IBM ID to download software from Passport Advantage.

About this task

Network Manager requires IBM Installation Manager V1.9.1.4 or later. On SuSE Linux V11 and V12 for System z, only the 32-bit version of IBM Installation Manager is supported.

You can download a compressed file from Passport Advantage that contains IBM Installation Manager, Network Manager, and the database creation scripts.

To install and configure IBM Installation Manager, complete the following tasks:

Procedure

1. Locate the part number for the Network Manager part from the download document at the following location:
<http://www.ibm.com/support/docview.wss?uid=swg24043360>
2. Follow the instructions in the download document to download the software.
3. Decompress the package that you downloaded.
4. If you want to use the Network Manager database creation scripts without running IBM Installation Manager, you can copy them from the top level of the decompressed installation package.
5. Install IBM Installation Manager in group mode (all modes are supported, but for the most control of where files are created, use group mode rather than nonadministrator mode or admin mode) by using the instructions on "Installing or Updating Installation Manager" for the appropriate version in the information at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

Note: You must always use the same user to install, start, or stop all products that were installed by using IBM Installation Manager. You cannot use a different user, even if the products were installed in group mode. This user must be an administrative user for all products installed on that server.

After IBM Installation Manager finishes installing, it restarts and continues with the installation of Network Manager. Install Network Manager as described in ["Installing the Network Manager core components"](#) on page 55 and ["Installing the Network Manager GUI components"](#) on page 64.

What to do next

The next time that you use this installation of IBM Installation Manager, configure any repositories that you need.

1. Click **File** > **Preferences**.
2. If a repository is set up for you, click **Repositories** and ensure that the correct repositories are selected.
3. If no repositories were set up for you, and you want to set up a repository yourself, refer to the information about using the IBM Packaging Utility in the IBM Installation Manager documentation: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html
4. If you want to connect directly to the IBM online repository to access the products to which you are entitled, click Passport Advantage, select Connect to Passport Advantage, and click **Apply**. Click **OK**. When you install or update a product, you are prompted for your credentials to access IBM Passport Advantage.

Installing IBM Installation Manager by connecting directly to Passport Advantage

If you want to install IBM Installation Manager and Network Manager on a server that can connect to ibm.com, install IBM Installation Manager and connect it to Passport Advantage.

Before you begin

Create an IBM ID at <http://www.ibm.com>. You need an IBM ID to download software from Passport Advantage.

About this task

Network Manager requires IBM Installation Manager V1.9.1.4 or later. On SuSE Linux V11 and V12 for System z, only the 32-bit version of IBM Installation Manager is supported.

Note:

If there is any difference between these instructions and the documentation for your version of IBM Installation Manager due to updates or changes, the IBM Installation Manager documentation takes precedence, and can be found at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

To install and configure IBM Installation Manager, complete the following tasks:

Procedure

1. If you already have IBM Installation Manager installed, check that you have the latest version. The following commands assume that the server you are installing on is connected to the internet, that you are connected to the ibm.com repositories, and that you are using wizard mode. For any other scenarios, see the IBM Installation Manager documentation: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html
 - a) Start IBM Installation Manager by changing to the installation directory. By default, the installation directory for the three installation modes is:

Group mode

```
/user_home_directory/IBM/InstallationManager_Group/eclipse
```

Nonadministrator mode

```
/user_home_directory/IBM/InstallationManager/eclipse
```

Administrator mode

```
/opt/IBM/InstallationManager/eclipse
```

and run the following command:

```
./IBMIM
```

- b) Click **File > Preferences**.
 - c) If you can access ibm.com from this server, on the **Repositories** tab, select **Search service repositories during installation and updates**.
 - d) If you cannot access ibm.com from this server, on the **Repositories** tab, do not select **Search service repositories during installation and updates**. Without access to ibm.com, the update will time out. Instead, download the latest updates for IBM Installation Manager onto your local repository and ensure that the repository is configured under **Repositories**. If no repositories were set up for you, and you want to set up a repository yourself, refer to the information about using the IBM Packaging Utility in the IBM Installation Manager documentation: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html
 - e) Click **Updates** and select the **Search for Installation Manager updates** option.
 - f) Click **OK** to close the **Preferences** page.
 - g) Click one of these wizards: **Install** or **Update**.
Installation Manager searches for updates to itself. If a later version is found, you are prompted to update Installation Manager.
 - h) For version information, click **Details**.
 - i) Click **Yes** to update Installation Manager.
2. If you have not installed IBM Installation Manager, install it now.
 - a) Download the latest version of IBM Installation Manager for your platform from the following website: <https://www.ibm.com/support/pages/node/609575>
 - b) Install IBM Installation Manager in group mode (all modes are supported, but for the most control of where files are created, use group mode rather than nonadministrator mode or admin mode) using the instructions on "Installing or Updating Installation Manager" for the appropriate version in the information at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html
Note: You must always use the same user to install, start, or stop all products that were installed by using IBM Installation Manager. You cannot use a different user, even if the products were installed in group mode. This user must be an administrative user for all products installed on that server.
 3. Connect to a repository that contains the products that you want to install:
A repository can be on a local server or online.
 - a) Click **File > Preferences**.
 - b) If a repository has been set up for you, click **Repositories** and ensure that the correct repositories are selected.
 - c) If no repositories have been set up for you, and you want to set up a repository yourself, refer to the information about *managing packages with the IBM Packaging Utility* in the IBM Installation Manager documentation: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html
 - d) If you want to connect directly to the IBM online repository to access the products to which you are entitled, click Passport Advantage, select **Connect to Passport Advantage**, and click **Apply**. Click **OK**.
When you install or update a product, you are prompted for your credentials to access IBM Passport Advantage.

Installing and configuring a topology database

Your database administrator must install and configure a supported topology database before you can install Network Manager.

About this task

Network Manager requires a database to use to store the network topology.

Network Manager supports the following topology databases:

- IBM Db2 version 10.1 Enterprise Server Edition
- IBM Db2 version 10.5 Workgroup Server Edition
- IBM Db2 version 10.5 Enterprise Server Edition
- IBM Db2 version 11.1 Enterprise Server Edition
- IBM Db2 version 11.5 Enterprise Server Edition
- **Fix Pack 3** IBM Db2 version 11.1 Advance Enterprise Server Edition
- Oracle Database version 11g, Enterprise Edition with Partitioning option (Support added in Network Manager 4.2 Interim Fix 2)
- Oracle Database version 12c, Enterprise Edition with Partitioning option
- Oracle Database version 19c, Enterprise Edition with Partitioning option

Important: All of the database systems cited above include table partitioning capability. The Oracle database systems require the Partitioning option to be included. Table partitioning is required for Network Manager to function properly.

Important: Ensure that your database has all the recommended patches applied, including the latest patch levels.

To install and configure a database, complete the following steps:

Procedure

1. Install one of the supported databases:
 - Install Db2 from Passport Advantage: http://www.ibm.com/software/howtobuy/passportadvantage/pao_customers.htm.
 - Install Oracle from your software provider.
2. Install the Network Manager topology database creation scripts using IBM Installation Manager.
3. Configure the database using the information in the following sections.

Related tasks

[Configuring Cognos Analytics](#)

Perform these tasks to configure Cognos Analytics.

Related reference

[Supported topology databases](#)

The default topology database for Network Manager is IBM Db2 10.5 Enterprise Server Edition.

Installing and running the Network Manager database scripts

After a supported database has been installed, you must install and run the database scripts to configure the topology database for use by Network Manager. You must run the scripts before installing Network Manager.

About this task

If you downloaded the compressed software package from Passport Advantage, as described in “Installing IBM Installation Manager by downloading the product files” on page 44, the database creation scripts are included at the top level of the uncompressed software file. Copy the scripts to the database server and use them.

Otherwise, install the Network Manager topology database creation scripts by completing the following tasks.

Procedure

1. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

2. Click **Install**.
3. On the **Install Packages** screen where you can select packages to install, select the latest available version of the **Network Manager topology database creation scripts**.
4. Click **Next**, agree to the terms in the license agreement, and click **Next** again.
5. Select the **IBM Netcool Core Server** package group and click **Next**.
6. On the **Install Packages** screen where you can select features to install, select the appropriate scripts for your database type.
7. Click **Next** and **Install**.

Results

The appropriate database scripts are now installed by default in the `precision/scripts/` directory in the installation directory (by default, `/opt/IBM/netcool/core/precision/scripts/`). For convenience, a compressed file containing the same database scripts is also created in the installation directory. If you installed the scripts on a different server to the database server, copy the compressed file to the database server and uncompress it to use the database scripts. Use the information in the following sections to configure the topology database using the scripts.

Setting up existing Db2 databases on UNIX

To use an existing Db2 database as the topology database on UNIX, you must have a Db2 instance available before installing Network Manager.

Before you begin

The database for Network Manager is created by scripts that are installed in the `precision/scripts/` directory in the installation directory (by default, `/opt/IBM/netcool/core/precision/scripts/`). You must have installed the scripts before you attempt to create the database. For more information about installing the database scripts on the database server, see *Installing and running the Network Manager database scripts* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

About this task

During installation of Network Manager, the NCIM topology database is installed on the Db2 database that you create.

For information on installing and configuring Db2, refer to the Db2 documentation at <http://www.ibm.com/support/knowledgecenter/SSEPGG/welcome>

Procedure

1. Ensure you have a Db2 instance in which the installation process can create the NCIM database. Multiple Network Manager domains can share the same instance
2. Change to the directory into which the instance was installed and then change to the `sqllib` subdirectory.
3. Set up the environment by typing the following command:

Shell	Command
Bourne	<code>. ./db2profile</code>
C	<code>source db2cshrc</code>

The Network Manager application wrapper scripts automatically set up the Db2 environment.

4. Change to the `precision/scripts/` directory in the installation directory (by default, `/opt/IBM/netcool/core/precision/scripts/`).
5. As the administrative user, for example the `db2inst1` user, run the `create_db2_database.sh` script as the Db2 administrative user by typing the following command on the Db2 server:
`./create_db2_database.sh database_name user_name -force`

Where:

database_name

Is the name of the database.

user_name

Is the Db2 user to use 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 argument that forces any Db2 users off the instance before the database is created.

For example, to create a Db2 database that is called ITNM for the Db2 user `ncim`, type:

```
./create_db2_database.sh ITNM ncim
```

After you run `create_db2_database.sh`, restart the database as the Db2 administrative user as follows: run **db2stop** and then run **db2start**.

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.

The installer populates the connection properties in the following files, you can check these files for any problems with your connection to the database. For more information about editing the following files, refer to *Configuring Network Manager for a changed IP address of the Db2 NCIM server* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

- The `DbLogins.DOMAIN.cfg` and `MibDbLogin.cfg` files in `NCHOME/etc/precision`. These files are used by the Network Manager core processes.
- The `tnm.properties` file in `$NMGUI_HOME/profile/etc/tnm`. These files are used by the Network Manager GUI.

Related concepts

[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.

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.

Before you begin

The database for Network Manager is created by scripts that are installed in the `precision/scripts/` directory in the installation directory (by default, `/opt/IBM/netcool/core/precision/scripts/`). You must install the scripts before you attempt to create the database.

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

About this task

Before you install Oracle, ensure that you have entitlement to use the Partitioning feature. This extra feature is required for Network Manager to function properly.

For information on installing and configuring Oracle, refer to the Oracle documentation at <http://docs.oracle.com/en/database/>.

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 that is created by this script is also `ncim`.

Procedure

1. Install Oracle, including the Partitioning feature, and configure a schema on which the installation process can create the NCIM database.
2. Make sure that 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 database administrator, change to the `precision/scripts/` directory in the installation directory (by default, `/opt/IBM/netcool/core/precision/scripts/`).

6. If you installed Oracle on a different server to Network Manager, copy the `oracle_creation_scripts.tar.gz` file to that server and extract all the files.
7. Run the `create_oracle_ncadmin_user.sh` script on the server where the database is installed. Log in to the Oracle host as the Oracle database administrator, run the `create_oracle_ncadmin_user.sh` script by supplying the sys user and password. Run the script as in the following example.

```
$NCHOME/precision/scripts/sql/oracle/create_oracle_ncadmin_user.sh
sys
password [-pdb pluggable_database_name]
```

Where the following parameters apply:

password

Specifies the password of the sys user.

-pdb pluggable_database_name

Optional: if you are running Oracle 12c with RAC, you must use a pluggable database. In this case, use this parameter to specify the Oracle 12c pluggable database name.

8. To create the database, run the `./create_oracle_database.sh` script. As the Oracle database administrator, run the `./create_oracle_database.sh` script by supplying the system user and password. On the Network Manager server, the script is in the `$ITNMHOME/scripts/sql/oracle` directory. Run the script on the server where the database is installed. Run the script as in the following example.

```
./create_oracle_database.sh system password [-asm]
[-pdb pluggable_database_name]
```

Where the following parameters apply:

password

Specifies the password of the system user.

-asm

Specify `-asm` if your Oracle DB uses ASM.

-pdb pluggable_database_name

Optional: if you are running Oracle 12c with RAC, you must use a pluggable database. In this case, use this parameter to specify the Oracle 12c pluggable database name.

9. When you run the Network Manager installer later on, 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.

The installer populates the connection properties in the following files, you can check these files for any problems with your connection to the database. For more information about editing the following files, refer to *Configuring Network Manager for a changed IP address of the Db2 NCIM server* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

- The `DbLogins.DOMAIN.cfg` and `MibDbLogin.cfg` files in `NCHOME/etc/precision`. These files are used by the Network Manager core processes.
- The `tnm.properties` file in `$NMGUI_HOME/profile/etc/tnm`. These files are used by the Network Manager GUI.

Note: If you are installing Network Manager in an Oracle high availability environment that uses Real Application Clusters (RAC), install Network Manager first with a direct connection to a single node in the Oracle cluster. After you install Network Manager successfully, you can set up high availability for Network Manager with an Oracle Single Client Access Name (SCAN) address as described in *Configuring Network Manager to work with Db2 HADR or Oracle RAC* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

10. Optional: After you install Network Manager, run the `$NCHOME/precision/scripts/sql/oracle/restrict_oracle_privileges.sh` script as a user with system privileges. Now that all databases and schemas have been created, this script can be used to revoke database creation

privileges from the NCIM database user. Only those operations that are required for Network Manager during run time will remain granted.

11. Optional: To enable Oracle Network Encryption, set encryption to REQUIRED on the database server. You do not need to configure Network Manager for Oracle Network Encryption. Refer to your Oracle documentation for details of how to enable Oracle Network Encryption.

Setting up NCIM to use multibyte characters

You must configure the NCIM database to use 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.

About this task

Ensure that you have the following settings for the NCIM database:

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`

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.

About this task

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

Procedure

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.
 - Go to the \$NCHOME directory and issue the following command: `source env.sh`.

Installing and configuring Tivoli Netcool/OMNIBus

You must install Tivoli Netcool/OMNIBus before installing Network Manager.

About this task

Network Manager requires Tivoli Netcool/OMNIBus. It supports the following versions of Tivoli Netcool/OMNIBus:

- V7.4
- V8.1 Fix Pack 24 or later

If you have not already installed Tivoli Netcool/OMNIBus, and you plan to install it on the same server as Network Manager, you do not need to do anything now.

When you install Network Manager, install Tivoli Netcool/OMNIBus at the same time by selecting the Tivoli Netcool/OMNIBus and Network Manager core components from the package **IBM Netcool Core Components**.

The Network Manager core component installer configures Tivoli Netcool/OMNIBus for you during the installation.

If you have not already installed Tivoli Netcool/OMNIBus and you plan to install it on a different server to Network Manager, install Tivoli Netcool/OMNIBus **before** Network Manager.

See the information about installing your version of Tivoli Netcool/OMNIBus at: <http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html>.

Then install the Netcool/OMNIBus Knowledge Library and the Probe for SNMP. See the information on installing the Netcool/OMNIBus Knowledge Library at http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/probes/nckl/wip/concept/nckl_intro.html and the information on installing the Probe for SNMP at http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/probes/snmp/wip/concept/snmp_introduction_c.html.

If you have already installed Tivoli Netcool/OMNIBus, the Netcool/OMNIBus Knowledge Library, and the Probe for SNMP, you can now install Network Manager.

The Network Manager installer configures Tivoli Netcool/OMNIBus for you during the installation process.

If you have already installed and configured Network Manager and Tivoli Netcool/OMNIBus but somebody changed the ObjectServer after the installation, then you must reintegrate the ObjectServer with Network Manager. To re-integrate the ObjectServer, you must be knowledgeable in the following areas.

- Network Manager core. If the ObjectServer name, port, or host name changes then manual changes must be made to Network Manager core.
- Integration with the Web GUI data source. For more information about integration with the Web GUI data source, see [“Configuring the Tivoli Netcool/OMNIBus Web GUI data source name”](#) on page 86.
- `config_object_server_for_itnm.sh` script. Support for this script was added in Network Manager 4.2 Interim Fix 2; if you have Interim Fix 2 then this script supersedes the **ConfigOMNI** script. It provides the ability to configure an existing Windows or UNIX ObjectServer to run with Network Manager. The script is run on the Network Manager core server and may be used to configure an ObjectServer on either the local server or on a remote server.
- **ConfigOMNI** script. Use the **ConfigOMNI** script to create and configure an ObjectServer to run with Network Manager. The script creates the Network Manager triggers. If the ObjectServer is on a remote server, then copy the `$NCHOME/precision/install/scripts/ConfigOMNI` script and the support script `$NCHOME/precision/scripts/create_itnm_triggers.sql` and put them into the same directory on the remote ObjectServer. If the ObjectServer is local to Network Manager, then you can use both scripts as is.

Related tasks

[Configuring an ObjectServer for use with Network Manager core processes](#)

For users with Network Manager 4.2 Interim Fix 2 only, you can use the `config_object_server_for_itnm.sh` script to configure an ObjectServer for use with Network Manager core processes. This script supports an ObjectServer running on Windows as well as UNIX. The script configures the connection to the ObjectServer and may be used to configure either a local or remote ObjectServer. It also runs a number of SQL commands that create and configure in the ObjectServer the tables and users required by Network Manager.

ConfigOMNI command-line options

Use the `$NCHOME/precision/install/scripts/ConfigOMNI` script, with optional advanced arguments, to configure Tivoli Netcool/OMNIBus for use with 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 ] [ -n portnumber ] [ -u password ] [ -z PA authentication ]
```

The following example runs the script on ObjectServer DIAMOND with the administrative password p3w0d. If the ObjectServer DIAMOND does not exist, it is created. Using the appropriate options, you can configure the script to add the `itnadmin` and `itnmuser` users to the ObjectServer, turn on AES encryption, and turn on process control for the Objectserver.

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.ibm.com/support/knowledgecenter/SSSTQ/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 6. ConfigOMNI command-line options	
Command-line options	Description
<code>-o name</code>	The name of the ObjectServer that you want to create or configure.
<code>-p password</code>	The administrative password of the ObjectServer that you want to create or configure.
<code>-a</code>	Optional. Runs the script in interactive mode, which prompts for all information.
<code>-c</code>	Optional. Configures the ObjectServer to run under Tivoli Netcool/OMNIBus process control.
<code>-e</code>	Optional. Set AES encryption for the ObjectServer password.
<code>-h directory</code>	Optional. The directory that contains the Tivoli Netcool/OMNIBus installation (OMNIHOME).
<code>-n portnumber</code>	Optional. The port number of the ObjectServer that you want to create or configure.
<code>-u password</code>	Optional. Create the <code>itnadmin</code> and <code>itnmuser</code> users in the ObjectServer.

Table 6. ConfigOMNI command-line options (continued)

Command-line options	Description
-z PA authentication	Optional. Provides authentication for the Tivoli Netcool/OMNIBus Process Agent NCO_PA, for when the NCO_PA starts up. If you don't enter a value, then the value defaults to PAM.

Installing the Network Manager core components

You must install the Network Manager core components before, or at the same time as, installing the GUI components.

Before you begin

Before you install the Network Manager core components, you must install and configure a topology database, installed IBM Installation Manager, and installed and started Tivoli Netcool/OMNIBus.

Ensure that a compatible version of Python is installed on this server before you start. On Linux, Network Manager requires Python 2 (not Python 3), version 2.6.6 or later, to be installed on the server where the core components are installed. On AIX, Network Manager requires Python 2 (not Python 3), version 2.7.5 or later.

About this task

Fix Pack 11

Important: If you want to use WebSphere Application Server version 9, you must have new installation of WebSphere Application Server version 9 and Network Manager Fix Pack 11. This is because of the upgrade path is not available for WebSphere Application Server from version 8 to version 9.

Fix Pack 6

Important: Installing Fix Pack 6 or later removes existing MIB files. Network Manager These Fix Packs do not contain the Management Information Base (MIB files). Network Manager Fix Pack 5 does contain the MIB files. The MIBs are required for network discovery.

If you are upgrading from Fix Pack 5 or earlier, complete the following steps to obtain the MIB files:

1. Locate a zip file named `com.ibm.tivoli.netcool.ncp.mibs.all.any_*.zip` within the IBM Installation Manager shared location that contains the MIB files from the previous Fix Pack installation. The exact path might be different in your installation. An example path is: `/opt/IBM/IBIM/native/`
2. Unzip this file.
3. Load the MIBs into the database by running the `ncp_mib` command, as described in *Loading updated MIB information* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

If you are installing Fix Pack 6, 7, 8, or 9 without upgrading, or you are unable to locate the MIB files using the above procedure, complete the following steps to obtain the MIB files:

1. Run the `ncp_mib` command, as described in: *Loading updated MIB information* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.
2. If you have Network Manager 4.2 Fix Pack 5 installed, back up the contents of the `$NCHOME/precision/mibs/` directory to a backup directory outside `$NCHOME`. For example, `/mibs_backup/`.
3. If you have an earlier version than 4.2 Fix Pack 5 installed, complete the following steps:
 - a. Back up the contents of the `$NCHOME/precision/mibs/` directory to a backup directory outside `$NCHOME`. For example, `/old_mibs/`. Keep this directory and its files in case you want to roll back to this version later.

- b. Download the Network Manager Fix Pack 5 (4.2.0.5) files from IBM Fix Central: <https://www.ibm.com/support/fixcentral/>

Important: Download the files for Linux x86, regardless of which platform you are using.

- c. Expand the Network Manager package into a temporary directory.
 - d. Expand the `repositories/disk1/ad/native/file000876` archive file into a backup directory outside `$NCHOME`, for example, `/mibs_backup/`. This directory now contains the default MIB files.
 - e. If you customized or added any MIB files, copy the customized or new MIB files from `/old_mibs/` over the default files in `/mibs_backup/`.
4. Regardless of the version of Network Manager you installed, the `/mibs_backup/` directory now contains the most current set of MIB files from Fix Pack 5, plus any additions and customizations.

After you obtain the MIB files, install the most recent version of Network Manager.

1. Install Network Manager Fix Pack 6 or later using the instructions in this procedure.
2. Copy the MIB files from your `/mibs_backup/` directory to the following location within the installation: `$NCHOME/precision/mibs/`
3. Run the **nbp_mib** command, as described in: *Loading updated MIB information* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

To uninstall Fix Pack 6 or later and use a previous version, complete the following steps:

1. Copy the MIB files from the following directory to a temporary directory: `$NCHOME/precision/mibs/`
2. Delete all the files in the `$NCHOME/precision/mibs` directory.
3. Uninstall Network Manager Fix Pack 6 or later using the instructions in: *Uninstalling fix packs* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.
4. If you are rolling back to 4.2 Fix Pack 5, copy the MIB files back from the temporary directory to the MIB directory: `$NCHOME/precision/mibs/`
5. If you are rolling back to a version prior to 4.2 Fix Pack 5, copy the MIB files back from the backup directory `/old_mibs/` to the MIB directory: `$NCHOME/precision/mibs/`
6. Run the **nbp_mib** command, as described in: *Loading updated MIB information* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*

To install the Network Manager core components, complete the following tasks.

Procedure

1. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

2. Click **Install**.
3. On the next **Install Packages** screen where you can select packages to install, select the latest available version of the **Network Manager Core Components**.
The prerequisites for installing the package are evaluated.
4. If any issues with prerequisites are displayed, resolve them using the information that is provided before you continue.

5. Click **Next**, agree to the terms in the license agreement, and click **Next** again.
6. Select the **IBM Netcool Core Components** package group and click **Next**.

Restriction: If you are installing Network Manager on the same server as Tivoli Netcool/OMNIBus, you must install the core components in the same package group as Tivoli Netcool/OMNIBus.

7. Select the **Core components** to be installed.
8. Select **Additional cryptographic routines** if you want to use all the cryptographic options that Network Manager provides. Clear this option if FIPS 140-2 compliance is important to you, because some of the components are not compliant with this standard. For more information, see [“FIPS 140-2 installations”](#) on page 36.
9. On the next **Install Packages** screens, provide configuration information for the packages that are being installed. Use **Next** and **Back** to go through the configuration options.
10. Optional: If you are installing Network Manager at the same time as Tivoli Netcool/OMNIBus, or in the same package group as an installation of Tivoli Netcool/OMNIBus that was not configured for use with Network Manager, a new aggregate ObjectServer is created. Configure the new ObjectServer:

Name

Accept the default name of NCO_AGG_P, or enter a new name for the ObjectServer. If this ObjectServer is intended for use in an architecture with multiple ObjectServers, keep the _AGG_P suffix to the name. By convention, ObjectServer names are in uppercase. You need this name later to start and stop the ObjectServer. Make a note of the name in the [“Checklist for installation”](#) on page 41.

Host

Enter the host name of the server where Tivoli Netcool/OMNIBus is installed.

Port

Enter a port to use for connection to the ObjectServer or accept the default.

Super user ID

The installation uses the root Tivoli Netcool/OMNIBus user.

Password

Enter the password for the root user.

Confirm password

Enter the password again.

11. Optional: If you are installing Network Manager on a different server to Tivoli Netcool/OMNIBus, Network Manager connects to an existing ObjectServer. The ObjectServer must be running and accessible from this server. Specify the details of the ObjectServer for Network Manager to connect to.

Name

Enter the name of the ObjectServer.

Host

Enter the host name of the server where Tivoli Netcool/OMNIBus is installed.

Port

Enter a port to use for connection to the ObjectServer or accept the default.

Super user ID

Enter the user name of a user with administrative permissions for Tivoli Netcool/OMNIBus.

Password

Enter the password for this user.

The connections details are checked against the running ObjectServer. Select **Skip ObjectServer connection details verification and configuration** if you are currently unable to verify the details, for example, if the ObjectServer is not accessible. If you skip this process, you must the changes later manually.

12. Configure the Network Manager default users. The users `itnmadmin` and `itnmuser` are created by the installer in the ObjectServer. The same password is used for both users.

Password

Specify a password for these users. Record the password.

Confirm password

Confirm the password.

13. Enter a name for the network domain. This name is visible to network operators and product administrators. You can also add, remove, and change domains later. Record the name that you choose. You need this name to start Network Manager components.
14. Enter the details for the topology database that is installed. Make a note of these details. You need the same details when you install the GUI components.

a) Select the database type.

b) Enter the database connection details:

If you selected Db2 as the database type, enter the following details:

Database name

Enter the name of the database.

Server host

Enter the host name of the server where the database is installed.

Server port

Enter the port number for connecting to the database.

User ID

Enter the ID of an existing Db2 user that has permissions to create tables.

Password

Enter the password for this user.

If you selected Oracle as the database type, enter the following details:

Oracle Service Name

Enter the Service Name for the database.

Server host

Enter the host name of the server on which the database is installed.

User ID

Enter the ID of an existing Oracle user that has permissions to access NCIM tables. The default user ID is ncim.

Password

Enter the password for this user.

- c) Select **Create tables to hold topology data in created database** to create the database tables that are needed by Network Manager. If you already created the database tables by using the database creation scripts, you do not need to select this option. If you already created the tables and you select the option to create them again, you receive an error at the end of the installation. This error indicates that the tables were not created.
 - d) Select **Skip database connection details verification** if you do not want to verify the connection, if the database is inaccessible or for other reasons.
15. Configure the details for the poller aggregation:

Python path

Enter the full path to a compatible version of Python.

Poller aggregation user

If you are installing as a root user, you must enter the user name of a non-root user here. This user is needed to run the poller aggregation engine. If you are installing as a non-root user, the installing user is used to run the poller aggregation engine and you do not see this option in the installer. This user must be created before poller aggregation can occur.

Poller aggregation group

Enter the group to which the poller aggregation user belongs. If the user belongs to a different group than the installing user, the installer changes default permissions on files and folders so that poller aggregation functions. The user must exist as a member of this group before poller aggregation can occur.

16. Review the summary information and click **Install**.

Results

The Network Manager core components are installed. Any errors are written to the installation log file, which you can view by clicking **View Log File**. Log files are kept in the /logs/ directory in the IBM Installation Manager data location.

Related tasks

Enabling historical polling

If you installed Network Manager as the root user, then you must run the `setup_run_storm_as_non_root.sh` script to enable the historical polling data processes to run. You do not need to run this script if you installed Network Manager as a non-root user.

Installing WebSphere Application Server

You must install the required WebSphere Application Server components before installing Jazz for Service Management.

Before you begin

You must install WebSphere Application Server on the server where you want to install the Network Manager GUI components.

About this task

Note:

If there is any difference between these instructions and the documentation for your version of WebSphere Application Server due to updates or changes, the WebSphere Application Server documentation takes precedence, and can be found at: https://www.ibm.com/support/knowledgecenter/SSEQTP/mapfiles/product_welcome_was.html

Procedure

1. On the server where you want to install the Network Manager GUI components, ensure that IBM Installation Manager is installed.
2. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

3. Click **Install**.
4. On the next **Install Packages** screen where you can select packages to install, select the following components and click **Next**:
 - IBM Websphere Application Server. Network Manager requires IBM Websphere Application Server Version 8.5.5.18 (version 8) or 9.0.5.6 (version 9).

Note: If you want to use WebSphere Application Server version 9, you must have new installation of WebSphere Application Server version 9, Network Manager Fix Pack 11 and Tivoli Netcool/OMNIBus Web GUI Version 8.1.0.20 or later. This is because the upgrade path is not available for WebSphere Application Server from version 8 to version 9.

- IBM Websphere SDK Java Technology Edition. For Network Manager Fix Pack 9 and earlier versions, this component must be installed separately, and version 8 is required. For Network Manager Fix Pack 10 and later versions, this component is installed with WebSphere Application Server and does not need to be selected here.
- Jazz® for Service Management extension for IBM Websphere. Use the version that corresponds to your version of IBM Websphere Application Server.

The prerequisites for installing the package are evaluated.

5. If any issues with prerequisites are displayed, resolve them using the information provided before continuing.
6. Click **Next**, agree to the terms in the license agreement, and click **Next** again.
7. Select the **IBM Websphere Application Server** package group.
8. Enter an installation directory for the package group, for example, a /was/ directory underneath the installation directory for IBM products, and click **Next**.
9. Select all the features of IBM Websphere Application server to be installed except **Sample applications**.
10. Select the 64-bit version of IBM Websphere SDK Java Technology Edition.
11. Select the JazzSM Websphere Extension to be installed and click **Next**.
12. After the components are installed, you are asked which programs you want to start. Select **None**.

Installing Dashboard Application Services Hub

You must install Dashboard Application Services Hub before installing the Network Manager GUI components.

About this task

Dashboard Application Services Hub is a component of Jazz for Service Management.

Before you install any components of Jazz for Service Management, you must run IBM Prerequisite Scanner and check for the prerequisites of all Jazz for Service Management components that you want to install. See [“Checking system prerequisites” on page 20](#) for more information.

Note:

If there is any difference between these instructions and the documentation for your version of Jazz for Service Management components due to updates or changes, the Jazz for Service Management documentation takes precedence, and can be found at: <https://www.ibm.com/support/knowledgecenter/SSEKCU>

Procedure

1. On the server where you want to install the Network Manager GUI components, ensure that IBM Installation Manager is installed.
2. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the

IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

3. Click **Install**.
4. On the next **Install Packages** screen where you can select packages to install, select **IBM Dashboard Application Services Hub** and click **Next**. Network Manager requires Dashboard Application Services Hub Version 3.1.3.9 or later.
The prerequisites for installing the package are evaluated.
5. If any issues with prerequisites are displayed, resolve them using the information provided before continuing.
6. Click **Next**, agree to the terms in the license agreement, and click **Next** again.
7. Select the **Core services in Jazz for Service Management** package group.
8. Enter an installation directory for the package group, for example, a `/jazz/` directory underneath the installation directory for IBM products, and click **Next**.
9. Select the 64-bit version of IBM Dashboard Application Services Hub.
10. Select all the features of IBM Dashboard Application Services Hub to be installed.
11. On the next **Install Packages** screens, provide configuration information for the packages being installed. Use **Next** and **Back** to navigate through the configuration options.
12. Optional: Configure details for WebSphere Application Server.

If this is the first component to be installed into WebSphere Application Server on this server, you must configure all the details. If another component was already installed into WebSphere Application Server, the existing details are used. Details that were configured previously are shown grayed out, and you must reconfirm only the username and password.

Websphere installation location

Enter the location where WebSphere Application Server was installed.

Profile deployment type

Select **Create Websphere profile**. A profile is a way of grouping applications together in WebSphere Application Server. If you have a large WebSphere Application Server deployment, consult your administrator to find out which profile to use.

Profile location

Leave the default location or enter a new location for the profile. The following characters cannot be used in the WebSphere Application Server profile path.

```
` ! # $ % ^ & * + = { } [ ] | ; " < > , ? @ ~ .
```

Profile name

Enter a unique, descriptive name for the profile.

Node name

Enter a unique, descriptive name for the node.

Server name

Enter a unique, descriptive name for the logical server that is created in WebSphere Application Server and associated with this profile. Make a note of this information; you will need it when you install other applications into WebSphere Application Server.

User name

Leave the default `smadmin` username. This user will be created within WebSphere Application Server. Make a note of this information; you will need it when you install other applications into WebSphere Application Server

Password

Enter a password for this user. Make a note of this information; you will need it when you install other applications into WebSphere Application Server

Confirm password

Confirm the password.

13. Optional: Configure the ports for WebSphere Application Server.

If this is the first component to be installed into WebSphere Application Server, you must configure the ports. If another component was already installed into WebSphere Application Server, this panel is not shown. Leave the port values at the defaults unless there is a conflict with other applications.

HTTP transport port

The port used to access WebSphere Application Server.

Important: Make a note of this value. You will need this to access any applications installed into WebSphere Application Server.

HTTPS secure transport port

The port used to access WebSphere Application Server using HTTPS.

Important: Make a note of this value. You will need this to access any applications installed into WebSphere Application Server if you use HTTPS.

Bootstrap port

A port used for applications running outside the application server to connect to the message bus.

SOAP connector port

A port used for making Java Management Extensions (JMX) connections with the server using Simple Object Access Protocol (SOAP).

IPC connector port

A port used for making Java Management Extensions (JMX) connections with the server using Inter-Process Communications (IPC).

Administrative console port

Port to access the administrative console of WebSphere Application Server.

Important: Make a note of this value. You will need this to access the WebSphere Application Server administrative console.

Administrative console secure port

Port to access the administrative console of WebSphere Application Server using HTTPS.

High availability manager communication port

Port used to access the high availability manager.

ORB listener port

A port used by the Object Request Broker.

SAS SSL server authentication port

Secure Authentication Service authentication port.

CSIV2 client authentication listener port

Listener port for the Common Secure Interoperability Specification, Version 2 (CSIV2) client.

CSIV2 server authentication listener port

Listener port for the Common Secure Interoperability Specification, Version 2 (CSIV2) server.

REST notification port

The Representational State Transfer (REST) notification port that is associated with the applications installed in the Jazz for Service Management WebSphere® profile.

For more information on specific ports, refer to the documentation for your version of WebSphere Application Server at: https://www.ibm.com/support/knowledgecenter/SSEQTP/mapfiles/product_welcome_was.html

14. Enter a value for the context root for Dashboard Application Services Hub in the **Context Root** field.

Dashboard Application Services Hub is an application that is hosted in WebSphere Application Server.

The context root for Dashboard Application Services Hub defines the directory within the WebSphere Application Server context in which Dashboard Application Services Hub runs.

For example, if the root URL for WebSphere Application Server is `http://hostname:16310`, and you set a context root of `/ibm/console/` for Dashboard Application Services Hub, then the URL to access Dashboard Application Services Hub is `http://hostname:16310/ibm/console/`. The URL to access any applications hosted in Dashboard Application Services Hub, would be `http://hostname:16310/ibm/console/application_name`.

15. Click **Validate** to validate the configuration values, and then click **Next**.
16. Review the summary information and click **Install**.
17. After the components are installed, you are asked which programs you want to start. Select **None**.

Installing Tivoli Netcool/OMNIBus Web GUI

You must install Web GUI before installing the Network Manager GUI components.

Before you begin

Before you install Tivoli Netcool/OMNIBus Web GUI, you must install WebSphere Application Server and Jazz for Service Management.

About this task

You must install Web GUI on the server where you want to install the Network Manager GUI components.

If there is any difference between these instructions and the documentation for your version of Tivoli Netcool/OMNIBus Web GUI components due to updates or changes, the Tivoli Netcool/OMNIBus Web GUI documentation takes precedence, and can be found at: <http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html>.

Procedure

1. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

2. Click **Install**.
3. On the next **Install Packages** screen where you can select packages to install, select **IBM Tivoli Netcool/OMNIBus Web GUI** and click **Next**.

The prerequisites for installing the package are evaluated.
4. If any issues with prerequisites are displayed, resolve them using the information provided before continuing.
5. Click **Next**, agree to the terms in the license agreement, and click **Next** again.
6. Select the **IBM Netcool** package group.
7. Enter an installation directory for the package group, for example, a `/gui/` directory underneath the installation directory for IBM products, and click **Next**.
8. Select **Install base features**, any other features that are necessary for the product integrations you have.
9. On the next **Install Packages** screens, provide configuration information for the packages being installed. Use **Next** and **Back** to navigate through the configuration options.
10. Configure properties for WebSphere Application Server and Jazz for Service Management.

WebSphere Application Server installation directory

Enter the directory where WebSphere Application Server is installed.

Jazz for Service Management UI

Enter the directory where Dashboard Application Services Hub is installed.

Server name

Enter the name of the logical server that was created in WebSphere Application Server.

User name

Enter the user name that is configured to access this logical server.

Password

Enter the password for this user.

11. Review the summary information and click **Install**.

Installing the Network Manager GUI components

Install the Network Manager GUI components only after installing the core components. Install the GUI components on the server that has Jazz for Service Management already installed.

About this task

To install the Network Manager GUI components, complete the following tasks:

Procedure

1. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

2. Click **Install**.
3. On the next **Install Packages** screen where you can select packages to install, select the latest available version of the **Network Manager GUI Components**.

The prerequisites for installing the package are evaluated.
4. If any issues with prerequisites are displayed, resolve them using the information provided before continuing.
5. Click **Next**, agree to the terms in the license agreement, and click **Next** again.
6. Select the **IBM Netcool GUI Server** package group and click **Next**.
7. Select **Product Files** to be installed and click **Next**.
8. On the next **Install Packages** screens, provide configuration information for the packages being installed. Use **Next** and **Back** to navigate through the configuration options.
9. Confirm the properties of the Jazz for Service Management instance that you want to install into.

Installation directory details

The full path to the Dashboard Application Services Hub instance.

User name

Enter the user name for a user with administrative permissions in Dashboard Application Services Hub. If it has not been changed, you can use the default user `smadmin` with password `netcool`.

10. Network Manager connects to an existing ObjectServer. The ObjectServer must already exist and be running and accessible from this server. Specify the details of the ObjectServer for Network Manager to connect to. These details must match the details entered when installing the core components.

Name

Enter the name of the ObjectServer.

Host

Enter the host name of the server where Tivoli Netcool/OMNIBus is installed.

Port

Enter a port to use for connection to the ObjectServer or accept the default.

Super user ID

Enter the user name of a user with administrative permissions for Tivoli Netcool/OMNIBus.

Password

Enter the password for this user.

Select **Skip ObjectServer connection details verification and configuration** if any of the following conditions apply:

- Tivoli Netcool/OMNIBus WebGUI is already configured with a data source and an authentication source. If you configure different details, the installation overwrites the existing configuration.
- You are unable to verify the details at this time, for example, if the ObjectServer is not accessible. If you skip this process, you must make the changes later manually.

Jazz for Service Management is configured to use this ObjectServer for authentication.

11. Configure the Network Manager default users. The users `itnmadmin` and `itnmuser` are created by the installer in the ObjectServer. The same password is used for all users. If one or more of these users already exist, the password is not changed.

Password

Specify a password for these users. Record the password.

Confirm password

Confirm the password.

12. Enter the details for the topology database that is installed. These details must match the details entered when installing the core components.

a) Select the database type.

b) Enter the database connection details:

If you selected Db2 as the database type, enter the following details:

Database name

Enter the name of the database.

Server host

Enter the host name of the server where the database is installed.

Server port

Enter the port number for connecting to the database.

User ID

Enter the ID of an existing Db2 user that has permissions to create tables.

Password

Enter the password for this user.

If you selected Oracle as the database type, enter the following details:

Oracle Service Name

Enter the Service Name for the database.

Server host

Enter the host name of the server on which the database is installed.

User ID

Enter the ID of an existing Oracle user that has permissions to access NCIM tables. The default user ID is ncim.

Password

Enter the password for this user.

- c) Select **Create tables to hold topology data in created database** to create the database tables that are needed by Network Manager. If you already created the database tables by using the database creation scripts, you do not need to select this option. If you already created the tables and you select the option to create them again, you receive an error at the end of the installation. This error indicates that the tables were not created.
 - d) Select **Skip database connection details verification** if you do not want to verify the connection, if the database is inaccessible or for other reasons.
13. Review the summary information and click **Install**.

Results

The Network Manager GUI components are installed. Any errors are written to the installation log file, which you can view by clicking **View Log File**. Log files are kept in the /logs/ directory in the IBM Installation Manager data location.

Installing and configuring Cognos Analytics

As of Network Manager Fix Pack 11, Tivoli Common Reporting is not supported. To use reports, you must install and configure Cognos Analytics.

About this task

The documentation for your version of Cognos Analytics contains the most up-to-date and complete information about configuring that product. If there is any difference between the following information and the Cognos Analytics documentation, the latter takes precedence. Refer to the information at <https://www.ibm.com/support/knowledgecenter/SSEP7J>

Perform the following tasks to configure Cognos Analytics.

Procedure

1. Download the latest available fix pack for Cognos Analytics V11.
2. Install Cognos Analytics.
Use the detailed prerequisites and installation steps in the Cognos Analytics documentation.
 - a) Install as a root user.
 - b) When prompted to install components, select the application services and optional gateway.
3. Set the COGNOS_HOME environment variable to the directory where you installed Cognos Analytics. The path must end in analytics.
4. If you are using Db2 as the topology database, copy the following files from the Db2 database server to the **Cognos Reporting** server.
 - Copy \$Db2_HOME/sqlllib/java/db2jcc.jar to \$COGNOS_HOME/webapps/p2pd/WEB-INF/lib/.
 - Copy \$Db2_HOME/sqlllib/java/db2jcc_license_cu.jar to \$COGNOS_HOME/webapps/p2pd/WEB-INF/lib/.
 - Copy \$Db2_HOME/sqlllib/java/db2jcc.jar to \$COGNOS_HOME/drivers/.
5. Configure the data sources for reporting.
 - a) Start IBM Cognos Configuration using the appropriate command.

For example: \$COGNOS_HOME/bin64/cogconfig.sh

- b) Select **Data Access > Content Manager > Content Store**. Enter the details of your NCIM database.
- c) Click **Actions > Start** to start the Cognos server.
The server might take some time to start.
- d) Log in to the Cognos Analytics GUI.
By default, the URL to login is `http://host:9300/bi`.
- e) Click **Manage > Administration console** to start the administration console.
- f) Click **Configuration > Data Source Connection > New Data Source** to add the database connections.

Add the following connections:

Table 7. Database connections			
Product	Name	Type	JDBC connection parameters
ITNM	IBM_TRAM	IBM Db2	currentSchema=NCIM;
	NCIM		currentSchema=NCIM;
	NCMONITOR		currentSchema=NCMONITOR;
	NCPGUI		currentSchema=NCPGUI;
	NCPOLLDATA		currentSchema=NCPOLLDATA;
	PARAMETERS		currentSchema=NCPOLLDATA;

- g) Test the connections by clicking the **Test** toolbar button.
 - h) If you receive an error about `libdb2.so`, add the directory that contains the 32-bit version of this library to your `LD_LIBRARY_PATH`.
 - i) Stop the Cognos server from within the IBM Cognos Configuration GUI by clicking **Actions > Stop**.
 - j) Restart the IBM Cognos Configuration GUI.
 - k) Restart the Cognos server by clicking **Actions > Start**.
6. Install Network Manager reports by using IBM Installation Manager.
 7. Import Network Manager reports.
 - a) Copy the Network Manager reports from `$ITNM_HOME/precision_gui/reports/itnmcognos.zip` to the `$COGNOS_HOME/deployment` directory on the Cognos server.
 - b) Import the reports by clicking **Configuration > Content Administration > New Import** and selecting the **ITNM Reports** package.
 8. Configure Cognos Analytics to use HTTPS.
 9. Configure Cognos Analytics to use LDAP authentication.

If you do this, then to keep all user accounts in one place, configure Tivoli Netcool/OMNIBus to use LDAP authentication. Refer to information about *Configuring user authentication* within the Tivoli Netcool/OMNIBus documentation set. For example, refer to the topic *Configuring user authentication* within the IBM Knowledge Center for Tivoli Netcool/OMNIBus <http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html>.
 10. Edit the file `$NMGUI_HOME/profile/etc/tnm/reporting.properties`. Follow the instructions at the top of the file to edit the following properties:

```
reporting.useCognos=true
reporting.host=hostname
reporting.ui.path=/bi
reporting.path=/bi/v1/dispatch
```

11. Add the user role `ncp_reporting_user` to the appropriate Network Manager user group.
The **Cognos Reporting** menu option is shown only to users that have this role.
12. Restart the Network Manager GUI components.
13. Log in to the Cognos Analytics GUI as a user with the appropriate permissions and run a Network Manager report from **Team Content > Network Manager**.

Results

Reports are available to run from the **Reporting > Cognos Reporting** menu.

Related tasks

[Configuring Cognos Analytics](#)

Perform these tasks to configure Cognos Analytics.

Installing Network Manager reports

Before you install the Network Manager-specific reports, you must have installed Cognos Analytics.

About this task

To install Network Manager reports, complete the following tasks on the server where you installed Cognos Analytics.

Procedure

1. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

2. Click **Install**.
3. On the next **Install Packages** screen where you can select packages to install, select the latest available version of **Network Manager Reports**. The Network Manager reports package installs reports specific to Network Manager.
The prerequisites for installing the package are evaluated.
4. If any issues with prerequisites are displayed, resolve them using the information provided before continuing.
5. Click **Next**, agree to the terms in the license agreement, and click **Next** again.
6. Select the **IBM Netcool** package group.
7. Select the 64-bit version and click **Next**.
8. Select all the features of the **Network Manager reports** packages to be installed.
9. On the next **Install Packages** screens, provide configuration information for the packages being installed. Use **Next** and **Back** to navigate through the configuration options.
10. Confirm the properties of the Jazz for Service Management instance that you want to install into.

Installation directory details

The full path to the Dashboard Application Services Hub instance.

User name

Enter the user name for a user with administrative permissions in Jazz for Service Management. If it has not been changed, you can use the default user smadmin with password netcool.

Password

Enter the password for this user.

11. Confirm the details for the Network Manager topology database that was installed. The reports retrieve data from this database.

a) Select the database type.

b) Enter the database connection details:

If you selected Db2 as the database type, enter the following details:

Database name

Enter the name of the database.

Server host

Enter the hostname of the server where the database is installed.

Server port

Enter the port number for connecting to the database.

User ID

Enter the ID of an existing Db2 user that has permissions to create tables.

Password

Enter the password for this user.

If you selected Oracle as the database type, enter the following details:

Oracle Service Name

Enter the Service Name for the database.

Server host

Enter the hostname of the server on which the database is installed.

User ID

Enter the ID of an existing Db2 user that has permissions to create tables.

Password

Enter the password for this user.

- c) Select **Skip database connection details verification** if you do not want to verify the connection at this time, for example, if the database is currently inaccessible.

12. Review the summary information and click **Install**.

What to do next

After you install the Network Manager reports, you need to perform the following configuration tasks before using the reports.

1. Configure isolation level for Network Manager data sources (mandatory steps).

Change the isolation level to Read uncommitted for each of the Network Manager data sources NCPOLLDATA, PARAMETERS, NCPGUI, NCOMONITOR, NCIM, IBM_TRAM. The following data source configuration steps are mandatory to avoid database deadlock issues. Complete the following steps.

- a. Open the Dashboard Application Services Hub by specifying a URL similar to `https://itnm7.hursley.ibm.com:16311/ibm/console/logon.jsp`.
- b. Login to Dashboard Application Services Hub as the user smadmin.
- c. Click the **Reporting** icon and select **Cognos Reporting**. Within the widget select **Manage > Administration Console**.

- d. Within the **Configuration** tab, select a data source.
 - e. Open **Properties**.
 - f. Within the **Connection** tab, change the isolation level to Read uncommitted.
2. **Extend visibility of the reports function to the itnadmin user.**

After you complete the installation you must log in as smadmin to see the reports function, if you login as itnadmin you cannot see the reports function. For information about extending visibility of the reports function to the itnadmin user, see <http://www-01.ibm.com/support/docview.wss?uid=swg21963430>.

Installing the Network Health Dashboard (Netcool Operations Insight customers only)

If you have entitlement to Network Manager as part of Netcool Operations Insight, you can install the additional dashboard for Network Manager known as the **Network Health Dashboard**.

About this task

The **Network Health Dashboard** monitors a selected network view, and displays device and interface availability within that network view. It also reports on performance by presenting graphs, tables, and traces of KPI data for monitored devices and interfaces. A dashboard timeline reports on device configuration changes and event counts, enabling you to correlate events with configuration changes. The dashboard includes the event viewer, for more detailed event information.

Refer to the information on installing the **Network Health Dashboard** in the Netcool Operations Insight documentation at: <http://www.ibm.com/support/knowledgecenter/SSTPTP/welcome>.

Installing the **Network Health Dashboard** installs the following roles, which allow users to work with the **Network Health Dashboard**:

- ncp_networkhealth_dashboard
- ncp_networkhealth_dashboard_admin
- ncp_event_analytics

Installing and uninstalling fix packs

A fix pack involves moving from one minor release to another within a point version, for example, from 4.2.0.1 to 4.2.0.2. Such versions are usually called V4.2 fix pack 1 and V4.2 fix pack 2. You can install fix packs, and roll back to a previous version, using IBM Installation Manager.

About this task

You must install the GA version of Network Manager before installing a fix pack.

Post-installation tasks

After you install Network Manager, you need to perform some post-installation tasks.

About this task

To perform post-installation tasks:

Procedure

1. Ensure your Network Manager installation is completed.
You can check that the installation was successful by viewing the packages that the IBM Installation Manager successfully installed using the following commands:

- a) In IBM Installation Manager click **File > Installation History**.
 - b) Review the status of the installed packages.
The **Package Group Name** column lists the installed packages, and the **Status** column lists the results of the installation of that package.
 - c) Click **View Log** to view the log file for any selected package.
2. If you are integrating with Netcool Configuration Manager, you must now install it and then install the Netcool Configuration Manager Integration Pack. For instructions on installing these components, refer to the integration documentation at: <http://www.ibm.com/support/knowledgecenter/SS7UH9/welcome>
 3. Depending on the additional settings that are required, complete the steps in the following topics:

Option	Description
Configuring LDAP for user authentication	After a successful installation of Network Manager, you can configure LDAP for user authentication, as described in “Changing the user authentication method” on page 209 .
Configuring the Tivoli Netcool/OMNIBus Web GUI data source name	If you installed the Network Manager GUI components and chose not to create a new Web GUI data source, you must configure Network Manager to use an existing data source. Refer to the instructions at “Configuring the Tivoli Netcool/OMNIBus Web GUI data source name” on page 86 .
Non-root post-installation tasks (UNIX only)	- You can configure what user manages Network Manager processes, as described in “Configuring root/non-root permissions” on page 148 - For non-root installations, you can configure your Network Manager processes to start automatically when your system is started or restarted, as described in “Configuring processes to start automatically in a non-root installation” on page 151. Note: You do not need to perform these steps if you installed Network Manager as the root user. The automatic restart is set up as part of a root installation without the need for this postinstallation step.
Setting 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 <i>IBM Tivoli Network Manager IP Edition Administration Guide</i> .
Enabling poll data aggregation if you installed Network Manager as root	If you installed Network Manager as the root user, then you must run the <code>setup_run_storm_as_non_root.sh</code> script to enable the historical polling data processes. For details on how to do this see “Enabling historical polling” on page 153 .
Upgrading from a previous Network Manager version	Follow the steps in Chapter 8, “Upgrading and migrating,” on page 129 .
Installing the Monitoring agent	If you want to use IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, follow the steps in “Integrating with IBM Tivoli Monitoring” on page 118
Configuring Network Manager for different time zones.	If you are installing distributed Network Manager core component and Web application servers with different time zones, then you should set the same time zone on all servers which includes the database server as well as the core and GUI servers. This ensures that Network Manager is able to perform accurate timestamp comparisons from processes on different servers. You should also advise end users, such as network operators, that the system might display times that are different to the time in their location.

Option	Description
Configuring additional cryptographic routines for the GUI	By default, the GUI does not use any cryptographic routines that are excluded from a FIPS140-2 installation, regardless of the installation status of the core server. If you want to configure SNMP discovery options to enable MD5 and DES, set <code>tnm.fips.mode=false</code> in the <code>tnm.properties</code> file.
Setting up automatic network view maintenance	If you have multiple GUI servers, you must configure them so that only one server performs automatic network view and path view maintenance. If you have only one GUI server, you do not need to perform this task. For more information, see <i>Setting up automatic view maintenance</i> in the <i>IBM Tivoli Network Manager User Guide</i> .

4. Depending on your requirements, you might need to carry out further configuration tasks. Check the [Chapter 9, “Configuring Network Manager,”](#) on page 147 information.
5. After successfully installing and configuring Network Manager, see the getting started sections. For more information, see the tasks in the *IBM Tivoli Network Manager User Guide*.

Chapter 5. Uninstalling Network Manager

If you want to completely remove the product, or to roll back to a previous version, you must use IBM Installation Manager. Uninstalling the product by removing files and directories causes problems when you reinstall components.

About this task

You must uninstall the products and components in the order that is specified here. The IBM Installation Manager does not remove files that were created by running the products or configuration commands, that includes logs, updated configuration files, persisted data or cache.

If you uninstall components in a different order, you might not be able to remove some components.

Related tasks

Removing reports

Before you uninstall Network Manager, you must remove the Network Manager reports and the data sources for the reports. You can also uninstall Cognos Analytics at the same time.

Uninstalling the GUI applications

You can uninstall one or all of the following products at the same time: Network Manager GUI components, Tivoli Netcool/OMNIBus Web GUI, and Dashboard Application Services Hub.

Before you begin

The `itnm_user` user must be present in the ObjectServer. The ObjectServer must be running. Do not uninstall WebSphere Application Server until after all products installed into WebSphere Application Server are uninstalled.

About this task

To uninstall the GUI applications, complete the following steps:

Procedure

1. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

2. Click **Uninstall**.
3. Select one or more of the following components to uninstall, and click **Next**:
 - **IBM Tivoli Netcool/OMNIBus Web GUI**
 - **Network Manager GUI Components**
 - **IBM Dashboard Application Services Hub**. You cannot uninstall Dashboard Application Services Hub unless you first uninstall all components that are installed into it.
4. You are prompted for the details of WebSphere Application Server and Jazz for Service Management. If these details have not changed since installation, you can leave the defaults.

5. Review the summary information and click **Uninstall**.

Results

The selected packages are uninstalled.

Removing reports

Before you uninstall Network Manager, you must remove the Network Manager reports and the data sources for the reports. You can also uninstall Cognos Analytics at the same time.

About this task

Restriction: If you remove Cognos Analytics, the Network Manager reports do not work. If you want to use the Network Manager reports, do not uninstall Cognos Analytics.

To remove Network Manager reports and their data source settings, complete the following tasks:

Procedure

1. Log in to the Network Manager GUI in a supported browser as a user with administrator permissions.
2. Click **Common reporting** in the navigation pane on the left side of the window.
3. Select the check box next to Network Manager.
4. Click the delete icon to remove the Network Manager reports.
5. Click the **Launch** menu in the upper right of the window. Click **Cognos Administration** from the list and click the **Configuration** tab.
6. Select the check boxes next to the following data sources:
 - IBM_TRAM
 - NCIM
 - NCMONITOR
 - NCPGUI
 - NCPOLLDATA
 - PARAMETERS
7. Click the delete icon to remove the selected data sources.
8. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

9. Click **Uninstall**.
10. Select **Network Manager Reports** and **Cognos Analytics** and click **Next**.
11. Review the summary information and click **Uninstall**.

Results

The selected packages are uninstalled.

Uninstalling the Network Manager core components and Tivoli Netcool/OMNIBus

You can uninstall Network Manager core components and Tivoli Netcool/OMNIBus at the same time, if they are installed on the same server.

Before you begin

Before uninstalling Network Manager, remove the Network Manager reports and Cognos Analytics, as described in [“Removing reports” on page 74](#).

About this task

To uninstall Network Manager and Tivoli Netcool/OMNIBus, complete the following steps:

Procedure

1. Optional: If you installed as a non-root user and then ran **create_all_control.sh -auto_only** as a post-installation task to configure your Network Manager processes to start automatically on system start or restart, then run **create_all_control.sh** with the **-deinstall** option as the installing user to remove the startup scripts from the system.
2. Stop the Network Manager core components for each domain using the following command:
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 the **itnm_stop** command, it stops the default domain created at installation.

Ensure that all process starting with **ncp_** have stopped before continuing. Stop any remaining Network Manager processes if necessary.

3. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

4. Click **Uninstall**.
5. Select one or more of the following components to uninstall, and click **Next**:
 - **IBM Tivoli Netcool/OMNIBus**
 - **Network Manager Core Components**
6. Review the summary information and click **Uninstall**.

Results

The selected packages are uninstalled.

What to do next

If you installed as a non-root user, some files and directories might still be present. A user with the appropriate permissions can remove these files manually. Do not remove any files if Tivoli Netcool/OMNIBus or Probes are installed in the same location.

Uninstalling WebSphere Application Server

After uninstalling any products that were installed into WebSphere Application Server, you can uninstall WebSphere Application Server.

About this task

To uninstall WebSphere Application Server, complete the following steps:

Procedure

1. Remove the WebSphere Application Server profile that was created by Jazz for Service Management:
 - a) Stop the WebSphere Application Server profile using the following command:

```
stopServer.sh server_name -username smadin -password password
```

- b) List the profiles to get the name of the profile, using the following command:
`/opt/IBM/netcool/was/bin/manageprofiles.sh -listProfiles`
 - c) Delete the profile using the following command:
`/opt/IBM/netcool/was/bin/manageprofiles.sh -delete -profileName
profile_name`

2. Start IBM Installation Manager:

- a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

3. Click **Uninstall**.
4. Select **WebSphere Application Server** and all sub-components and click **Next**.
5. Review the summary information and click **Uninstall**.

Chapter 6. Installing and uninstalling fix packs

A fix pack involves moving from one minor release to another within a point version, for example, from 4.2.0.1 to 4.2.0.2. Such versions are usually called V4.2 fix pack 1 and V4.2 fix pack 2. You can install fix packs, and roll back to a previous version, using IBM Installation Manager.

About this task

You must install the GA version of Network Manager before installing a fix pack.

Installing fix packs

A fix pack involves moving from one minor release to another within a point version, for example, from 4.2.0.1 to 4.2.0.2, or V4.2 Fixpack 1 and V4.2 Fixpack 2.

Before you begin

You must install the GA version of Network Manager before installing a fix pack.

Prior to installing a fix pack, you should back up products and data as appropriate. For example, if you are running Network Manager on a virtual machine, then take a snapshot of your virtual machine.

About this task

Restriction: You must not use different versions of the same products or components together, unless advised otherwise by instructions in the IBM Knowledge Center or by IBM Support. If you need multiple instances of a product or component, you must install or upgrade them to the same version and fix pack. You must also ensure that the same set of test fixes, if any, are installed. For example, if you need multiple instances of the Network Manager GUI Components in one deployment, ensure that they are the same version, fix pack, and test fixes.

You must update the Network Manager core components before, or at the same time as, updating the GUI components. For example, install the fix pack on the Network Manager core server, and then on the GUI server.

Fix Pack 6

Important: Installing Fix Pack 6 or later removes existing MIB files. Network Manager These Fix Packs do not contain the Management Information Base (MIB files). Network Manager Fix Pack 5 does contain the MIB files. The MIBs are required for network discovery.

If you are upgrading from Fix Pack 5 or earlier, complete the following steps to obtain the MIB files:

1. Locate a zip file named `com.ibm.tivoli.netcool.ncp.mibs.all.any_*.zip` within the IBM Installation Manager shared location that contains the MIB files from the previous Fix Pack installation. The exact path might be different in your installation. An example path is: `/opt/IBM/IBMIM/native/`
2. Unzip this file.
3. Load the MIBs into the database by running the `ncp_mib` command, as described in *Loading updated MIB information* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

If you are installing Fix Pack 6, 7, 8, or 9 without upgrading, or you are unable to locate the MIB files using the above procedure, complete the following steps to obtain the MIB files:

1. Run the **ncp_mib** command, as described in: *Loading updated MIB information* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.
2. If you have Network Manager 4.2 Fix Pack 5 installed, back up the contents of the `$NCHOME/precision/mibs/` directory to a backup directory outside `$NCHOME`. For example, `/mibs_backup/`.

3. If you have an earlier version than 4.2 Fix Pack 5 installed, complete the following steps:
 - a. Back up the contents of the \$NCHOME/precision/mibs/ directory to a backup directory outside \$NCHOME. For example, /old_mibs/. Keep this directory and its files in case you want to roll back to this version later.
 - b. Download the Network Manager Fix Pack 5 (4.2.0.5) files from IBM Fix Central: <https://www.ibm.com/support/fixcentral/>
Important: Download the files for Linux x86, regardless of which platform you are using.
 - c. Expand the Network Manager package into a temporary directory.
 - d. Expand the repositories/disk1/ad/native/file000876 archive file into a backup directory outside \$NCHOME, for example, /mibs_backup/. This directory now contains the default MIB files.
 - e. If you customized or added any MIB files, copy the customized or new MIB files from /old_mibs/ over the default files in /mibs_backup/.
4. Regardless of the version of Network Manager you installed, the /mibs_backup/ directory now contains the most current set of MIB files from Fix Pack 5, plus any additions and customizations.

After you obtain the MIB files, install the most recent version of Network Manager.

1. Install Network Manager Fix Pack 6 using the instructions in this procedure.
2. Copy the MIB files from your /mibs_backup/ directory to the following location within the installation: \$NCHOME/precision/mibs/
3. Run the **ncp_mib** command, as described in: *Loading updated MIB information* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*.

To install a fix pack, perform the following steps:

Procedure

1. Install the fix pack on all Network Manager servers, for example, on the core and GUI server, unless otherwise directed in the fix pack Release Notes or README file.
2. Stop any running Network Manager processes.
3. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
./IBMIM
```

Fix Pack 1

Notice: If your current software versions are made up of any Network Manager 4.2 version prior to Fix Pack 1 with Jazz for Service Management V1.1.2.1 and you are upgrading to Network Manager 4.2 Fix Pack 1 and Jazz for Service Management V1.1.3.0 at the same time, then you must start IBM Installation Manager by running the `JazzSMgrpModeUpgrade.sh` script and specifying two mandatory parameters, as detailed in the technote at <https://www.ibm.com/support/pages/node/283105>.

You do not need to start IBM Installation Manager by running the `JazzSMgrpModeUpgrade.sh` script if your current software versions are any Network Manager 4.2 version prior to Fix Pack 1 with Jazz for Service Management V1.1.3.0, and you are only upgrading to 4.2 Fix Pack 1 without changing the version of Jazz for Service Management.

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

4. **Fix Pack 1**

Configure the IBM Installation Manager repositories to point at the locations of the updated packages.

5. Click **Update**.
6. Choose the package group that you want to install a fixpack for. Alternatively, select **Update all packages with recommended updates and recommended fixes**. Click **Next**.
7. Select the updates that you want to install and click **Next**.
8. Review the summary information and click **Update**.
9. After a Fix Pack upgrade on a non-root install, you must run the following scripts as the root user to enable those core processes which requires root access to operate normally:
 - `$NCHOME/precision/scripts/setup_run_as_setuid_root.sh`
 - `$NCHOME/precision/scripts/setup_run_storm_as_non_root.sh`

Fix Pack 1 Applying schema updates for a fixpack

Run the schema updater script, `update_db_schemas.pl`, to apply all necessary NCIM topology database schema updates for one or more fixpacks or interim fixes.

Before you begin

Before you can run the `update_db_schemas.pl` script, you must first have installed the fixpack or interim fix for which you want to apply schema updates.

About this task

Starting with Network Manager V4.2, when you download a new fixpack or interim fix, the download includes the `update_db_schemas.pl` and associated update files. These update files include all NCIM topology database schema changes for all fixpacks and interim fixes up to the current fix.

You can bring your NCIM topology database up to date with all schema changes for the current fixpack or interim fix, by running the `update_db_schemas.pl` script. The script will also apply schema changes for multiple fixpacks or interim fixes. For example, if for a particular major release you did not install fixpack 1, but are now installing fixpack 2, running the `update_db_schemas.pl` script will bring the NCIM topology database up to date with all schema changes for both fixpack 1 and fixpack 2.

For more information on the `update_db_schemas.pl` script, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Procedure

1. Source your environment.

On the server where the Network Manager core components are installed, the environment script is `installation_directory/netcool/core/env.sh`.

For example, on Bash, Bourne, and Korn shells, source the `env.sh` script using a command similar to the following:

```
. /opt/IBM/netcool/core/env.sh
```

2. Run the script in preview mode to list out the schema updates that will be applied.

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/sql/  
update_db_schemas.pl -domain DOMAIN_NAME -preview
```

This command prints the schema changes to be made to a file where you can review them prior to applying them to the database. By default, this file is located in `/tmp/nm-update.sql`. To give the file a different name, specify the name after the `-preview` option. If you do this, then the preview is written to a file with that name in the current directory.

3. Run the script to apply the schema updates.

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/sql/
```

```
update_db_schemas.pl -domain DOMAIN_NAME
```

Note: When the schema updater has successfully applied all the changes for a given fixpack, it writes a row to the `ncim.schemaAudit` table, giving the name of the file that contained those changes and the timestamp when they were applied.

Fix Pack 1 Checking schema updates

You can check which fixpack and interim fix schema updates have been applied to the NCIM topology database.

About this task

You can perform this check in one of the following ways:

- By running the following select statement on the NCIM topology database:

```
SELECT * FROM ncim.schemaAudit ORDER BY lastTraced;
```

- By running the `list_applied_updates.pl` script. To do this, first source your environment, and then run the script using a command similar to the following:

```
$NCHOME/precision/bin/ncp_perl $NCHOME/precision/scripts/sql/  
list_applied_updates.pl -domain DOMAIN_NAME
```

Note: If you have more than one domain that shares the same login details, you only need to run the script for one of the domains. Running the script for the other domains that use those same login details will simply produce the same output.

Uninstalling fix packs

You can uninstall a previously installed fixpack. This is known as rolling back to a previous version.

About this task

IBM Installation Manager stores installation files in its data location. These files are used to roll back to a previous version.

If you have deleted necessary rollback files, refer to the information about rolling back and entitlement in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html

Important: Network Manager Fix Pack 6 does not include the Management Information Base (MIB files). The MIBs are required for network discovery.

To uninstall Fix Pack 6 and use a previous version, complete the following steps:

1. Copy the MIB files from the following directory to a temporary directory: `$NCHOME/precision/mibs/`
2. Delete all the files in the `$NCHOME/precision/mibs` directory.
3. Uninstall Network Manager Fix Pack 6 using the instructions below.
4. If you are rolling back to 4.2 Fix Pack 5, copy the MIB files back from the temporary directory to the MIB directory: `$NCHOME/precision/mibs/`
5. If you are rolling back to a version prior to 4.2 Fix Pack 5, copy the MIB files back from the backup directory `/old_mibs/` to the MIB directory: `$NCHOME/precision/mibs/`
6. Run the `ncp_mib` command, as described in: *Loading updated MIB information* in the *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*

To uninstall a fix pack, perform the following steps:

Procedure

1. Stop any running Network Manager processes.
2. Start IBM Installation Manager:
 - a) Change to the directory where IBM Installation Manager is installed.
 - b) Run the following command:

```
. /IBMIM
```

IBM Installation Manager starts in wizard mode. To use command line, silent, console, or web browser mode, refer to the information on *Managing installations with Installation Manager* in the IBM Installation Manager documentation at: https://www.ibm.com/support/knowledgecenter/SSDV2W/im_family_welcome.html. Not all products and components support all installation modes.

3. Click **Roll Back**.
4. From the **Package Group Name** list, select the package group that contains the packages that you want to roll back. Click **Next**.
5. Select the version of the package that you want to roll back to and click **Next**.
6. Review the summary information and click **Roll Back**.

Chapter 7. 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.

About this task

Network Manager can be integrated with the following IBM products:

IBM Netcool Operations Insight

Network Manager is a key component within that solution, where it is also tightly integrated with Netcool/Impact, and IBM Operations Analytics - Log Analysis.

IBM Netcool Configuration Manager

Netcool Configuration Manager provides extensive configuration management capabilities for network devices, as well as network policy thresholding capabilities.

If it is integrated with Network Manager, then you can use the **Configuration and Event Timeline** in the **Network Health Dashboard** to correlate configuration data with alert data.

Netcool Configuration Manager can also be integrated with Network Manager and Tivoli Netcool/OMNIBus to provide more powerful diagnostic functionality to network operators.

IBM Cognos Analytics

The integration with Cognos Analytics provides ready-to-use reports, including reports on network configuration information.

IBM Tivoli Application Dependency Discovery Manager

IBM Tivoli Application Dependency Discovery Manager provides the following functionality:

- Imports network topology information discovered by Network Manager into IBM Tivoli Application Dependency Discovery Manager to complete the view of application-to-network dependencies.
- The Network Manager inventory report is available in IBM Tivoli Application Dependency Discovery Manager.
- Allows users to launch in context into Network Views to investigate which problems in the infrastructure might be affecting application performance.
- Network Manager can also launch in context into IBM Tivoli Application Dependency Discovery Manager to display the Change History view and the Details view associated with the devices.

IBM Tivoli Monitoring

IBM Tivoli Monitoring provides the following functionality:

- Monitors the health of the Network Manager application and displays key metrics and situations that help administrators monitor the health and status of Network Manager.
- Can be used to monitor resources within the Network Manager network.
- It is possible to launch from IBM Tivoli Monitoring directly into Network Manager, although this is not an in-context launch.

IBM Tivoli Business Service Manager

IBM Tivoli Business Service Manager provides the following functionality:

- Populates the business service model using network information discovered by several applications, including Network Manager.
- Maps events from multiple sources to the resources in IBM Tivoli Business Service Manager, including those resources discovered in Network Manager. In this case resources refers to devices, interfaces, and so on.

- Troubleshoots faults in the infrastructure by launching in context from the IBM Tivoli Business Service Manager service views to one of several Network Manager topology views.

Related reference

[Compatibility requirements for other products](#)

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.

About this task

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 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

[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.

Configuring an ObjectServer for use with Network Manager core processes

For users with Network Manager 4.2 Interim Fix 2 only, you can use the `config_object_server_for_itnm.sh` script to configure an ObjectServer for use with Network Manager core processes. This script supports an ObjectServer running on Windows as well as UNIX. The script configures the connection to the ObjectServer and may be used to configure either a local or remote ObjectServer. It also runs a number of SQL commands that create and configure in the ObjectServer the tables and users required by Network Manager.

Before you begin

Before you run the `config_object_server_for_itnm.sh` script, you must ensure that the ObjectServer is up and running.

You must run the `config_object_server_for_itnm.sh` script on the server where Network Manager core processes are installed.

About this task

To configure the ObjectServer for use with Network Manager core processes, perform the following steps:

Procedure

1. Source the Network Manager core environment variables.
2. Change to the following directory:

```
$NCHOME/precision/scripts
```

3. Issue the following command to run the `config_object_server_for_itnm.sh` script:

```
./config_object_server_for_itnm -o OS_name -u OS_admin_user  
-p OS_admin_password -I itnm_account_password
```

Where:

- *OS_name* is the name of the ObjectServer to be configured.
- *OS_admin_user* is the user identifier of the administrative user for the ObjectServer.
- *OS_admin_password* is password of the administrative user for the ObjectServer.
- *itnm_account_password* is the password of the Network Manager itnadmin and itnmuser user accounts which will be created on the ObjectServer.

During the execution of the script, you will be asked whether you want to use an existing ObjectServer connection defined within the `$NCHOME/etc/omni.dat` configuration file. Answer this question as follows:

- y to use a connection already defined in the `$NCHOME/etc/omni.dat` configuration file.
- n to supply the following new ObjectServer connection details:
 - Hostname.
 - Port.
 - Whether the connection uses SSL.

Note: If you choose this option, then, on completion of script execution, the connection details are written to the `$NCHOME/etc/omni.dat` configuration file.

Results

On completion, the script advises that you must configure a probe for the ObjectServer.

Related tasks

[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.

Configuring the user repository

If you want to use an ObjectServer as the user repository and you did not install this ObjectServer with the Network Manager installation, then you must run scripts to configure the users and assign roles to these users.

About this task

To configure the ObjectServer as the user repository, perform the following steps:

Procedure

1. Log into the machine where the Network Manager GUI components are located.
2. Source the Network Manager GUI environment variables.
3. Go to the `$WAS_HOME/bin` directory.
4. Create the users by running the following command:

```
./wsadmin.sh -conntype SOAP -user jazz_admin_name -password jazz_admin_password  
-lang jython -f $NMGUI_HOME/bin/scripts/users.py itnadmin_password
```

Where:

- *jazz_admin_name* is the administrator username for Jazz for Service Management. By default, this is `smadmin`.
- *jazz_admin_password* is the administrator password for Jazz for Service Management.
- *itnadmin_password* is the password for both the `itnadmin` and `itnmuser` accounts.

5. Assign roles to users and to user groups by running the following command:

```
$NMGUI_HOME/bin/assigns_users_to_roles -u jazz_admin_name  
-p jazz_admin_password -r
```

Where:

- *jazz_admin_name* is the administrator username for Jazz for Service Management.
- *jazz_admin_password* is the administrator password for Jazz for Service Management.
- *-r* is a flag to rebuild the list of user identifiers. Specifying this flag instructs the script to assign roles to the Jazz for Service Management administrator user (by default, smadmin) as well as to all of the Network Manager users and groups.

Configuring the Tivoli Netcool/OMNIBus Web GUI data source name

If you installed the Network Manager GUI components and chose not to create a new Web GUI data source, you must configure Network Manager to use an existing data source. You can also follow these instructions if you want to change the data source.

About this task

A data source is another term for an ObjectServer or ObjectServer failover pair used by the Web GUI for event information. Some deployments contain many ObjectServers, and the Web GUI can contain events from several different ObjectServers. 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 a data source used by the Web GUI.

If you want to add a new data source in Web GUI, use the instructions about *configuring data sources* in the Web GUI documentation at the following location:

<http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html>

Ensure Network Manager is configured to use an existing Web GUI data source by completing the following steps.

Procedure

1. Back up and edit the `NCHOME/etc/precision/ModelNcimDb.DOMAIN_NAME.cfg` file.
2. Change the `WebTopDataSource` property to the new data source name.
3. Save and close the file.
4. Restart the `ncp_model1` process.

Configuring topology event types

To integrate the topology views and filtered **Event Viewer** views, the view name and type must match. If you change the defaults in the **Event Viewer**, you must configure the name and type in Network Manager.

About this task

In a filtered **Event Viewer** view, you can configure the name and view type. If you change the view name and type from the default values of `NetworkManagementEvents` and `global`, then the **Event Viewer** 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 **Event Viewer**, complete the following steps:

Procedure

1. Back up and edit the file `$NMGUI_HOME/profile/etc/tnm/topoviz.properties`.
2. Change the values of the following properties:

```
topoviz.webtop.view.name=NetworkManagementEvents
topoviz.webtop.view.type=global
```

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.

About this task

To ensure that your Tivoli Netcool/OMNIBus installation receives events from the network, you must configure the relevant Tivoli Netcool/OMNIBus probes. In particular, in order to ensure that you can process SNMP traps from your network, you must install and configure the SNMP probe (also known as the `mttrapd` probe).

For more information about probe installation and configuration, see the relevant probe reference guide, available from the Information Center at http://www.ibm.com/support/knowledgecenter/SSSHTQ/omnibus/common/kc_welcome-444.html.

Installing the Knowledge Library

You must install the Netcool/OMNIBus Knowledge Library in order to enable Network Manager to fully process network events.

About this task

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.

Tivoli Netcool/OMNIBus integration reference

Read about settings for additional interaction between Network Manager and Tivoli Netcool/OMNIBus.

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 at <http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html>.

Related tasks

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.

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 uncomment and then modify the value as required. String values must be enclosed in quotation marks; other values do not require quotation marks. For example:

```
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.

Note: The following properties have standard default values:

Server

Defaults to the ObjectServer identified in the `ConfigItnm` schema, thereby ensuring consistency with the Network Manager gateway.

PropsFile

Defaults to `$NCHOME/probes/platform/nco_p_ncpmonitor.props`.

RulesFile

Defaults to `$NCHOME/probes/platform/nco_p_ncpmonitor.rules`.

MessageLog

Defaults to `$NCHOME/log/precision/nco_p_ncpmonitor.domain_name.log`.

RawCaptureFile

Defaults to `$NCHOME/var/precision/nco_p_ncpmonitor.domain_name.cap`.

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://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html>.

nco_p_ncpmonitor.rules configuration reference

The `$NCHOME/probes/arch/nco_p_ncpmonitor.rules` file defines how the Probe for Tivoli Netcool/OMNIbus processes Network Manager event data to create a meaningful Tivoli Netcool/OMNIbus event.

In practice, this 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://www.ibm.com/support/knowledgecenter/SSHTQ/landingpage/NetcoolOMNIBus.html>.

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

Note: The full input to and output from the probe rules can be seen in the probe trace file. Set the trace to debug 4. The probe trace file can be found at: \$NCHOME/log/precision. For more information on setting log levels, see *IBM Tivoli Network Manager IP Edition Administration Guide*.

Related reference

[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.

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 8. Network Manager fields that populate events		
Network Manager field name	Field content	Always available?
Description	A brief description of the event.	Yes
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

Table 8. Network Manager fields that populate events (continued)

Network Manager field name	Field content	Always available?
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
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

<i>Table 8. Network Manager fields that populate events (continued)</i>		
Network Manager field name	Field content	Always available?
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
ExtraInfo_sysObjectId	If available, the sysObjectId value is given for ItnmEntityCreation events only	No

<i>Table 8. Network Manager fields that populate events (continued)</i>		
Network Manager field name	Field content	Always available?
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

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.)

<i>Table 9. alerts.status fields used by Network Manager</i>			
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 Event Viewer 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.

<i>Table 9. alerts.status fields used by Network Manager (continued)</i>			
alerts.status field	Data type	Description	Network Manager field name/ Default value in rules file
Class	integer	The alert class assigned 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.
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

<i>Table 9. alerts.status fields used by Network Manager (continued)</i>			
alerts.status field	Data type	Description	Network Manager field name/ Default value in rules file
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
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

Table 9. alerts.status fields used by Network Manager (continued)

alerts.status field	Data type	Description	Network Manager field name/ Default value in rules file
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.	
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.

<i>Table 9. alerts.status fields used by Network Manager (continued)</i>			
alerts.status field	Data type	Description	Network Manager field name/ Default value in rules file
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.	

Table 9. alerts.status fields used by Network Manager (continued)			
alerts.status field	Data type	Description	Network Manager field name/ Default value in rules file
Summary	varchar(255)	A textual description of the event.	Description
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 Event Viewer , and in the Occurred column in the <code>mojo.events</code> 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 at [IBM Tivoli Netcool/OMNIBus product information](#).

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 10. 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

Table 10. Tivoli Netcool/OMNIBus automations added by Network Manager (continued)			
Automation	Description	Added during installation?	Default status
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.

About this task

You can configure integration between Network Manager, Tivoli Netcool/OMNIBus, and Netcool Configuration Manager.

You must install Network Manager before installing Netcool Configuration Manager. You must install Netcool Configuration Manager using certain configuration options.

For more information on configuring the integration, select your version of Netcool Configuration Manager from the Knowledge Center at <http://www.ibm.com/support/knowledgecenter/SS7UH9/welcome>, 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*.

Note: On the Netcool Configuration Manager Knowledge Center you will also find full details on how to remove the integration with Netcool Configuration Manager.

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.

About this task

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.

Note: To load Discovery Library (IdML) books containing information about virtual machines into TADDM, you must have TADDM 7.2.1 Fix Pack 1 or later.

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 using the DLA

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 run the `ncp_dla.sh` script with an IBM Java JRE in your `$PATH` environment variable. To check your Java version, run the following command: `java -version`. If the Java version is not from IBM, locate an IBM JRE and add the directory that contains it to the start of the `$PATH` environment variable. A suitable JRE is located in the following directory: `$WAS_HOME/java/bin`.
- 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 IBM Knowledge Center at the following Web address:
<http://www.ibm.com/support/knowledgecenter/SSPLFC/welcome>
 - For more information about IBM Tivoli Business Service Manager, see the IBM Knowledge Center at the following Web address:
<http://www.ibm.com/support/knowledgecenter/SSSPFK/welcome>
 - For more information about IBM Tivoli Change and Configuration Management Database, see the IBM Knowledge Center at the following Web address: <http://www.ibm.com/support/knowledgecenter/SSPLFC/welcome>

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.

About this task

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 `$NMGUI_HOME/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.

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 103. 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.

Procedure

1. Go to `$NMGUI_HOME/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. Set the 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
 - LTE - generates the following data for LTE classes:
 - Function
 - HomogeneousCollection
 - Zone
 - Card
 - NetworkInterface
 - 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
 - Daughter Card

To generate data you must add a value using the following format to the **ncp.dla.generationFilter** parameter:

```
ncp_dla.generationFilter=ComputerSystem[,data]
```

Where *data* is one of the specific types of data listed in this step.

Examples:

- To generate system data, add the following values to the parameter:

```
ncp_dla.generationFilter=ComputerSystem
```

Note: At a minimum, you must specify this value. If you do not specify any values in the **ncp.dla.generationFilter** parameter, then the DLA will not generate any data.

- To generate system and LTE data, add the following values to the parameter:

```
ncp_dla.generationFilter=ComputerSystem,LTE
```

- 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
- **Oracle** Oracle

ncp.dla.datasource.driver

Specify the JDBC driver to use:

- **DB2** `com.ibm.db2.jcc.Db2Driver`
- **Oracle** `oracle.jdbc.driver.OracleDriver`

ncp.dla.datasource.url

Specify the JDBC URL for connecting to the NCIM database:

- **DB2** `jdbc:db2://host_name:port_number/database_name`
- **Oracle** `jdbc:oracle:thin:@//host_name:port_number/service_name` where *service_name* is the Oracle service name that refers to the Oracle database instance running on the server.

ncp.dla.datasource.schema

The NCIM database schema name, typically "ncim"

ncp.dla.datasource.ncpgui.schema

The NCPGUI database schema name, typically "ncpgui"

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 `$NMGUI_HOME/profile/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 `$NMGUI_HOME/profile/etc/tnm/tnm.properties` file.

ncp.dla.datasource.loginTimeout

The login timeout, default 5 seconds

7. Use the `ncp.dla.refresh.book` parameter to specify whether the DLA should refresh existing Discovery Library books or create new ones. The default option is `true`; this default option updates existing instances and creates new ones, if necessary.

```
ncp.dla.refresh.book=true
```

8. Use the `ncp.dla.lte.topology` parameter to export LTE control and user plane topology. This option can produce very large amounts of data for large networks. The volume of data generated might have an adverse affect on your TADDM deployment.. The default option is `false`.

```
ncp.dla.lte.topology=false
```

9. 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%'
```

10. Use the `ncp.dla.entity.details` parameter to specify whether the DLA should query for entity detail data and export this data as an extended attribute. The default option is `false`.

```
ncp.dla.entity.details=false
```

11. Use the `ncp.dla.signatureGenExcludeMAC` parameter to exclude certain MAC addresses from the signature generation algorithm.

This is useful when MAC addresses present on network devices are duplicated across the network, and you want to prevent the signature generation process from unnecessarily generating the same signature multiple times.

To use this capability, for each potentially duplicated MAC address in the network you must enter a `signatureGenExcludeMAC` property. The format of this property is as follows:

`ncp.dla.signatureGenExcludeMAC.n=MAC`

Where:

- *n* is an incrementing number for each exclusion starting from 1.
- *MAC* is the colon-delimited MAC address to exclude from the signature generation process.

For example, the default values in the `ncp_dla.properties` file specify the that following MAC addresses are to be excluded from the signature generation process:

- 00:00:00:00:00:00, which is an all-zero default MAC address.
- 02:00:00:00:00:04, which is a Juniper fpx1 internal interface MAC address.
- 00:0B:CA:FE:00:00, which is a Juniper bme0 management interface MAC address.

```
ncp.dla.signatureGenExcludeMAC.1=00:00:00:00:00:00
ncp.dla.signatureGenExcludeMAC.2=02:00:00:00:00:04
ncp.dla.signatureGenExcludeMAC.3=00:0B:CA:FE:00:00
```

12. Use the `ncp.dla.signatureOverride` parameter to manually configure the signature used by the DLA on a per-device basis, in this way bypassing automated signature generation.

This is useful when the devices exported by the DLA are not properly reconciled within TADDM, such as when the signature attribute differs for the same device.

In order to use this capability, for each device whose signature you want to override you must know the following information:

- a. Network Manager `entityName`
- b. TADDM signature
- c. `SignatureOverride` property

The format of this property is as follows:

`ncp.dla.signatureOverride.n=entityName=signature`

Where:

- *n* is an incrementing number for each override starting from 1.
- *entityName* is the Network Manager `entityName` of the device to apply the signature to.

- *signature* is a valid CDM signature of the form IP address(MAC address) or IP address.

Note: You must ensure that you choose a signature IP and MAC address relating to the specified device when using this capability.

For example, to override the signature for the devices "fred" and "barney", add the following configuration properties:

```
ncp.dla.signatureOverride.1=fred=172.20.1.6(00:21:28:FF:1A:3A)
ncp.dla.signatureOverride.2=barney=172.20.1.7(00:21:EE:6B:1A:2A)
```

- 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/netcool/core/var/precision/ccmdb`. If you specify this option, skip step [“14” on page 106](#) and proceed to step [“17” on page 107](#).

FTP

The Discovery Library books are transferred to a remote server by FTP. If you specify this option, you must complete step [“14” on page 106](#)

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**.

- 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 `$NMGUI_HOME/profile/etc/tnm/tnm.properties` file.

- Optional: You can limit the scope of data collection by filtering the results by chassis identifiers. Do this by specifying an SQL query within the `ncp.dla.chassis.ids` parameter.

Specifying a filter using the `ncp.dla.chassis.ids` property enables you to retrieve only the ComputerSystem records that match the entity ids returned by the SQL query.

Note: This filtering method is preferable to filtering using the `ncp.dla.network.view` parameter, as it enables you to more precisely specify the chassis of interest.

The following example shows an SQL query that returns the chassis identifiers that were tagged on the network edge.

Note: For ease of reading this SQL query is presented indented on multiple lines. However, in the `ncp.dla.properties` configuration file, the entire SQL query must be presented on a single line; otherwise the operation will return an error.

```
ncp.dla.chassis.ids=SELECT e.mainNodeEntityId
                      FROM entity e
                      INNER JOIN domainMgr d ON d.domainMgrId = e.domainMgrId
                      WHERE d.domainName = 'NCPPUP' AND EXISTS
                            (SELECT ed.entityId FROM entityDetails ed
                             WHERE ed.entityId = e.entityId
                             AND ed.keyName = 'NetworkEdge'
                             AND ed.keyValue = 1)
                      GROUP BY e.mainNodeEntityId
```

16. Optional: You can exclude model and manufacturer information from the output using the `ncp.dla.ExcludeModel` and `ncp.dla.ExcludeManufacturer` parameters.

The format of these parameters is as follows:

```
ncp.dla.ExcludeModel.N=MODEL_NAME
ncp.dla.ExcludeManufacturer.N=MANUFACTURER_NAME
```

Where:

- *N* is a number that increments for each exclusion, starting from 1.
- *MODEL_NAME* is a model name to exclude.
- *MANUFACTURER_NAME* is a manufacturer name to exclude.

Matching values are suppressed from the output.

The following example shows how to exclude the manufacturers Windows and net-snmp.

```
ncp.dla.ExcludeManufacturer.1=Windows
ncp.dla.ExcludeManufacturer.2=net-snmp
```

17. 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

18. 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.

19. 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.

20. Create a copy of the edited configuration file, giving the file a name of your choice.
21. 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`).

What to do next

If you want to start the IBM Tivoli Application Dependency Discovery Manager GUIs from Network Manager, complete the additional configuration tasks to add a menu option to the Network Manager GUIs, and add the JSP inventory report to TADDM.

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 begin

Before you can run the DLA, the DLA properties file must have been configured correctly.

About this task

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.

Procedure

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:

```
./ncp_dla.sh ncp_dla.properties.domain_name [ -getmore ]
```

Note: The `-getmore` flag is optional. It generates all entities including stacked switches for ComputerSystem CDM filters.

See [“Example” on page 108](#) 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@abc.test]# ./ncp_dla.sh ncp_dla.properties.NCOMS
ncp_DLA ( IBM Tivoli Network Manager IP Edition - Discovery Library Adapter )
Copyright (C) 1997 - 2013 By IBM Corporation. All Rights Reserved.
See product license for details.

[IDML Generation Mode]
Initializing...
WARNING: user.install.root not defined, using /opt/IBM/netcool
/core/precision/profiles/TIPProfile
Loading properties from /opt/IBM/netcool/core/precision/profiles
/TIPProfile/etc/tnm/tnm.properties
FINE: database.type = db2
```

```

FINE: database.dbname = ITNM
FINE: database.jdbc.url = null
FINE: database.host = abc.test.ibm.com
FINE: database.port = 50000
FINE: database.username = ncim
FINE: database.connection.defaultFetchSize = null
FINE: database.connection.propertiesFile = null
FINE: Getting encrypted password
Jun 3, 2013 9:15:09 AM DbConnectionPool getJdbcURL
FINE: JDBC URL = jdbc:db2://abc.test.ibm.com:50000/ITNM
INFO: HNMXB0006I=JDBC Driver: com.ibm.db2.jcc.Db2Driver
INFO: HNMXB0007I=JDBC URL : jdbc:db2://abc.test.ibm.com:50000/ITNM
INFO: HNMXB0007I=JDBC URL : jdbc:db2://abc.test.ibm.com:50000/ITNM
Jun 3, 2013 9:15:10 AM DbConnectionPool getConnection
FINEST: Connection Pool READ has size 0
Working on ITNM domain 'NCOMS'...
Processing 142 ComputerSystem(s)...
% Complete: 0...10...20...30...40...50...60...70...80...90...100
Writing IDML Book to '/tmp/dla/ITNMIP39.9.42.16.62.2013-06-03T13.15.11.579Z.
refresh.xml'...
Shutting down...
Finished.

```

Related tasks

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.

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.

About this task

To set up a more fine-tuned data collection and export, perform the following steps:

Procedure

1. Discover the network using Network Manager.
2. Run the **itnmTagNetworkEdgeEntities.pl** tagging utility to identify network edge entities, as described in [“Identifying network edge entities”](#) on page 109.
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 110.
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 112.
5. Run the adaptor to create the Discovery Library book, as described in [“Creating a Discovery Library book for network edge data”](#) on page 112.

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.

Before you begin

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.

About this task

To run the utility to automatically tag the entities considered as being on the edge of the network in a domain:

Procedure

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:
 - `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -domain NCOMS -autoEndNodeTags`
3. Optional: You can use the `-includeNextHop` option with the `-autoEndNodeTags` option to go one hop further from the edge entities. Using the `-includeNextHop` option automatically includes the edge entities that are included when using only the `-autoEndNodeTags`, plus any routers or switches directly connected to the edge entities. For example, to automatically tag such interfaces, enter:
 - `$NCHOME/precision/bin/ncp_perl 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:

- `$NCHOME/precision/bin/ncp_perl 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:
 - `$NCHOME/precision/bin/ncp_perl itnmTagNetworkEdgeEntities.pl -help`

Results

The utility adds an `entityDetails->NetworkEdge=1` attribute in the `ncimCache.entityData` database.

What to do next

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.

Before you begin

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.

About this task

To create a filtered view of the edge of your network:

Procedure

1. Click the **Incident** icon and select **Network Availability > Network Views > Libraries**.
2. Click **New View** .
3. 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 icon to represent the view, click **Browse**  to browse for an icon.

Tree Icon

If you want a different icon than the default 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 **Event Viewer** event with the highest severity, and can appear with an additional severity icon.

4. 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'`.
5. Set **End Nodes** to Include
6. Set **Connectivity** to Layer 2.
7. Click **Ok** and then **Save**.

What to do next

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.

About this task

To edit the file:

Procedure

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.

What to do next

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](#)

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.

Before you begin

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.

About this task

To create a DLA book containing network edge data:

Procedure

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:

```
./ncp_dla.sh ncp_dla.properties.domain_name [ -getmore ]
```

Note: The -getmore flag is optional. It generates all entities including stacked switches for ComputerSystem CDM filters.

For example, to run the adaptor for the domain called NCOMS, enter the following: `./ncp_dla.sh ncp_dla.properties.NCOMS`

Example

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: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.

About this task

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:

Procedure

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 -x -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](#)

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](#)

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.

About this task

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

launch in context is installed (or updated if already exists) by the TADDM installation. For more information, see the documentation at <http://www.ibm.com/support/knowledgecenter/SSPLFC/welcome>.

The JSP report is provided; to use the report, the files must be copied to the correct location on your TADDM server.

Procedure

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.

Results

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 configure the TADDM menu options to Network Manager.

Before you begin

The following steps assume that the Discovery Library Adapter (DLA) is installed on the same server as Dashboard Application Services Hub 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 Dashboard Application Services Hub and the Network Manager GUI components are installed.

For more information about IBM Tivoli Application Dependency Discovery Manager, see: <http://www.ibm.com/support/knowledgecenter/SSPLFC/welcome>

Procedure

1. Configure the launch points from the menu to the TADDM installation:

- a) Edit the following file: `$NMGUI_HOME/profile/etc/tnm/tnm.properties`

- i) Update the `tnm.taddm.serverName` property to the IP address or host name of your TADDM server.
- ii) Update the `tnm.taddm.serverPort` property to the TCP port on which your TADDM server is listening.
- iii) Update the `tnm.taddm.username` and `tnm.taddm.password` properties to the user name and password (unencrypted) to use to access your TADDM server.

- b) 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.

What to do next

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](#)

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.

Procedure

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 XSLT 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” on page 117](#) 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.Db2
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](#)

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).

Before you begin

You must have both IBM Tivoli Network Manager IP Edition and IBM Tivoli Business Service Manager installed and configured.

Results

The probe provides IBM Tivoli Business Service Manager with BSM_Identity tokens for Network Manager.

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 using the DLA

Before you configure and use the Discovery Library Adapter (DLA), make sure the prerequisites are met.

Configuring the Dashboard Application Services Hub

After installation, you might need to configure Dashboard Application Services Hub security or single sign-on. You can find information on configuring Dashboard Application Services Hub on the Jazz for Service Management Knowledge Center.

About this task

The Jazz for Service Management Knowledge Center is located at <https://www.ibm.com/support/knowledgecenter/SSEKCU>

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.

Before you begin

You must have installed Network Manager before installing IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.

About this task

For instructions on how to install and configure IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, refer to the *IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition User's Guide*.

IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition

IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition is an agent that runs on the server where Network Manager is installed.

The agent works with IBM Tivoli Monitoring and provides the following functions:

- Monitor IBM Tivoli Network Manager IP Edition (Network Manager) for alerts on the systems that you are managing by using predefined situations or custom situations.
- Establish your own performance thresholds.
- Trace the causes leading to an alert.
- Gather comprehensive data about system conditions.
- Use policies to perform actions, schedule work, and automate manual tasks.

The agent is managed in the same way and using the same GUIs as your other IBM Tivoli Monitoring agents.

The Tivoli Enterprise Portal is the interface for IBM Tivoli Monitoring products. You can use the consolidated view of your environment provided by the Tivoli Enterprise Portal to monitor and resolve performance issues.

Installing and configuring

Install IBM Tivoli Monitoring, apply application support to the IBM Tivoli Monitoring components, and then install and configure IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.

About this task

To install and configure IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, complete the following steps in order:

Procedure

1. Install and configure a compatible version of IBM Tivoli Monitoring. Use the procedures in the *IBM Tivoli Monitoring Installation and Setup Guide*.
2. Check the requirements for the IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition agent. Use the information in [“Requirements for installing the monitoring agent”](#) on page 122.
3. Apply application support on all the servers where IBM Tivoli Monitoring components are installed. Use the procedures described in the section [“Installing application support ”](#) on page 119.
4. Install the IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition agent. Use the procedures described in [“Installing the monitoring agent ”](#) on page 122.

What to do next

Configure the IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition agent. Use the procedures described in [“Configuring the monitoring agent ”](#) on page 124.

Installing application support

Application support ensures the correct communication between IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition and IBM Tivoli Monitoring components.

Before you begin

Applying application support involves stopping and restarting IBM Tivoli Monitoring components. Work with your IBM Tivoli Monitoring administrator to choose an appropriate time to do this.

About this task

You install the application support on the following IBM Tivoli Monitoring components, which store and analyze data received from the agent

- Tivoli Enterprise Monitoring Server
- Tivoli Enterprise Portal Server

- Tivoli Enterprise Portal Desktop Client
- Tivoli Enterprise Portal browser (applies to UNIX version of the browser)

This task describes installing application support on a local sever. For information about configuring application support on remote servers, see the *IBM Tivoli Monitoring Installation and Setup Guide*.

Installing application support on Linux and AIX

Installing application support on Linux and AIX involves different steps to other platforms.

About this task

Application support is supported on the same Linux and AIX versions as Network Manager.

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

- AIX 6.1 iSeries and pSeries
- AIX 7.1 iSeries and pSeries
- AIX 7.2 iSeries and pSeries

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

- Red Hat Enterprise Linux Server 6 (x86-64)
- Red Hat Enterprise Linux Server 7 (x86-64)
- **Fix Pack 11** Red Hat Enterprise Linux Server 8 (x86-64)
- SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 and SP3
- **Fix Pack 3** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)
- **Fix Pack 10** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP4
- **Fix Pack 11** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP5

Fix Pack 6 From Fix Pack 6 onwards, on Linux on IBM z Systems, the following versions are supported:

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP2 and SP3 on IBM z Systems (s390x, 64 bit)

To apply the application support for IBM Tivoli Monitoring components on Linux and AIX systems, complete the following steps.

Procedure

1. On the server where IBM Tivoli Monitoring is installed, download the installation package for IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.
2. Decompress the installation package.
3. Start the installation wizard using the `install.sh` script in the `ITMAgent` directory.
4. Accept the suggested install directory.
The installation finds the IBM Tivoli Monitoring installation directory and displays it. By default, the location is `/opt/IBM/ITM`, but it might be different if IBM Tivoli Monitoring was installed in a different location.
5. Confirm that it is OK to restart existing processes.
6. Select **Install products to the local host**.
7. Accept the default key, `IBMTivoliMonitoringEncryptionKey`, unless you use a different key for each product.
8. Accept the licensing agreement.

9. Specify an application support package to install. The list of support packages varies depending on your operating system and on which IBM Tivoli Monitoring components are installed. Install all of the displayed support packages.
10. If the Tivoli Enterprise Portal Server, Tivoli Enterprise Monitoring Server, Tivoli Enterprise Portal Desktop, and Tivoli Enterprise Portal Browser are all installed on the same machine, configure the agent support for all these applications using a script.

Restriction: Only use this option if all components are installed on the same server.

- a) Change to the IBM Tivoli Monitoring directory.
 - b) If you are not using the default /opt/IBM/ITM location, set CANDLE_HOME to the IBM Tivoli Monitoring installation directory.
 - c) Run the setupITNMAgentSupport.sh script.
11. If some of the IBM Tivoli Monitoring components are installed on different servers, complete the following steps on the appropriate servers:
 12. If the Tivoli Enterprise Monitoring Server is installed on a different server, run the following commands on that server from the \$ITMHOME/bin directory, where ITMHOME is the directory where IBM Tivoli Monitoring is installed:
 - a) If it is not already started, start the monitoring server using the following command, where *tems_name* is the name of the monitoring server. You can find out the name of the monitoring server by looking for the value TEMS Name in the monitoring server configuration screen.

```
./itmcmd server start tems_name
```

- b) Activate application support on the monitoring server using the following command.

```
./itmcmd support -f install -t tems_name np
```

- c) Stop the monitoring server using the following command:

```
./itmcmd server stop tems_name
```

- d) Restart the monitoring server using the following command:

```
./itmcmd server start tems_name
```

13. If the Tivoli Enterprise Portal Server is installed on a different server, run the following commands on that server from the \$ITMHOME/bin directory, where ITMHOME is the directory where IBM Tivoli Monitoring is installed.

- a) Stop the portal server using the following command:

```
./itmcmd agent stop cq
```

- b) Configure the portal server with the new agent information using the following command:

```
./itmcmd config -A cq
```

- c) Restart the portal server using the following command:

```
./itmcmd agent start cq
```

14. If the Tivoli Enterprise Portal Desktop is installed on a different server, run the following commands on that server from the \$ITMHOME/bin directory, where ITMHOME is the directory where the desktop client is installed.

- a) Stop the desktop client using the following command:

```
./itmcmd agent stop cj
```

- b) Configure the desktop client with the new agent information using the following command:

```
./itmcmd config -A cj
```

c) Restart the desktop client using the following command:

```
./itmcmd agent start cj
```

d) Restart any Web Start Tivoli Enterprise Portal clients to view the new agent workspaces.

Installing application support on Windows

Installing application support on Windows involves different steps to other operating systems.

About this task

Application support is supported on the same versions of Windows that IBM Tivoli Monitoring supports. Refer to the documentation for your version of IBM Tivoli Monitoring for more information on the supported versions of Windows.

To apply the application support for IBM Tivoli Monitoring components on Windows systems, complete the following steps.

Procedure

1. On the server where IBM Tivoli Monitoring is installed, download the installation package for IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.
2. Decompress the installation package.
3. Change to the ITMagent/windows/ directory and run the setup.exe file to start the agent installer.
4. Accept the recommendation for the JRE version.
5. Accept the suggested installation directory. By default, the location is /opt/IBM/ITM, but it might be different if IBM Tivoli Monitoring was installed in a different location.
6. If you do not have a product custom key, accept the default key, IBMTivoliMonitoringEncryptionKey.
7. Select one or more of the following components to apply application support to. Components are only displayed if they are installed on the current server.
 - Tivoli Enterprise Monitoring Server
 - Tivoli Enterprise Portal Server
 - Tivoli Enterprise Portal Desktop Client

Select **IBM Tivoli Network Manager** for each option you selected. If the framework is not installed on your system, also select **TEMA Agent Framework** for each option you selected.

Installing the monitoring agent

Install the monitoring agent on the server where the Network Manager core components are installed.

About this task

Install the agent once. Configure one instance of the agent for each Network Manager domain.

Requirements for installing the monitoring agent

In addition to the requirements described in the IBM Tivoli Monitoring installation documentation, IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition has the following requirements.

Prerequisite software

Install the following prerequisite software before installing the monitoring agent:

- IBM Tivoli Monitoring V6.3 Fix Pack 1 or later
- Tivoli Enterprise Portal V6.3 Fix Pack 1 or later

Sizing requirements

A single server that hosts the hub monitoring server, portal server, and a monitoring agent requires approximately 300 MB of space.

A server that hosts only the monitoring agent requires approximately 30 MB of space, including the specific enablement code for the monitoring agent. More space is required for each additional monitoring agent that you deploy on the monitoring computer.

Supported operating systems

The monitoring agent can be installed on any of the operating systems that are supported for Network Manager 4.2.

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

- AIX 6.1 iSeries and pSeries
- AIX 7.1 iSeries and pSeries
- AIX 7.2 iSeries and pSeries

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

- Red Hat Enterprise Linux Server 6 (x86-64)
- Red Hat Enterprise Linux Server 7 (x86-64)
- **Fix Pack 11** Red Hat Enterprise Linux Server 8 (x86-64)
- SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 and SP3
- **Fix Pack 3** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)
- **Fix Pack 10** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP4
- **Fix Pack 11** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64) SP5

Fix Pack 3 From Fix Pack 3 to Fix Pack 5, on Linux on IBM z Systems, the following versions are supported:

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP1 on IBM z Systems (s390x, 64 bit)

Fix Pack 6 From Fix Pack 6 onwards, on Linux on IBM z Systems, the following versions are supported:

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP2 and SP3 on IBM z Systems (s390x, 64 bit)

Fix Pack 10 From Fix Pack 10 onwards, on Linux on IBM z Systems, the following versions are supported:

- Red Hat Enterprise Linux Server 7.3 on IBM z Systems (s390x, 64 bit)
- SuSE Linux Enterprise Server (SLES) 12.0 SP5 on IBM z Systems (s390x, 64 bit)

The following hypervisor and operating system combinations are supported:

- VMware ESX 5.0, 5.5, 6.0:
 - Red Hat Enterprise Linux Server 7 (x86-64)
 - SuSE Linux Enterprise Server (SLES) 11.0 (x86-64) SP2 and SP3
 - **Fix Pack 3** SuSE Linux Enterprise Server (SLES) 12.0 (x86-64)

Requirements for searching the online help

To use the search function for the online help for this monitoring agent, ensure that you have selected the **IBM Eclipse help server** check box when installing the Tivoli Enterprise Portal Server.

The 'Searching Agent Help' topic in the online help for this monitoring agent contains a link to the Eclipse help, where the search function is enabled. From the Table of Contents in the left-hand pane of the help, select the 'Searching Agent Help' topic to find the link to the Eclipse help in the right-hand pane.

Installing the monitoring agent on a local server

Complete these steps to install and configure the monitoring agent on the Network Manager server.

Before you begin

If you are using Red Hat Enterprise Linux 7 or SuSE Linux Enterprise Server 12, run the following command before installing, uninstalling, starting, or stopping the monitoring agent:

```
setarch $(uname -m) --uname-2.6
```

Procedure

1. On the server where you want to install the monitoring agent, download the installation package for IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition.
2. Decompress the installation package.
3. Start the installation wizard using the `install.sh` script in the `ITMAgent` directory.
4. Accept the suggested install directory.
The installation finds the IBM Tivoli Monitoring installation directory and displays it. By default, the location is `/opt/IBM/ITM`, but it might be different if IBM Tivoli Monitoring was installed in a different location.
5. Select **Install products to the local host**.
6. Accept the licensing agreement.
7. Accept the default key, `IBMTivoliMonitoringEncryptionKey`, unless you use a different key for each product.
8. If you are running the installer as a non-root user, specify the root password so that the agent can be restarted automatically.
9. Specify an operating system or an application support package to install. This list varies depending on your operating system and on whether any IBM Tivoli Monitoring components are installed. Accept the default or choose your operating system from the list.
10. Select **All of the above** from the options listed below.
 - IBM Tivoli Network Manager
 - Tivoli Enterprise Services User Interface
 - All of the above
11. When asked for additional products, choose **No** to exit the installation.

What to do next

Configure an instance of the agent for each domain.

Configuring the monitoring agent

You only install the agent once, but you configure one instance of the agent for each Network Manager domain.

About this task

See the IBM Tivoli Monitoring documentation for information about configuring the monitoring agent using the `itmcmd config`; the Manage Tivoli Monitoring Services user interface; or the Tivoli Enterprise Portal.

To configure the agent from the command line, complete the following steps:

Procedure

1. Run the following command to instantiate an instance of the agent:

```
$ITMHOME/bin/itmcmd config -A np
```

Where *ITMHOME* is the installation path of the agent.

2. Choose a name for each monitoring agent and enter the name in the **Instance name** field. Define a new agent instance for each Network Manager domain.

The instance name can be any unique meaningful name. For example, the instance name of each agent could include the name of the poller with which it is associated.

Note:

If you use multiple pollers, and you want to monitor the pollers individually using the Availability workspace, you must define a unique name for the pollers by editing the `knp.ref` file. For more information on how to edit the `knp.ref` file to name the pollers, see the following technote: <http://www-01.ibm.com/support/docview.wss?uid=swg21600387>

3. Specify a value for **NCHOME Path**. The default is `/opt/IBM/netcool/core`.
4. Specify a Network Manager domain name. The default is `NCOMS`.
5. Specify a value for the Network Manager poller name. If you leave this field blank, the agent is mapped to the default poller. If you have more than one poller, you must specify a value. This field is empty if you are not using distributed polling.
6. Specify a username for the Network Manager OQL database. By default, the username is `admin`.
7. Specify a username for the Network Manager OQL database. This password is empty by default.
8. Specify a refresh interval in minutes. The default value is 10. This number specifies the maximum amount of time, in minutes, before data is cached. If you specify a value of zero, then a database query is done each time data is requested. Otherwise, a database query is done at the specified time interval. Specifying a low number can impact performance for the Network Manager server because some queries require a significant amount of processing time.
9. Select **Yes** to connect the agent to a Tivoli Enterprise Monitoring Server.
10. Specify the DNS name for the Tivoli Enterprise Monitoring Server when you are prompted for the Tivoli Enterprise Monitoring Server Host Name.

Note: Do not specify the name of the Tivoli Enterprise Monitoring Server. Specify the DNS name.

11. Unless your IBM Tivoli Monitoring administrator gives you different settings, accept the defaults for the following options:
 - Network Protocol. The default is `ip.pipe`.
 - Choose the next protocol from the following options:
 - `sna`
 - `ip.spip`
 - 0 (none)
 - Network Protocol 2 (The default value is 0)
 - IP.PIPE Port Number (The default value is: 1918)
 - `KDC_PARTITION` (The default value is null.)
 - Configure connection for a secondary TEMS? [1=YES, 2=NO] (The default value is 2.)
 - Optional Primary Network Name (The default value is 0 or none.)
12. Optional: For a non-root installation only, you must complete the following extra tasks:
 - a) Specify the root password to update the automatic restart scripts.
 - b) As the root user, run the `ITMHOME/bin/SetPerm` from the directory where IBM Tivoli Monitoring is installed.

c) As the root user, run the `ITMHOME/bin/UpdateAutoRun.sh` script from the directory where IBM Tivoli Monitoring is installed.

If you are running the `SetPerm` utility on AIX 6.X or 7.X, you must select the AIX 5.X options.

13. Repeat this whole procedure to configure an instance of the agent for each Network Manager domain. Use different poller names for each agent instance.

What to do next

After you have configured IBM Tivoli Monitoring for IBM Tivoli Network Manager IP Edition, you can enable the Health views and launch in context from Tivoli Enterprise Portal.

Starting the monitoring agent

Use a command to start the monitoring agent.

Before you begin

If you are using Red Hat Enterprise Linux 7 or SuSE Linux Enterprise Server 12, run the following command before installing, uninstalling, starting, or stopping the monitoring agent:

```
setarch $(uname -m) --uname-2.6
```

About this task

When you install the monitoring agent, the files used to start the agent when the system reboots are automatically set up. The file used to restart the agent is `/etc/init.d/ITMAgents2`. If you install another agent, the 2 is incremented; for example, the next agent installed would be `ITMAgents3`.

Run the following command to start the agent: `./ITMAgents2`

Accessing discovery data from dNCIM

You can take advantage of post-discovery dNCIM broadcasts to retrieve updates to the network topology after each discovery completes. Internal Network Manager processes read this information on completion of a discovery. You can also configure third-party systems (Tivoli-based or external) to access this topology data so that they have the latest topology updates.

About this task

Examples of such third-party systems that you might want to configure to read dNCIM data include the following:

- TADDM can use this data in order to feed its application discovery. The data from dNCIM tells TADDM which hosts are present on the network, which is a first step to discovering the applications on those hosts.
- IBM Director can use this data to support the discovery of storage devices
- An asset database can use this data to upload its asset information.
- A security system can use the data to identify possible intrusions.

Getting data from dNCIM rather than using the DLA differs in the following ways.

- The data is in a different format to the DLA.
- The dNCIM data has not yet been sent to the Topology Manager, `ncp_model`, so the data is not consolidated with previous discoveries:
- The data is lighter weight than the data that can be retrieved using the DLA.
- The dNCIM broadcasts have the same format as the NCIM broadcasts transmitted by `ncp_model`, and the NCIM cache files.

To configure third-party systems to access discovery data from dNCIM, you must write a script to configure the Java or Perl API to listen for messages with the DNCIM2NCIM subject on the message bus. For information on the format of dNCIM broadcasts, see the *IBM Tivoli Network Manager Reference*.

Chapter 8. Upgrading and migrating

Upgrading from a previous version of Network Manager involves installing the latest version and migrating your existing configurations and customizations.

About upgrading

Understand what options are available to you to upgrade, and what the upgrade involves.

Upgrade paths and limitations

You can upgrade to Network Manager V4.2 from certain previous versions, with limitations.

You can migrate from any of the following versions to Network Manager V4.2:

- V3.9 Fix Pack 3 or later
- V4.1
- V4.1.1

If you have a version of Network Manager prior to V3.9, upgrade to V3.9 Fixpack 3 before upgrading.

You can also use the migration procedure to copy one V4.2 installation to another server. The procedure for all of these versions is the same.

Note:

If you have IBM Netcool Operations Insight V1.2 or V1.3 installed and are upgrading to IBM Netcool Operations Insight V1.4, run IBM Installation Manager and uninstall the **Network Management Integration for OMNIBus 8.1** component before installing Network Manager V4.2.

The following limitations apply to upgrading:

- You can only migrate to a 64-bit server.
- Migrating from Windows systems is not supported.
- The source and target machines must use the same database type. The only exceptions are the following:
 - V3.9: migrating from the previously default Informix source to the default Db2 or an Oracle database in V4.2 on the target system is supported.
- 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.

Note: If you use Network Manager as part of a solution, you must also check the compatibility of the versions of all component products in the solution documentation. For example, if you use Netcool Operations Insight, check the *product and component version matrix* for your version of Netcool Operations Insight at <https://www.ibm.com/support/knowledgecenter/en/SSTPTP>.

Related tasks

Uninstalling Network Manager

If you want to completely remove the product, or to roll back to a previous version, you must use IBM Installation Manager. Uninstalling the product by removing files and directories causes problems when you reinstall components.

Default locations for different product versions

The different versions of Network Manager and related components use different directory structures and have configuration files in different locations.

If you are looking for a file or other system component that you expected to find based on the location on your old system, use the following table to determine where to find the item on Network Manager 4.2. As

a reference, the following table contains an overview of how the default location of configuration files has changed over the releases.

Table 11. Default locations of configuration files		
Item	Versions 3.9, 4.1, and 4.1.1	Version 4.2
NCHOME	/opt/IBM/tivoli/netcool	/opt/IBM/netcool/core
ITNMHOME	/opt/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.	/opt/IBM/netcool/core/precision Note: By default, PRECISION_HOME is set to the same location as ITNMHOME, but is used by other parts of the product.
TIPHOME	/opt/IBM/tivoli/tipv2	No longer applicable. Tivoli Integrated Portal has been replaced by Dashboard Application Services Hub
JazzSM_HOME	Not applicable	See the Jazz for Service Management Knowledge Center for details.
GUI properties files	ITNMHOME/profiles/ TIPProfile/etc/tnm	\$NMGUI_HOME/profile/etc/tnm/ Note: \$NMGUI_HOME is the location where the Network Manager GUI components are installed. By default, it is /opt/IBM/netcool/gui/precision_gui.
Dynamic view templates	ITNMHOME/profiles/ TIPProfile/etc/tnm/ dynamictemplates	\$NMGUI_HOME/profile/etc/tnm/ dynamictemplates/
Right-click menu and tool definition files	ITNMHOME/profiles/ TIPProfile/etc/tnm/menus	\$NMGUI_HOME/profile/etc/tnm/ menus/
	ITNMHOME/profiles/ TIPProfile/etc/tnm/tools	\$NMGUI_HOME/profile/etc/tnm/ tools/
GUI icon files	ITNMHOME/profiles/ TIPProfile/etc/tnm/resource	\$NMGUI_HOME/profile/etc/tnm/ resource/
WebTools configuration files	ITNMHOME/profiles/ TIPProfile/etc/tnm/tools	\$NMGUI_HOME/profile/etc/tnm/ tools/

What data is migrated

Network Manager migrates most files, and highlights files that you must migrate manually.

Files that have been changed can be classified in the following two ways.

Configuration changes

Standard settings for processes, discovery and monitoring configuration, and topology views can be migrated by following the directions in this document. The person who performs the migration must be the administrator or have a similar level of understanding of Network Manager. Configuration files are fully or partially migrated by the migration process. Any files that must be migrated manually are highlighted.

Customization changes

Network Manager can be extensively customized to add new capability or integrate with your existing environment. The following are some examples of configuration changes:

- Additional device support
- Additional data from devices and customer proprietary data sources for visualization and monitoring
- Modified logic for building connections within and between network devices, and collections for grouping devices
- Building sets of network views using the dynamic template API
- Event enrichment via the Event Gateway and `nco_p_ncpmonitor` probe rules file
- Right-click topology map tools using Webtools and other technologies
- Extending the Service Affecting Events system for other collections
- Integrations with other products, including LDAP and TADDM

All customization changes require some level of knowledge of the product data flow and APIs, plus programming skills. These same skills are required to successfully migrate the same customizations. You must also take account of any new logic changes that might require changes to the existing custom code.

Customization changes are not migrated automatically. The upgrade process highlights files that have changed and must be migrated manually.

Data that is not migrated

The following kinds of data can not be migrated:

- NCIM cache files are not migrated between different versions of Network Manager. NCIM cache files are copied from one installation to another only if you copy an existing V4.2 installation to another V4.2 installation.
- Discovery cache files
- Network topology is not migrated. You must run a new discovery on the target installation.

Data that is migrated

The following kinds of data are migrated.

- Configuration files.
- Network views.
- Discovery configuration data.
- Multiple domains. Your domains are automatically recreated, and the network views and monitoring policies are imported.
- Passwords and SNMP community names. This data is unencrypted, imported, and re-encrypted automatically.
- Poll policies and poll definitions.
- MIBs. The SNMP MIBs have been moved from the GUI server to the core components server in Network Manager 4.2.
- New or customized discovery collectors

Upgrading Network Manager

Complete the upgrading tasks in the order that they are given.

About this task

In these instructions, "source" server or installation refers to the Network Manager server or installation that you upgrade from. Usually, this version is a previous, older version.

The "target" server or installation refers to the Network Manager server or installation that you upgrade to. Usually, this version is the current version, 4.2.

Important: A Fix Pack upgrade deploys a new .war file for each Web application such as Network Views, Structure Browser, geographic views, and so on. Any modified files in the same directory as the WAR file are overwritten. You must back up any changes that you have made to files within the WAR file deployment location.

Preparing to upgrade

You must prepare the target systems before you begin the upgrade.

About this task

To prepare for upgrade, complete the following tasks:

Procedure

1. Install the Network Manager core components.
2. Start the Network Manager core components.
Do not perform any further configuration of the primary domain as this would limit automatic configuration migration.
3. Install the Network Manager GUI components.
4. Ensure that you can log into the Network Manager GUI.
5. Recreate all the Network Manager users from the source installation on the target installation. Create the users in the appropriate repository: LDAP or ObjectServer. If there were any users created in the Tivoli Integrated Portal, create these users again. Network Manager 4.2 does not use the Tivoli Integrated Portal. Note the user names and passwords. You need these credentials when you migrate user roles.
6. Optional: If you are migrating from an installation of Network Manager that is integrated with IBM Tivoli Netcool Configuration Manager, export your custom reports before you upgrade. If you do not export your custom reports, they might be overwritten during the upgrade. Refer to the information on *Exporting custom reports* for your version of Netcool Configuration Manager at: <http://www.ibm.com/support/knowledgecenter/SS7UH9/welcome>.
7. Do not start a discovery or begin to work with Network Manager. Begin the upgrade.

Updating the database

You must identify any customizations that you made to the NCIM topology database and update the new database with those customizations.

Before you begin

As part of installing the target system, you must install the new database and run the Network Manager create database schema scripts to set up the tables and schemas.

Note: You only need to run `ncp_ncim_diff.pl` script if you have customized changes in your source database.

Ensure that the DbLogins.*DOMAIN*.cfg files from the previous installation are available. These files contain the information for connecting to your NCIM database.

About this task

To update the topology database schema, complete the following steps:

Procedure

1. Log in to your source Network Manager installation.
2. Change to the \$NCHOME/precision/scripts/perl/scripts directory and run the following command:

```
./ncp_ncim_diff.pl -domain DOMAIN -password NCIM_database_password
```

Where *DOMAIN* is required to identify a DbLogins.*DOMAIN*.cfg file that contains the options for connecting to your NCIM database. This command reports on all domains and only needs to be run once.

For more information on the ncp_ncim_diff.pl Perl script see *IBM Tivoli Network Manager IP Edition Administration Guide*.

The script reports the differences between your NCIM database schema and the default NCIM database schema for your version of Network Manager.

3. Manually update the NCIM topology database schema with the customizations reported by the script.

The script might report new tables that were introduced with a Fix Pack. These changes are already present in the new system and do not need to be migrated. Take care when applying customizations to the new NCIM schema because table names and field names might change between versions.

Related tasks

[Installing and configuring a topology database](#)

Your database administrator must install and configure a supported topology database before you can install Network Manager.

Migrating the core components

Migrate the core components by exporting data from the source server and importing it into the target server. Start and stop all processes, import the data, define multiple pollers, scope all poll policies, and complete any necessary manual steps.

About this task

If the core components and GUI components are on the same server, you must still migrate them separately by following the appropriate steps.

Complete the following steps to migrate the core components.

Procedure

1. On the target server where the core components are installed, run the following script:

```
$ITNMHOME/install/scripts/makeExportPackageCore
```

The script creates a package that contains the scripts that you use to export data from the source installation. The package is named ExportPackageCore.tar.

2. Copy the ExportPackageCore.tar file to a temporary location on the source server where the core components are installed.

Note: The location must not be in or contained by the installation directory \$NCHOME.

3. Decompress the ExportPackageCore.tar file.

4. In the `scripts` directory that was created by decompressing the file, run the `nmExport` script. Provide the required information and choose a location for the export file to be saved.

Restriction: You must run the script as the same user that installed the product.

The script creates a `.pkg` file containing discovery configuration data, network views, poll policies and definitions, other configuration files, and log files containing information about the successful export. If the export is unsuccessful, log files are saved to the `/itnmExportLogs/` directory in your home directory.

5. Copy the `.pkg` that was created file to the target server.
6. On the target server, ensure that all Network Manager processes are running by using the following command:

```
itnm_start ncp -domain DOMAIN
```

Run this command for all domains that exist in the target server. Specify the domain name explicitly each time.

7. Now stop all Network Manager processes by using the following command:

```
itnm_stop ncp -domain DOMAIN
```

Run this command for all domains. Specify the domain name explicitly each time. Starting and stopping the processes ensures that the appropriate database tables are populated.

If you have failover configured, stop all domains on the backup server as well.

8. On the target server, go to the location `$NCHOME/precision/install/data/` and extract the package `ExportPackageCore.tar`.
9. As the same user that installed the product, run the `nmImport` script from the `scripts` subdirectory.
10. Provide the information required by the script when you are prompted. Provide the path to the `.pkg` file that contains the customization data that you exported from the source server.
11. Optional: If you are migrating your NCIM topology database to an Oracle database that uses Oracle clustering technology, then provide the relevant Oracle information, paying attention to the following prompts:
 - a) After the prompt that lists the current database server settings, answer `n` to the following question:

```
Are the server settings correct [y|n]?
```

- b) Answer `y` to the following question:

```
Is this an Oracle service name [y|n] ?
```

- c) When the script displays the current database server settings, check that the following setting is displayed: `oracleService = 1`.
12. When prompted if you want to allocate new entity IDs, which are unique device identifiers, during the import, answer `N` in order to preserve links with other products that use Network Manager data such as TADDM, IBM Tivoli Business Service Manager, IBM Control Desk.

If you already have topology data in the target installation, for example from a previous import or network discovery, you cannot preserve the previous entity IDs and must answer `Y`. If you answer `N` the script returns an error, stating that entity data already exists.

If you have a domain on the target system that has the same name as on the source system, ensure the domain on the target system does not contain topology data. Domain names cannot be changed during the migration process.

13. Review your network views for duplicates. Duplicate network views can be created if, for example, a discovery was run before the upgrade. You can delete duplicate views, or move sections of views into the existing views.

14. Change the default domain, if desired, by setting the `PRECISION_DOMAIN` environment variable to the desired default domain

The default domain is the domain that is created at installation. When the control scripts, for example, `itnm_start`, are used without a `-domain` argument then the actions specified in the scripts are applied to the default domain.

Results

The import script imports the configuration data from your source installation to the target installation. The following log files are written to the `$NCHOME/log/precision` directory: `ITNMDataImport.log`, `get_policies.domain name.log`, and `ITNMImportNetworkViews.log`.

What to do next

Now you must review the results of the import and perform any necessary manual migration steps.

Migrating polling

Migrate poll policies and, if applicable, multiple pollers.

About this task

You must define a scope for each poll policy that you want to use. Ensure that all policies are associated with the appropriate named poller.

Procedure

1. Configure the poll policies on the target installation by completing the following steps for each poll policy that you migrated:
 - a) Log into the Web applications on your new installation.
 - b) Make sure the network views exist for your system. Click the **Incident** icon and select **Network Availability > Network Views**.
 - c) Click the **Administration** icon and select **Network > Network Polling**.
 - d) Select a policy that was available on the source 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.
 - e) If necessary, reassign the policy to the appropriate named poller.
 - f) Select the **Network Views** tab and select the network view that was used on the source system.
 - g) Select the **Device Filter** tab and set up the filter as it was on the source system.
 - h) Edit each poll definition and ensure that the Class filter and Interface filter are set as you expect. Classes might have been added or removed between versions.
2. Optional: Policies for a single poller on the source system are automatically assigned to the new **nep_poller_default** poller on the target installation. If you used multiple pollers on the source installation, configure multiple pollers on the target installation by completing the following steps:
 - a) Edit the `CtrlServices.cfg` file on the target installation with the entries from the source system.
If you use the new **nep_poller_default** poller, any poll policies default to that poller automatically.
 - b) Repeat for each domain on the target installation.

Migrating core components files manually

Some files that contain configuration changes cannot be migrated automatically. Review the suggested list of files and migrate changes manually.

About this task

The migration process updates as much of the configuration on the target system as possible. Changes are handled in the following ways:

- If a configuration file was changed from the default on the source system, that file is automatically copied over the equivalent file on the target system. The migration process applies your changes automatically, as long as there are no conflicts.
- If a configuration file was changed from the default on the source system, but the default for the version of the product on the target system is different from the source system, there is a conflict between your change and a change in the product. If the difference can not be automatically resolved by the migration scripts, the file is flagged as needing review.
- If a configuration file was not changed on the source system, it is not migrated.
- If a configuration file is no longer needed in the target installation, it is not migrated.

To migrate files manually, complete the following tasks:

Procedure

1. Review the `$NCHOME/log/precision/NMCoreFilesForManualReview.txt` log file. For example, `/opt/IBM/netcool/log/precision/NMCoreFilesForManualReview.txt`. This file has an entry for each item that requires attention. If an entry says that a file requires manual migration steps, you must review each file and decide how to incorporate the differences into the files on the target installation.
2. Optional: Review the `NMCoreFilesMigrated.txt` log file to see all files that were migrated, and which files were not migrated. It is likely that no action is needed for files that were not migrated. Some files do not need to be migrated. If you think that such a file contains important configuration information that you want to preserve, review the file. Review the `$NCHOME/log/precision/NMCoreConfigFileAutoMigrationReport.txt` log file for extra information about files that could not be migrated successfully.
3. For files that need manual migration, locate the appropriate versions of the files to review.
 - For files that were changed by a user, compare the original version from the source installation with the changed version from the source installation. These files are copied to the target server for convenience. The locations differ by file type and are listed out in the `NMCoreFilesForManualReview.txt` file.
 - For files that were changed by IBM between versions, compare the version from the source installation with the version from the target installation. Files from the source server are copied to the target server for convenience. The locations differ by file type and are listed out in the `NMCoreFilesForManualReview.txt` file.
 - For files that were changed by a user and by IBM between versions, compare all three versions. Files from the source server are copied to the target server for convenience. The locations differ by file type and are listed out in the `NMCoreFilesForManualReview.txt` file.
4. Run the **ncp_mib** utility if you customized any MIBs on the source system.
Custom MIBs from the source installation are copied into the `$NCHOME/precision/mibs/` directory. MIB files moved from the GUI to the core components server in V4.2.
5. Review the `DbEntityDetails.cfg` file and replace `&ExtraInfo` with `&m_ExtraInfo`.
This change is necessary due to database changes between V3.9 and V4.1 and later.
6. Review the domain-specific `DbLogins.cfg` files on the target installation with the new database connection details for the target installation.

The migration scripts create domain-specific `DbLogins.cfg` files for each domain from the source installation.

7. Optional: If you used discovery collectors on the source installation, copy the `.cfg` and `.drv` files to the target installation and ensure the collectors are set up correctly.
8. Optional: If you created new discovery collectors on the source installation, refer to the *EMS Collector Developer Guide* for migration instructions.
9. If you used seed files for discovery on the source server, copy the seed files to the equivalent location on the target server. When you run a discovery, update the seed file reference in the **Seed** tab of the **Discovery Configuration GUI**.
10. If you used DNS files for discovery on the source server, copy the files to the equivalent location on the target server. When you run a discovery, update the DNS file reference in the **DNS** tab of the **Discovery Configuration GUI**.
11. Review the list of files that are not migrated in [“Core components file reference” on page 137](#) and decide if any customization changes need to be migrated.
12. Review the changes you made to the `NcoGateInserts.DOMAIN.cfg` files, which are deprecated in Network Manager 4.2, and migrate the changes:
 - a) Go to the directory that is listed for the `NcoGateInserts.DOMAIN.cfg` entry in the `$NCHOME/log/precision/NMCoreFilesForManualReview.txt` file.
 - b) Locate the `NcoGateInserts.DOMAIN.cfg` files for each domain for which you have made customizations.
 - c) Locate your customizations. You only need to migrate customizations that you made yourself. All the default customizations were moved from the `NcoGateInserts.cfg` file to the Probe rules in Netcool/OMNIbus Knowledge Library V4.4.3.
 - d) On the server where the Netcool/OMNIbus Knowledge Library is installed, locate the rules file that corresponds to the eventID of the type of events that you want to customize. For vendor-specific rules, the rules files are placed under the vendor directory, for example, `include-snmpttrap/cisco`.
 - e) Locate the appropriate rules file with the suffix `user.include.rules`. For example, `/include-snmpttrap/adtran/adtran-ADTRAN-ACTDAXL3-MIB.user.include.snmpttrap.rules`. Putting your customizations in a separate file makes it easier to identify and back them up later.
 - f) Edit the file and locate the section that corresponds to the type of trap that you want to customize. For example, to override the default rules for `adACTDAXL3systemHdwFailureClear` trap, add the customized rules under the following section:

```
case "906": ### adACTDAXL3systemHdwFailureClear
```

- g) Set the `@NmosEventManager` field using the following format: *event map name.precedence value*.

For example:

```
@NmosEventManager = "LinkDownIfIndex.910"
```

13. Optional: If you want to review the list of files that were migrated successfully, review the files listed in `NCHOME/log/precision/NMCoreFilesMigrated.txt`.

Core components file reference

The core components migration scripts process files within their scope.

Files within the scope of the core components migration scripts

The core components migration scripts examine the configuration files in the following directories and process them as described in [“Migrating core components files manually” on page 136](#).

- `$NCHOME/precision/aoc/*.aoc`
- `$NCHOME/precision/disco/stitchers/*.stch`

- \$NCHOME/precision/disco/stitchers/DNCIM/*agnt
- \$NCHOME/precision/disco/agents/*
- \$NCHOME/precision/adapters/ncp_dla/ncp_dla.properties.*
- \$NCHOME/precision/eventGateway/stitchers/*
- \$NCHOME/probes/*platform*/nco_p_ncpmonitor.rules*
- \$NCHOME/precision/mibs/*.mib
- \$NCHOME/etc/precision/*.cfg
- \$NCHOME/precision/storm/conf/*.cfg, *.conf, *.yaml, *.properties

Files that are not migrated by the core components migration scripts

The following files are not migrated by the migration scripts:

- \$NCHOME/precision/scripts/webtools.

You must manually save these files on the source installation, and reimplement them on the target installation. An example of such customization is the settings to launch into IBM Tivoli Application Dependency Discovery Manager.

- \$NCHOME/etc/omni.dat.

These settings are not needed because connection details are set during installation of the target system.

- \$NCHOME/etc/interfaces.<arch>
- \$NCHOME/precision/collectors. If you use discovery collectors, you must manually migrate any configuration changes for the collector.
- \$NCHOME/etc/precision/ConfigSchema.cfg
- \$NCHOME/etc/precision/DbLogins.cfg
- \$NCHOME/etc/precision/DiscoDncimDb.cfg. This file is obsolete in V4.2.
- \$NCHOME/etc/precision/DncimDbEntityDetail.cfg. This file is obsolete in V4.2.
- \$NCHOME/etc/precision/MibDbLogin.cfg
- \$NCHOME/etc/precision/NcoLogin.cfg
- \$NCHOME/etc/precision/ServiceData.cfg

Migrating the GUI components

Migrate the GUI components by exporting the data from the source installation to the target installation. Import the data, assign users to groups, and review the `NMGUIFilesForManualReview.txt` file for any necessary manual steps.

About this task

Migrate data for the Network Manager GUI using the instructions below.

For instructions about migrating Web GUI, refer to the information for your version of Web GUI at: <http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html>.

Procedure

1. On the target server where the GUI components are installed, ensure that the environment variables for Network Manager are set by running the environment script. The environment script is in the following location: `installation_directory/nmgui_profile.sh`, for example, `/opt/IBM/netcool/nmgui_profile.sh`.
2. On the target server where the GUI components are installed, run the following command:

```
$NMGUI_HOME/install/scripts/makeExportPackageGUI -j $JazzSM_HOME -n $NMGUI_HOME
```

Where:

- `$NMGUI_HOME` is the environment variable that defines where the Network Manager GUI is installed. By default, this is `/opt/IBM/netcool/gui/precision_gui`.
- `$JazzSM_HOME` is the Jazz for Service Management installation directory. By default, this location is `/opt/IBM/JazzSM`.

For example, using the default install locations, run the following command:

```
/opt/IBM/netcool/gui/precision_gui/install/scripts/makeExportPackageGUI -j  
/opt/IBM/JazzSM -n /opt/IBM/netcool/gui/precision_gui
```

The script creates a package containing the scripts that you use to export data from the source installation. The package is named `ExportPackageGUI.tar`.

3. Copy the `ExportPackageGUI.tar` file to a temporary location on the source server where the GUI components are installed. If you have GUI components installed on multiple servers, you only need to export the data from one of the servers, unless you have set them up differently.

Note: The location must not be in or contained by the installation directory.

4. On the source server, decompress the `ExportPackageGUI.tar` file.
5. Ensure that the environment variables for Network Manager are set on the source server, by running the appropriate environment script.

In Network Manager 4.2, there are two environment scripts.

On the server where the Network Manager GUI components are installed, the script is `installation_directory/nmgui_profile.sh`, for example, `/opt/IBM/netcool/nmgui_profile.sh`.

On the server where the Network Manager core components are installed, the environment script is `installation_directory/netcool/core/env.sh`.

In previous versions of Network Manager, the script is stored in the `installation_directory/netcool` directory.

6. The `ExportPackageGUI.tar` file contains a file called `Preupgrade.tar`. Extract the `Preupgrade.tar` file to the following location on the source server: `$TIPHOME/profiles/TIPProfile`.
7. In the `scripts` directory that was created by decompressing the file, run the `nmGuiExport` script using the following command:

```
nmGuiExport -u tipadmin|smadmin -p password
```

Where:

- `-u` takes either the Tivoli Integrated Portal administrative user name (`tipadmin` by default) for versions of Network Manager prior to V4.2, or the Jazz for Service Management administrative user name (`smadmin` by default).
- `password` is the password for that user.

Restriction: You must run the script as the same user that installed the product.

The script creates a `data.zip` file in one of the following directories: `$TIPHOME/profiles/TIPProfile/output/` or `$JazzSM_HOME/ui/upgrade/data/`. The file contains configuration data, user roles, and custom Tivoli Integrated Portal pages, views, and roles. Any errors are saved to one of the following directories: `$TIPHOME/profiles/TIPProfile/logs/tipcli.log` or `$JazzSM_HOME/ui/logs/consolecli.log`.

8. Create the `$JazzSM_HOME/ui/input/` directory on the target GUI server and copy the `data.zip` export file into it. If you are installing multiple Dashboard Application Services Hub servers, copy the export file to each server.

9. Ensure that Dashboard Application Services Hub is running.
10. Ensure that the environment variables for Network Manager are set on the target server, by running the environment script `installation_directory/netcool/gui/precision_gui/nmgui_profile.sh`.
11. In the scripts directory on the target server, run the nmGuiImport script using the following command:

```
nmGuiImport -u smadmin -p password [ -f path_to_zip_file ]
```

Where:

- `-u` takes the Jazz for Service Management administrative user name (smadmin by default).
- `password` is the password for that user.
- `path_to_zip_file` is the path to the data.zip export file that contains the GUI data. If the `-f` option is not specified, the script searches for the data.zip file in the default location: `$JazzSM_HOME/ui/input/`.

Restriction: You must run the script as the same user that installed the product.

The exported GUI data is imported into the new installation. If the same users exist on the target Dashboard Application Services Hub installation as on the source installation, the same user roles are added to them. Results of the import are logged to the following file: `$JazzSM_HOME/ui/logs/consolecli.log`

12. Manually add users to the appropriate user groups on your new system. The import of GUI data does not include user group membership data.
13. Review any custom pages from the source installation that contain the **Event Viewer**. Replace every **Event Viewer** widget with an **Event Viewer** widget.

The **Event Viewer** widget is not available in Network Manager V4.2. For information on how to edit pages, refer to the *Developing custom dashboards* topic within the *IBM Tivoli Network Manager User Guide*.

14. If you used the Discovery Library Adapter on the source server, migrate the settings.
 - a) Go to the location on the source server where the DLA properties are stored. For versions of Network Manager prior to V4.2, the location is `$NCHOME/precision/adapters/ncp_dla/`. For Network Manager V4.2, the location is `$NMGUI_HOME/adapters/ncp_dla`. Locate the DLA properties files. Each domain has an `ncp_dla.properties.domain_name` file. Use the DLA properties files for each domain to recreate the same DLA settings on your new installation.
 - b) Go to `$NMGUI_HOME/adapters/ncp_dla`.
 - c) 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`.
 - d) Open the DLA properties file for each domain and make the same settings in the new respective domain-specific file as in the previous `ncp_dla.properties.domain_name` file, thus recreating the DLA file for each respective domain on the new system.

Restriction: 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.

15. Review the results of the import in the `NMGUIFilesForManualReview.txt` file and perform any necessary manual migration steps.

Related reference

[Supported operating systems](#)

Network Manager is supported on the following operating systems.

Migrating GUI components files manually

Some files that contain configuration changes cannot be migrated automatically. Review the suggested list of files and migrate changes manually.

About this task

The migration process updates as much of the configuration on the target system as possible. Changes are handled in the following ways:

- If a configuration file was changed from the default on the source system, that file is automatically copied over the equivalent file on the target system. The migration process applies your changes automatically, as long as there are no conflicts.
- If a configuration file was changed from the default on the source system, but the default for the version of the product on the target system is different from the source system, there is a conflict between your change and a change in the product. If the difference can not be automatically resolved by the migration scripts, the file is flagged as needing review.
- If a configuration file was not changed on the source system, it is not migrated.
- If a configuration file is no longer needed in the target installation, it is not migrated.

Procedure

1. Review the `$NMGUI_HOME/./log/install/NMGUIFilesForManualReview.txt` log file, which is located in the GUI components installation directory. For example, `/opt/IBM/netcool/gui/log/install/NMGUIFilesForManualReview.txt`. This file has an entry for each item that requires attention.
 - a) If an entry says that a file was merged automatically, no action is needed.
 - b) If an entry says that a file was not migrated, it is likely that no action is needed. Some files do not need to be migrated. If you think that such a file contains important configuration information that you want to preserve, review the file.

Which files are migrated is controlled by the configuration file `$NMGUI_HOME/integration/properties/mergeDefinition.json`. You do not need to edit this file.
 - c) If an entry says that a file requires manual migration steps, you must review each file and decide how to incorporate the differences into the files on the target installation.
2. For files that need manual migration, locate the appropriate versions of the files to review.
 - For files that were changed by a user, compare the original version from the source installation with the changed version from the source installation. These files are copied to the target server for convenience. The locations differ by file type and are listed out in the `NMGUIFilesForManualReview.txt` file.
 - For files that were changed by IBM between versions, compare the version from the source installation with the version from the target installation. Files from the source server are copied to the target server for convenience. The locations differ by file type and are listed out in the `NMGUIFilesForManualReview.txt` file.
 - For files that were changed by a user and by IBM between versions, compare all three versions. Files from the source server are copied to the target server for convenience. The locations differ by file type and are listed out in the `NMGUIFilesForManualReview.txt` file.

GUI file reference

The GUI migration scripts process some files and ignore others.

Files within the scope of the GUI migration scripts

The GUI migration scripts examine the configuration files in the following directories and process them as described in [“Migrating GUI components files manually” on page 141](#).

- \$NMGUI_HOME/profile/etc/tnm/autoprovision/*
- \$NMGUI_HOME/profile/etc/tnm/dynamictemplates/*
- \$NMGUI_HOME/profile/etc/tnm/*
- \$NMGUI_HOME/profile/etc/tnm/menus/*
- \$NMGUI_HOME/profile/etc/tnm/tools/*
- \$NMGUI_HOME/profile/etc/tnm/resource/*

Files that are ignored by the GUI migration scripts

The following GUI files are ignored by the migration scripts:

- tnm.properties
- ncpolldata.properties. This file is obsolete in Network Manager 4.2.
- etc/tnm/locale/*

Migrating network topology

To ensure that you have network topology on the target system, run a full discovery. Optionally, migrate managed status for devices, and any custom, manually created topology.

About this task

To migrate network topology, perform the following steps for each discovery domain:

Procedure

1. Stop and start all Network Manager processes on the target installation to ensure that the domain is updated with customization changes.
2. Run a full discovery on the target installation.
3. If you created manual topology on your source installation, complete all the following steps. If you did not manually add or remove any devices to your network topology on your source installation, skip to step 7.
4. On your new installation, navigate to the following location `$NCHOME/var/precision/export/manualtopology`.
This directory contains XML files listing the devices and connections manually added to each domain on your previous system. There is one file for each domain. Each file is named as follows:

```
ManualTopology.DOMAIN.xml
```

Where *DOMAIN* is the name of the relevant domain.

5. Open the XML file for the domain you want to update with manually created topology data.
6. Apply the changes to your new discovery using the topology management wizards within the **Network Hop View**.
 - You can manually add devices from any **Network Hop View** window.

- To manually add connections, the best practice is to point the **Network Hop View** window to the a-end device (specified using the `fromdevice` attribute in the connection) and create a manual connection to the b-end device (specified using the `todevice` attribute).

For more information on editing network topology using the topology management wizards, see the *IBM Tivoli Network Manager User Guide*.

Perform the following steps to use the topology management wizards to add the devices and connections in the example XML code snippet to the topology.

- a) Click the **Incident** icon and select **Network Availability > Network Hop View**.
- b) Select a network domain from the **Domain** drop-down list corresponding to line 2 in the example XML code below.
- c) Add all the devices specified in the XML file by performing the following steps:
 - i) Right click anywhere within **Network Hop View** and then click **Topology Management > Add Device**.
 - ii) In the **Add Device** wizard, add the device `aog.dom39.1` by specifying the attributes listed in lines 21 to 35 of the XML file.
Note: Be aware of the following:
 - Attributes in the XML file appear in alphabetical order. This is different to the order in which they are requested by the GUI.
 - The XML file might not show all attributes requested by the GUI for a given device or connection. Where attributes are missing, do not enter any values in the GUI.
 Complete all the wizard screens and click **Finish**, followed by **Close**. The device you added appears in the **Network Hop View**. For more information on editing network topology using the topology management wizards, see the *IBM Tivoli Network Manager User Guide*
 - iii) Right click anywhere within **Network Hop View**, then click **Topology Management > Add Device** and add the device `aog.dom39.2` by specifying the attributes listed in lines 36 to 42 of the XML file. Complete all the wizard screens and click **Finish**, followed by **Close**. The device you added appears in the **Network Hop View**.
 - iv) Right click anywhere within **Network Hop View**, then click **Topology Management > Add Device** and add the device `aog.dom39.3` by specifying the attributes listed in lines 43 to 48 of the XML file. Complete all the wizard screens and click **Finish**, followed by **Close**. The device you added appears in the **Network Hop View**.
- d) Add all the connections specified in the XML file by performing the following steps:
 - i) In the **Network Hop View**, navigate to a hop view that contains the device `aog.dom39.1`. For more information on finding device in the **Network Hop View**, see the *IBM Tivoli Network Manager User Guide*
 - ii) Right click device `aog.dom39.1` and click **Topology Management > Add Connection**.
 - iii) In the **Add Connection** wizard, add a connection from device `aog.dom39.1` to device `aog.dom39.2` by specifying the attributes listed in lines 4 to 8 of the XML file. Complete all the wizard screens and click **Finish**, followed by **Recenter & Close**. The connection you added appears in the **Network Hop View**. For more information on editing network topology using the topology management wizards, see the *IBM Tivoli Network Manager User Guide*
 - iv) In the **Network Hop View**, ensure that you are in a hop view that contains the device `aog.dom39.2`, then right click device `aog.dom39.2` and click **Topology Management > Add Connection**. Add a connection from device `aog.dom39.2` to interface [`GigabitEthernet0/1/0/1`] on device `172.20.1.3` by specifying the attributes listed in lines 9 to 13 of the XML file. Complete all the wizard screens and click **Finish**, followed by **Recenter & Close**. The connection you added appears in the **Network Hop View**.
 - v) In the **Network Hop View**, ensure that you are in a hop view that contains the device `172.20.1.3`, then right click device `172.20.1.3` and click **Topology Management > Add Connection**. Add a connection from interface [`Null0`] on device `172.20.1.3` to interface [`Nu0`]

on device 172.20.3.3 by specifying the attributes listed in lines 14 to 20 of the XML file.

Complete all the wizard screens and click **Finish**, followed by **Recenter & Close**. The connection you added appears in the **Network Hop View**.

7. If you had any devices on your source installation that were unmanaged, complete the following steps for each domain. Unmanaged devices are not polled by Network Manager and not included in RCA. If all your devices were managed, then you do not need to complete the following steps.
8. On the target installation, change to the following directory: `$NCHOME/precision/bin`
9. Run the `UnmanageNode.pl` script for the domain you want to update with managed status data.

Use a command similar to the following:

```
ncp_perl UnmanageNode.pl -domain DOMAIN_NAME -user ncim -pwd password
-noMainNodeLookup -file
$NCHOME/var/precision/export/managedstatus/UnmanagedEntities.DOMAIN_NAME.dat
```

Where:

- `DOMAIN_NAME` is the domain you are updating with managed status data.
- `password` is the password for the ncim user.
- The `.dat` file is a list of unmanaged entities that was generated by the export process. There is one list for each domain.

For more information on the `UnmanageNode` script, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

The script outputs the names of the main nodes and interfaces that were placed into unmanaged status. For example:

```
'aaa-11-12345.core.test.lab[ Lo0 ]' unmanaged.
'bbb-22-12345.core.eu.test.lab' unmanaged.
```

Adding a manually added device and connection to the network topology

The following example shows how to add a device and how to add a connection using an XML code snippet from an XML file produced by the import script. The XML code snippet below represents three manually added devices, and three manually added connections.

Note: Tag entries for connections appear before entries for devices in the XML file. However, when reapplying the manual topology using the Topology Editor, you must first add all of the devices specified in the file, and subsequently add the connections.

Table 12. XML code snippet from a manual topology file

```

1  <?xml version='1.0' standalone='yes'?>
2  <ManualTopology domain="DOMAIN_39"
3      version="3.9" >
4      <Connection connectivity="Layer 3 Meshed Topology"
5          fromdevice="aog.dom39.1"
6          reason="reas"
7          speed="1111"
8          todevice="aog.dom39.2" />
9      <Connection connectivity="Layer 3 Meshed Topology"
10         fromdevice="aog.dom39.2"
11         reason=""
12         todevice="172.20.1.3"
13         tointerface="[ GigabitEthernet0/1/0/1 ]" />
14      <Connection connectivity="Layer 2 Topology"
15         fromdevice="172.20.1.3"
16         frominterface="[ Null0 ]"
17         reason=""
18         speed="2345"
19         todevice="172.20.3.3"
20         tointerface="[ Nu0 ]" />
21      <Device entityname="aog.dom39.1"
22         accessipaddress="192.168.11.1"
23         accessprotocol="IPv4"
24         classname="Cisco"
25         description="aog.dom39.1 desc"
26         displaylabel="aog.dom39.1"
27         ipforwarding="forwarding"
28         modelname="aog.dom39.1 modelname"
29         reason="aog.dom39.1 reason"
30         serialnumber="ser.123"
31         syscontact="aog.dom39.1 syscont"
32         sysdescr="aog.dom39.1 sysdesc"
33         syslocation="aog.dom39.1 sysloc"
34         sysname="aog.dom39.1 sysname"
35         typename="Chassis" />
36      <Device entityname="aog.dom39.2"
37         accessipaddress="192.168.11.2"
38         accessprotocol="IPv4"
39         classname="Cisco"
40         displaylabel="aog.dom39.2"
41         reason=""
42         typename="Chassis" />
43      <Device entityname="aog.dom39.3"
44         accessprotocol="IPv4"
45         classname="Cisco"
46         displaylabel="aog.dom39.3"
47         reason=""
48         typename="Chassis" />
49  </ManualTopology>

```

The following table summarizes the elements and attributes in this XML code snippet:

Table 13. Description of the XML code snippet from a manual topology file	
Line number	Description
2	Domain to which this manual topology applies.
4 - 8	Manual connection between a manually added device "aog.dom39.1" and another manually added device "aog.dom39.2".
9 - 13	Manual connection between a manually added device "aog.dom39.2" and interface [GigabitEthernet0/1/0/1] on discovered device 172.20.1.3. Note: The device 172.20.1.3 does not appear within a <Device> tag in this file; hence it is not a manually added device and therefore must be a discovered device.

<i>Table 13. Description of the XML code snippet from a manual topology file (continued)</i>	
Line number	Description
14 - 20	Manual connection between interface [Null0] on discovered device 72.20.1.3 to interface [Nu0] on discovered device 172.20.3.3. Note: The device 172.20.3.3 does not appear within a <Device> tag in this file; hence it is not a manually added device and therefore must be a discovered device.
21 - 35	Manually added device aog.dom39.1.
36 -42	Manually added device aog.dom39.2.
43 - 49	Manually added device aog.dom39.3.

Chapter 9. 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.

Configuring NCIM connection properties

You can configure vendor-specific properties for the JDBC driver manager after installing the NCIM topology database and the GUI components.

About this task

To set vendor-specific properties, for the JDBC driver manager, complete the following steps:

Procedure

1. Create a Java properties file with the properties and values that you want.
Refer to your database vendor's documentation about JDBC for details of available properties.
2. Save the file into a directory on the server where the GUI components are installed:
`$NMGUI_HOME/profile/etc/tnm/`
3. Edit the `$NMGUI_HOME/profile/etc/tnm/tnm.properties` file and add a line that reads:
`tnm.database.connection.propertiesFile=properties_file`
Where *properties_file* is the name of the properties file you just created.

Configuring encryption length and type

Starting with Network Manager Fix Pack 9, you can use encryption keys between 128 and 256 bits. You can also choose CBC or EBC encryption. After upgrading to Fix Pack 9, you must complete some post-installation configuration steps in order to change from the default of 128 bits.

About this task

To use the default 128-bit encryption, you do not need to make any changes. To use 192-bit or 256-bit encryption, you must configure the Network Manager core components or GUI components manually. The encryption for the core components and the GUI is separate and can be different. Ensure that Storm uses the same encryption file and type as the core components.

Procedure

Configure the Network Manager core components.

1. Shut down all Network Manager processes.
You can use the `itnm_stop` command.
2. If you want to change the length of the encryption key, edit the `$NCHOME/etc/precision/ConfigSchema.cfg` file and change the value that is inserted into `config.settings.m_KeyLength` to the length of the new key in bits. Permitted values are 128, 192 and 256.
3. If you want to configure the encryption type, change the `m_EncryptAlgorithm` value to `AES_CBC` or `AES_EBC`.
4. Use the **nco_keygen** utility to generate a new encryption key. Ensure that you specify the output file as `$NCHOME/etc/security/keys/conf.key`.

For more information, refer to the topic *Generating a key in a key file* within the IBM Knowledge Center for IBM Tivoli Netcool/OMNIbus at <http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIbus.html>.

5. Restart all Network Manager processes.

You can use the `itnm_start` command.

6. Using the new encryption key, re-encrypt all the passwords currently used in configuration files using the **ncp_crypt** utility by typing the following command.

```
ncp_crypt -password password
```

Where *password* is the password to encrypt.

If you changed the location of the key file or the encryption type for the core components, configure Storm to match.

7. Edit the `$NCHOME/precision/storm/conf/NMstormTopology.properties` file.

8. Configure the location of the key file by editing the following property:

```
tnm.fips.key.location=/opt/IBM/tivoli/netcool/etc/security/keys/conf.key
```

9. To change the encryption mode, edit the following property and set it to CBC or EBC:

```
nm.cipher_mode=CBC
```

Configure the GUI components.

10. Stop the GUI processes.

You can use the `itnm_stop` command.

11. Use the **nco_keygen** utility to generate a new encryption key. Ensure that you specify the output file as `$NMGUI_HOME/profile/etc/tnm/encryption/keys/conf.key`. You can overwrite the existing key file or use a new name.
12. If necessary, adjust the file ownership of the key file to be owned by the operating system user who runs the GUI, and adjust the file permissions of the key file so that only that user has read permission on it.
13. If you gave the key file a new name, edit the `$NMGUI_HOME/profile/etc/tnm/tnm.properties` file and change `tnm.fips.key.location` to point to it. The location is relative to `$NMGUI_HOME/profile/etc/tnm`.
14. Restart the GUI processes.
You can use the `itnm_start` command.
15. Log in to the GUI as an administrator.
16. Select **Administration > Database Access Configuration** from the menu.
17. Enter the topology database password in the **Password** and **Confirm password** boxes.
18. Click the **Save** icon.
19. Log out.
20. Restart the GUI again.

Configuring Network Manager for UNIX operating systems

On UNIX systems, 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.

About this task

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. However, as a post-installation task for non-root installations, you can configure the processes to start automatically when your system is rebooted, as described in [“Configuring processes to start automatically in a non-root installation” on page 151](#).

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.

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.

Before you begin

The Network Manager Web applications must always be run as the user who installed the product.

About this task

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.

Procedure

1. Log in to the server where the Network Manager core components are installed. Log in as the root user.
2. Run the `NCHOME/precision/scripts/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.

Before you begin



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.

About this task

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 on IBM z Systems, you must install the GSKit software before running the setuid script.

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).

Before you begin

Make sure you have version 8.0.50.87 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.

About this task

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.

Procedure

1. Log on as the root user.
2. Change to the following directory: `$NCHOME/precision/scripts/`.
3. Open a command prompt and enter the following commands.

```
installp -acgXd . GSKit8.gskcrypt64.ppc.rte
installp -acgXd . GSKit8.gskssl64.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.

Configuring the core components to run as non-root

Complete the following configuration steps in order to run the core components as a non-root user.

About this task

Procedure

1. Log in as the root user.
2. Run the `NCHOME/precision/scripts/setup_run_as_setuid_root.sh` script.
3. If you are running the mtrttrapd probe (also known as the SNMP probe) on the same server as Network Manager, perform additional configuration to enable the probe to run with root privileges:
 - Configure the probe to run as a non-root user using the instructions on *Running probes as SUID root* in the *IBM Tivoli Netcool/OMNIbus Probe and Gateway 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.

Results

After this script has completed, the user who performed the Network Manager installation can log in and run the Network Manager core components.

Configuring processes to start automatically in a non-root installation

On UNIX systems, as a postinstallation task for non-root installations you can configure your Network Manager processes to start automatically when your system is started or restarted.

Before you begin

Your Network Manager installation must complete successfully before you start the following steps.

Note: You do not need to perform these steps if you installed Network Manager as the root user. The automatic restart is set up as part of a root installation without the need for this postinstallation step.

About this task

To configure the Network Manager processes to start automatically:

Procedure

1. Log in to the server where the Network Manager core components are installed. Log in as the root user.
2. Run the `NCHOME/precision/install/scripts/create_all_control.sh -auto_only` script.

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.

About this task

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: 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 MIB database for all domains. The `-domain` option, if specified, configures **ncp_mib** to use a domain-specific `MibDbLogin.domain.cfg` file. If no `-domain` option is specified, the generic `MibDbLogin.cfg` file is used. There are no process dependencies for this command.

In a distributed installation, `ncp_mib` is installed on the Dashboard Application Services Hub 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**.

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 Dashboard Application Services Hub is installed.

Procedure

1. Copy any new MIB files to the `NCHOME/precision/mibs` 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.

What to do next

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 Db2):

```
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 User Guide*.

Configuring Cognos Analytics

Perform these tasks to configure Cognos Analytics.

Related tasks

[Installing and configuring a topology database](#)

Your database administrator must install and configure a supported topology database before you can install Network Manager.

[Installing and configuring Cognos Analytics](#)

As of Network Manager Fix Pack 11, Tivoli Common Reporting is not supported. To use reports, you must install and configure Cognos Analytics.

Configuring reports for existing installations

You can configure the network management reports provided by Network Manager to use with Cognos Analytics.

Before you begin

To enable network management reports, you must have Cognos Analytics installed. If you installed Network Manager GUI components on a machine where Cognos Analytics was already present, then you do not need to complete these steps.

About this task

To configure network management reports, use the information in the Cognos Analytics Knowledge Center at <https://www.ibm.com/support/knowledgecenter/SSEP7J>.

Enabling historical polling

If you installed Network Manager as the root user, then you must run the `setup_run_storm_as_non_root.sh` script to enable the historical polling data processes to run. You do not need to run this script if you installed Network Manager as a non-root user.

About this task

As the root user, run the `setup_run_storm_as_non_root.sh` script on the server where the Network Manager core components are installed. Run the script as the following example:

```
$NCHOME/precision/scripts/setup_run_storm_as_non_root.sh -g group_name
```

Where *group_name* is the name of the poller aggregation group that you specified when you installed the Network Manager core components.

Note: When you installed the Network Manager core components, you specified values for both the poller aggregation group and the poller aggregation user, which is a member of the poller aggregation group. The poller aggregation user is listed in the `$NCHOME/precision/storm/conf/supervisor.conf` configuration file, within the `user` field of the `[supervisord]` section of that file.

For more information on the `setup_run_storm_as_non_root.sh` script, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Related tasks

[Installing the Network Manager core components](#)

You must install the Network Manager core components before, or at the same time as, installing the GUI components.

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 Polling engine and Event Gateway (which embeds the root cause analysis component)
- The NCIM topology database
- Tivoli Netcool/OMNIBus, including the ObjectServer (for event management)
- The Tivoli Netcool/OMNIBus Web GUI, which is installed within the Dashboard Application Services Hub server framework

Restriction: Network Manager does not support the Dashboard Application Services Hub 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.
- 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.

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 [“Installing and configuring a topology database” on page 47](#).

Related concepts

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.

[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.

Related tasks

[Installing and configuring a topology database](#)

Your database administrator must install and configure a supported topology database before you can install Network Manager.

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
- 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.
- 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.

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.

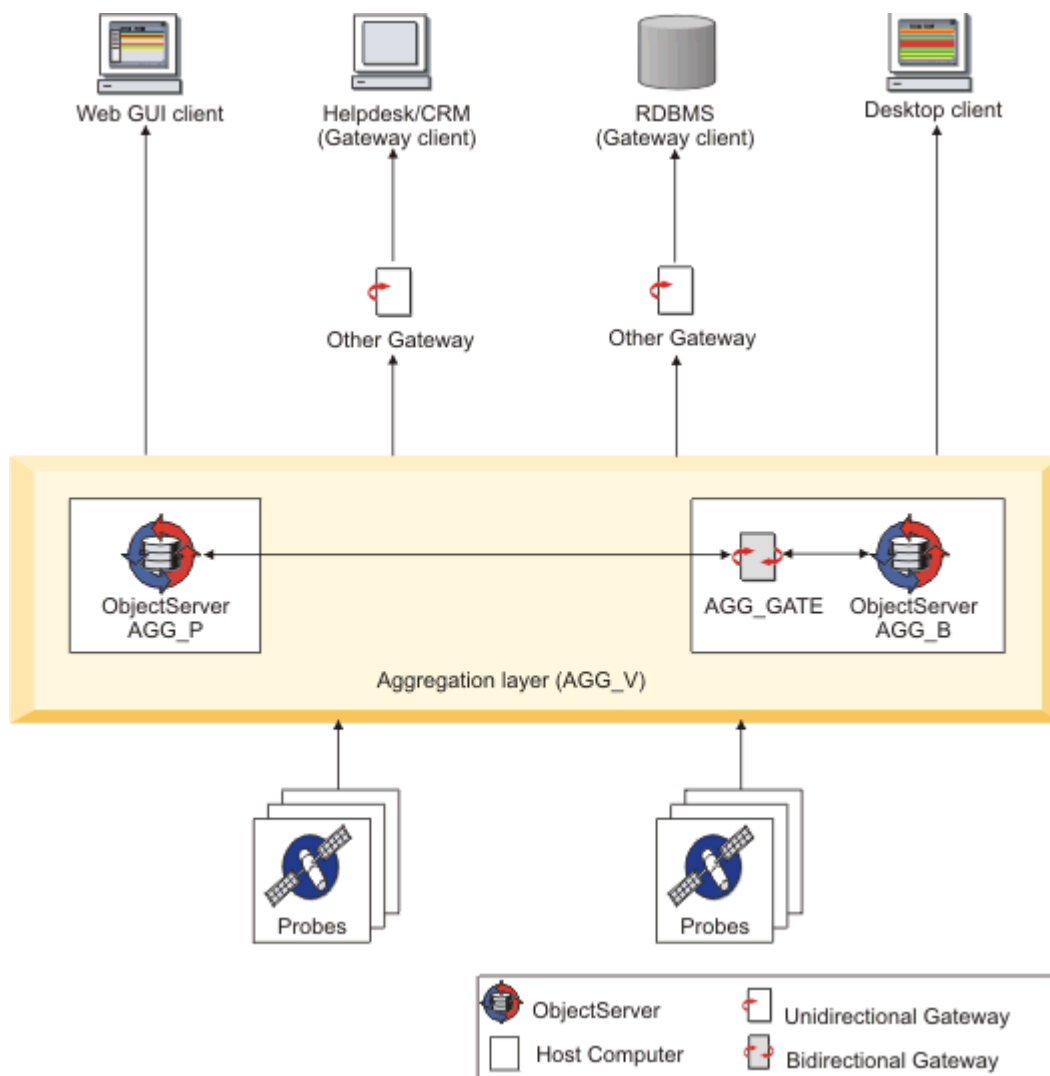


Figure 7. ObjectServer failover architecture

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://www.ibm.com/support/knowledgecenter/SSHTQ/landingpage/NetcoolOMNIBus.html>.

Related concepts

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.

Related tasks

Configuring ObjectServer failover

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 7 on page 156; 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://www.ibm.com/support/knowledgecenter/SSHTQ/landingpage/NetcoolOMNIBus.html>.

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.

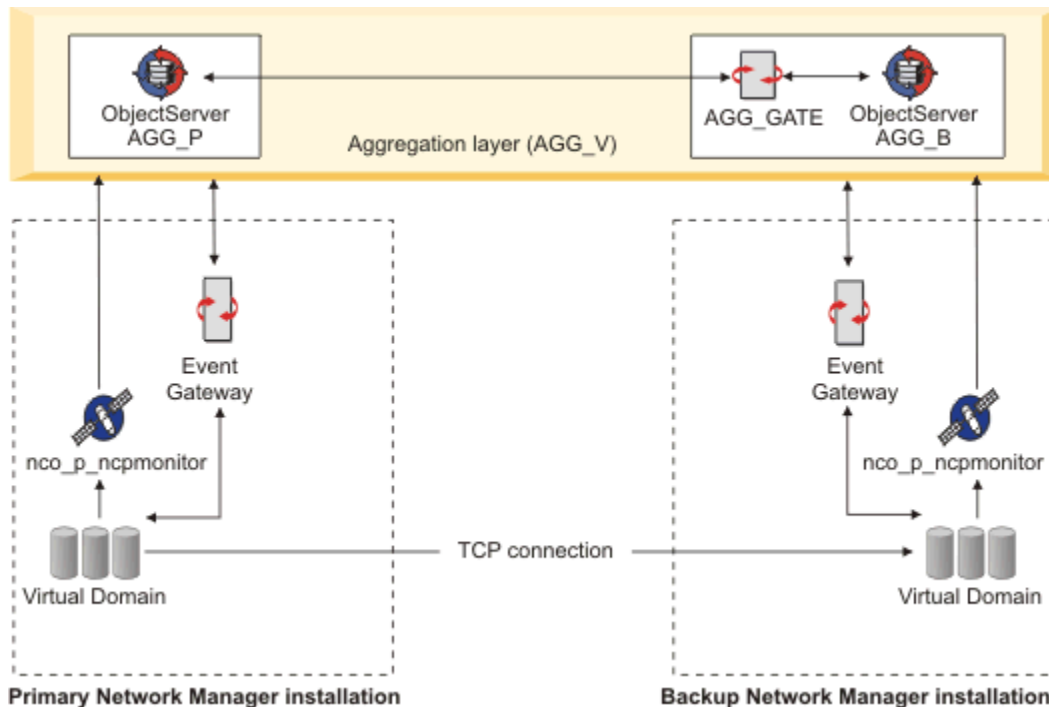


Figure 8. Network Manager failover architecture

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*. Also, to update the NCIM and ObjectServer passwords use the Perl script `ncp_password_update.pl`. For more details on the Perl script `ncp_password_update.pl`, 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.
- 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. 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

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

All processes on the backup installation point to the NCIM topology database on the primary installation. The NCIM topology database on the primary can be a standalone database or one configured 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.

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.

Related tasks

Configuring failover of the Network Manager core processes

Setting up existing Db2 databases on UNIX

To use an existing Db2 database as the topology database on UNIX, you must have a Db2 instance available before installing Network Manager.

Configuring Network Manager to work with Db2 HADR or Oracle RAC

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 tasks

[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.

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 Dashboard Application Services Hub server would each be installed on separate hosts. However, this might not be practical.

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.

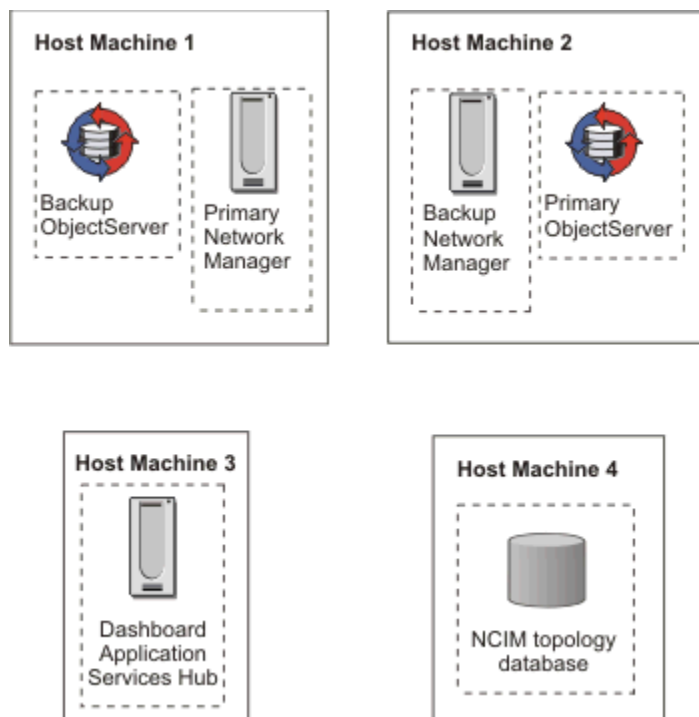


Figure 9. Example failover hosting

For performance reasons, the NCIM topology database requires a high bandwidth connection to the Dashboard Application Services Hub 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, 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*. Also, to update the NCIM and ObjectServer passwords use the Perl script `ncp_password_update.pl`. For more details on the Perl script `ncp_password_update.pl`, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Related concepts

[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.

[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.

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.
- 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.

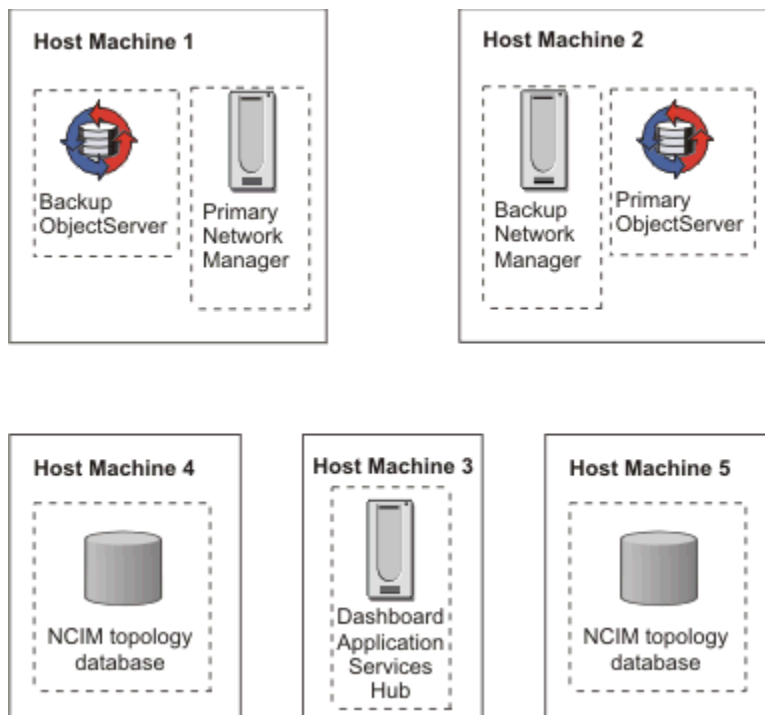


Figure 10. Example failover hosting with backup NCIM topology database

For performance reasons, the NCIM topology database requires a high bandwidth connection to the Dashboard Application Services Hub 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.

Related concepts

Failover on the backup installation

All processes on the backup installation point to the NCIM topology database on the primary installation. The NCIM topology database on the primary can be a standalone database or one configured for high availability.

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.

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.

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.

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](#)

Related tasks

[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.

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.

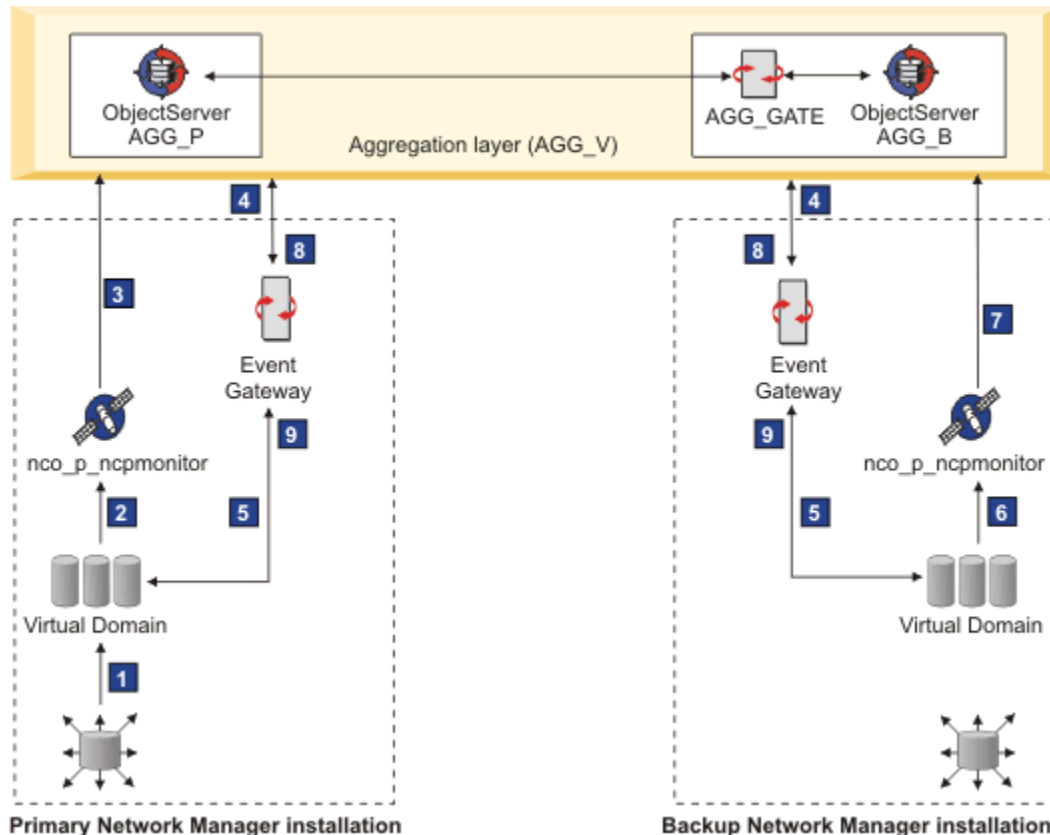


Figure 11. Process flow of a health check event

1 Status report

The **nco_p_ctl** 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 **Event Viewer**.

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 **Event Viewer**.

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 fallback

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. Fallback 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 **nep_poller** process suspends all polls.

For further information about the standby filter and incoming event filter, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

The Apache Storm realtime computation system, which is used to aggregate raw poll data into historical poll data, fails over in a different way to the other Network Manager core processes. In a failover configuration each Network Manager has a fully functioning Apache Storm server which performs aggregation of poll data, but only one of these Apache Storm servers is active at any one time. When an Apache Storm server first starts it checks the database to see if the poll data is already being processed by another Apache Storm server.

- If it is then the first Apache Storm server goes into a standby state.
- if not, then the Storm assumes the responsibility of processing the poll data.

When failover occurs, the current Apache Storm server does not stop processing. The Apache Storm server fails over only if it is stopped by the user or is unable to update the database. For more information on how poll data aggregation works in a multiple Network Manager configuration, see the *IBM Tivoli Network Manager IP Edition Administration 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

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

All processes on the backup installation point to the NCIM topology database on the primary installation. The NCIM topology database on the primary can be a standalone 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.
- 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 Network Manager failover architecture, where the NCIM topology database is configured for high availability.

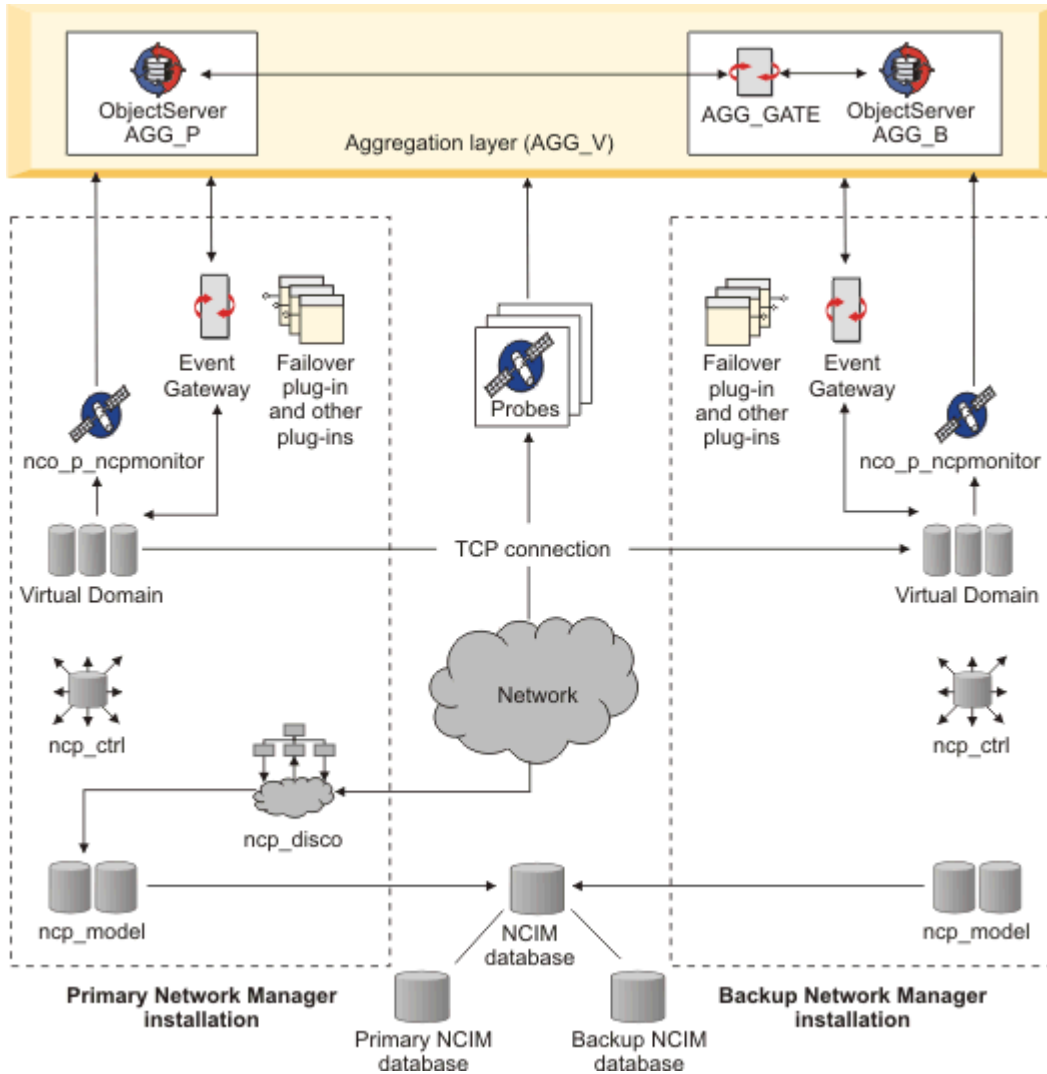


Figure 12. Example failover architecture with NCIM high availability

The following figure differs from the previous one in that the NCIM topology database is not configured for high availability.

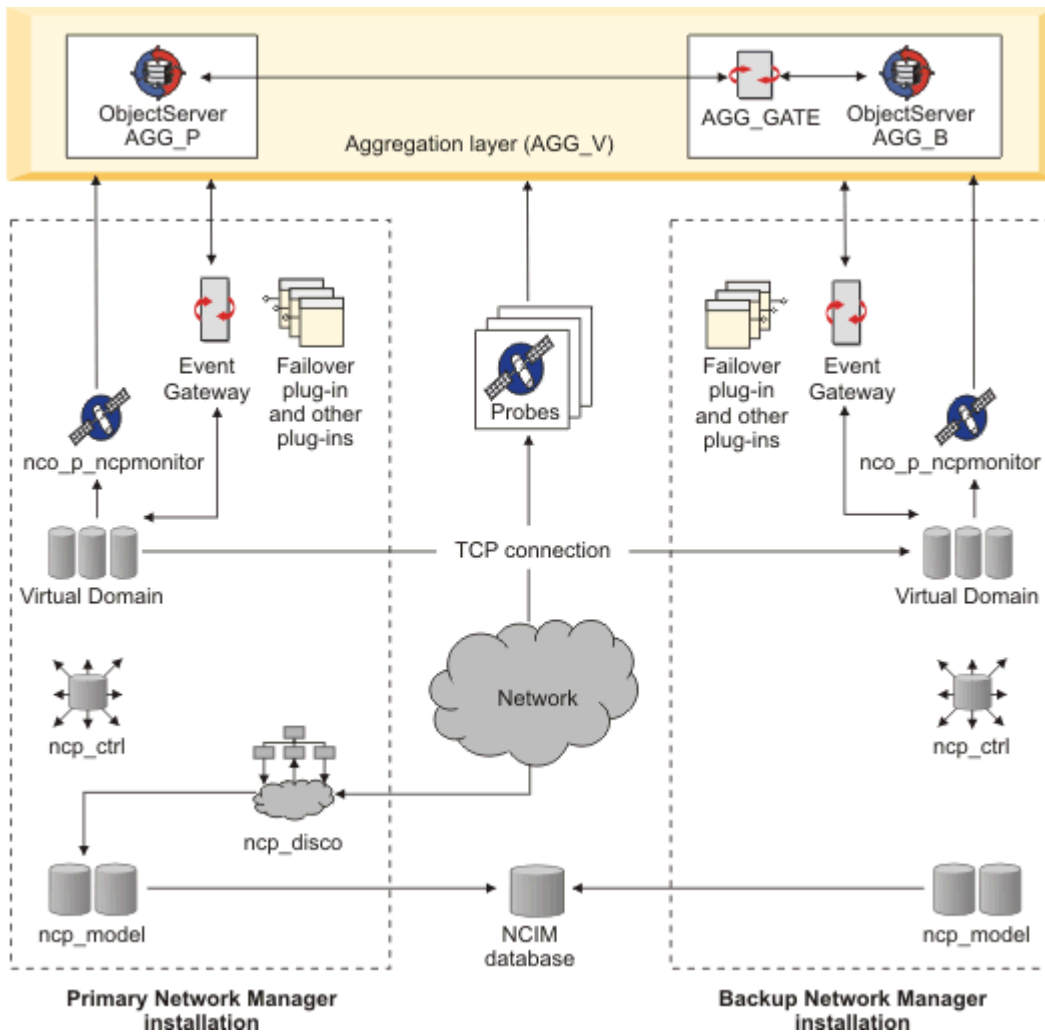


Figure 13. Example failover architecture without NCIM high availability

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.

Event Gateway

When the backup domain is in standby mode, the Event Gateway does not enrich events on the ObjectServer. When the backup domain becomes active, the Event Gateway switches from the standby filter (StandbyEventFilter) to the incoming event filter (EventFilter).

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 that is 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.

Related concepts

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.

[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.

[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.

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.

The WebTools do not function when the backup server is in primary mode.

The Web applications do not connect to the backup server when it becomes primary during failover. Some Web applications, such as the SNMP MIB Browser and SNMP MIB Grapher, do not function when the backup server is in primary mode.

Restriction: Network Manager does not support the Dashboard Application Services Hub load balancing feature that the Tivoli Netcool/OMNIBus Web GUI does.

If you are running more than one Dashboard Application Services Hub server, they each run independently. If one of the Dashboard Application Services Hub servers fails, any remaining servers continue to run as individual entities. To minimize the effect of a server failing:

- A user session on one Dashboard Application Services Hub server cannot be transferred, or continued, on another. If the first Dashboard Application Services Hub server fails, users must log in to another active Dashboard Application Services Hub server.
- Ensure that each of the servers is configured with the same set of users, roles, groups, preference profiles, and resources such as pages, views, widgets, and reports.
- Configure the servers to whatever the database high availability requires. For example, for Db2 you would configure the servers according to the requirements of the Db2 HADR feature. 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](#)

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

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.

About this task

As a prerequisite to configuring failover:

Procedure

- 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 topology database high availability, you require two topology databases.
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.
 - If you have an Oracle database, you can use the Real Application Clusters (RAC) feature to set up failover for NCIM.
- You must have installed and configured the Web GUI and the Network Manager Web applications within the Dashboard Application Services Hub 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

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.

Configuring ObjectServer failover

The way in which you configure ObjectServer failover is dependent on the Tivoli Netcool/OMNIBus version.

Before you begin

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:

- **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.)

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 bidirectional 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://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html>.

Related concepts

[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.

Configuring ObjectServers and gateways for failover

The following procedures provide guidance for setting up ObjectServer failover in Tivoli Netcool/OMNIBus.

About this task

[“Tivoli Netcool/OMNIBus V7.3 or later” on page 172: Configuring failover](#)

[“Tivoli Netcool/OMNIBus V7.2.1 or earlier” on page 173: Configuring failover](#)

For the most recent and complete information about ObjectServer failover, see the Tivoli Netcool/OMNIBus documentation at <http://www.ibm.com/support/knowledgecenter/SSHTQ/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

About this task

To configure failover:

Procedure

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:

```
Linux $NCHOME/omnibus/bin/nco_sql -server AGG_P -user user_name -password password < $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:

```
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” on page 172.

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” on page 172.

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

About this task

To configure failover:

Procedure

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” on page 173.
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” on page 173.
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.

About this task

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) should be available in the NCHOME installation location.

Procedure

- When Tivoli Netcool/OMNIBus is installed on the same server as Network Manager, they must both be installed into the same NCHOME location. In such cases, no further action is required to ensure that Network Manager processes can connect to an ObjectServer failover pair.
- If Network Manager and Tivoli Netcool/OMNIBus are installed on different servers, perform the following steps on the primary and backup Network Manager servers:

Copy the `$NCHOME/etc/interfaces.arch` file from the Tivoli Netcool/OMNIBus NCHOME location to the NCHOME installation location on the server where Network Manager is installed.

For more information about configuring server communication information and generating the Tivoli Netcool/OMNIBus `interfaces.arch` file, see the Tivoli Netcool/OMNIBus documentation at <http://www.ibm.com/support/knowledgecenter/SSHTQ/landingpage/NetcoolOMNIBus.html>.

Note: The name of the virtual ObjectServer pair should be specified in the `ConfigItnm.DOMAIN.cfg` file.

Related tasks

Configuring ObjectServer failover

The way in which you configure ObjectServer failover is dependent on the Tivoli Netcool/OMNIBus version.

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.

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.

About this task

This file is located in `webgui_home_dir/etc/datasources`, where *webgui_home_dir* is the installation directory for Web GUI; for example, `$NCHOME/omnibus_webgui`.

To configure data source failover:

Procedure

1. On the Dashboard Application Services Hub 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 176](#).

- c) Restart the Dashboard Application Services Hub server for the changes to take effect.
Use the following command:

- **Linux** `startServer.sh server1`

For the most recent and complete information about configuring data source failover in the Web GUI, see the Web GUI documentation at <http://www.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 176](#), 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,
"0S"
);
```

- 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 `0S` 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 Dashboard Application Services Hub to configure the Virtual Member Manager adapter for the ObjectServer. Configure the adapter for both of the ObjectServers in the failover pair.

About this task

On each Dashboard Application Services Hub server where the Network Manager Web applications and the Web GUI are installed:

Procedure

1. Go to the \$WAS_HOME/bin directory.
2. Enter the following command at the command line:

```
./confvmm4ncos jazzsm_profile_dir user password address port address2 port2
```

Where:

- jazzsm_profile_dir is the Jazz for Service Management profile directory.

- *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 Dashboard Application Services Hub server.

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 \(core processes\)](#)

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.

About this task

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:

Procedure

1. On the primary Network Manager server, edit the `$NCHOME/etc/precision/ConfigItnm.PRIMARY_DOMAIN.cfg` file as follows:
 - a) Enable failover 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,
    PrimaryDomainName,
    BackupDomainName,
    VirtualDomainName
)
values
(
    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.
PrimaryDomainName	Replace NCOMS_P with the actual name of the Network Manager primary domain in the failover pair. Note: The PrimaryDomainName is the only one that is stored in NCIM, and as a result the only name that is displayed in the GUI. The backup domain name is not used in NCIM, and consequently, not displayed in the GUI either.
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.

- Save the file.
- 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.

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.

About this task

To configure the TCP connection:

Procedure

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.

About this task

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:

Procedure

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](#)

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.

About this task

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.
- 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:

Procedure

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 If you have an 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 181.

Related concepts

[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.

Related tasks

[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.

[Configuring Network Manager to work with Db2 HADR or Oracle RAC](#)

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. 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*. Also, to update the NCIM and ObjectServer passwords use the Perl script `ncp_password_update.pl`. For more details on the Perl script `ncp_password_update.pl`, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Related concepts

[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.

[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.

Configuring Network Manager to use Db2HADR or an Oracle RAC service

Use this information to force the Network Manager core processes to use the Db2 alias or to connect to an Oracle RAC service name, depending on your database type.

Before you begin

DB2 For Db2 databases, the Network Manager core processes need to use the Db2 alias to obtain information about the alternate Db2 server. To force the Network Manager core processes to use the Db2 alias, edit two configuration files (`DbLogins.Domain.cfg` and `MibDbLogin.cfg`) and then edit the driver file:

```
$NCHOME/precision/platform/linux2x86/db2-version-number/odbc_cli/clidriver/  
cfg/db2dsdriver.cfg
```

Where *version-number* is the Db2 version number; for example, 10.5.0.5.

Oracle For Oracle databases, the Network Manager core processes need to connect to the service name used by Oracle RAC. To configure the Network Manager core processes to use an SID instead of a service name, edit the `DbLogins.Domain.cfg` and `MibDbLogin.cfg` configuration files.

About this task

The `DbLogins.Domain.cfg` and `MibDbLogin.cfg` configuration files are part of the Network Manager core installation. These files are stored on the Network Manager server. If you have Network Manager failover configured, edit these configuration files on both the primary and backup Network Manager servers.

Procedure

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	a. Search for the attribute called <code>m_PortNum</code>. b. Set the value of all <code>m_PortNum</code> attributes to 0 (zero). c. Write and quit the configuration file. Perform the same steps on the Network Manager backup server, if necessary.
Oracle For Oracle databases	a. Search for the attribute called <code>m_OracleService</code> and add it after <code>m_PortNum</code> if it does not already exist. b. Do not change the value of the <code>m_OracleService</code> attribute for "DNCIM", . Set the value of all the other <code>m_OracleService</code> attributes to 1. c. Ensure <code>m_DbName</code> is set to the Oracle <code>SERVICE_NAME</code> as specified in <code>\$ORACLE_HOME/network/admin/tnsnames.ora</code> d. Ensure <code>m_Hostname</code> is set to the Oracle RAC SCAN host name. e. Optionally, you can define your own custom Oracle RAC connection string using the attribute <code>m_ConnectionString</code>, as described here. This connection string can be used for connecting to an Oracle RAC cluster, or for other purposes. f. 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	a. Search for the attribute called <code>m_PortNum</code>. b. Set the value of <code>m_PortNum</code> attribute to 0 (zero). c. Write and quit the configuration file. Perform the same steps on the Network Manager backup server, if necessary.
Oracle For Oracle databases	a. Search for the attribute called <code>m_OracleService</code> and add it after <code>m_PortNum</code> if it does not already exist. b. Set the value of <code>m_OracleService</code> attribute to 1. c. Ensure <code>m_DbName</code> is set to the Oracle <code>SERVICE_NAME</code> as specified in <code>\$ORACLE_HOME/network/admin/tnsnames.ora</code> d. Ensure <code>m_Hostname</code> is set to the Oracle RAC SCAN host name.

Option	Description
	e. Optionally, you can define your own custom Oracle connection string using the attribute <code>m_ConnectionString</code>, as described here. This connection string can be used for connecting to an Oracle RAC cluster, or for other purposes. f. Write and quit the configuration file. Perform the same steps on the Network Manager backup server, if necessary.

3. DB2

For Db2 databases, you also need to perform the following procedure:

- a) Copy the following sample driver file to the same location with a new file name, as follows:

```
cp $NCHOME/precision/platform/linux2x86/db2-version-number/odbc_cli/
clidriver/cfg/db2dsdriver.cfg.sample $NCHOME/precision/platform/linux2x86/
db2-version-number/odbc_cli/clidriver/cfg/db2dsdriver.cfg
```

Where *version-number* is the Db2 version number; for example, 10.5.0.5

Note: If you are already using this driver file, then make a backup of the file and edit the driver file directly rather than copying the sample driver file.

- b) Find the <configuration> section of the driver file.

- c) Update the <configuration> section as follows:

```
<configuration>
  <dsncollection>
    <dsn alias="Database_alias"
      name="Primary_database_name" host="Primary_database_host"
      port="Primary_database_port" />
  </dsncollection>
  <databases>
    <database name="Primary_database_name"
      host="Primary_database_host" port="Primary_database_port" />
    <wlb>
      <parameter name="enableWLB" value="true" />
      <parameter name="maxTransports" value="50" />
    </wlb>
    <acr>
      <parameter name="enableAcr" value="true" />
      <parameter name="maxAcrRetries" value="10" />
      <parameter name="acrRetryInterval" value="5" />
      <parameter name="enableAlternateServerListFirstConnect"
value="true" />
    <alternateserverlist>
      <server name="server1" hostname="Standby_database_host"
      port="Standby_database_port" />
    </alternateserverlist>
    </acr>
    <database name="Standby_database_name"
      host="Standby_database_host"
      port="Standby_database_port" />
  </databases>
</configuration>
```

Where the following items are all listed in the `DbLogins_DOMAIN.cfg` configuration file:

- *Database_alias* is the name of the primary database.

Note: For convenience, the name of the primary database is also used as the database alias.

- *Primary_database_name* is the name of the primary database.
- *Primary_database_host* is the hostname of the primary database server.
- *Primary_database_port* is the port for the primary database.
- *Standby_database_name* is the name of the standby database
- *Standby_database_host* is the hostname of the standby database server.
- *Standby_database_port* is the port for the standby database.

d) Save the `db2dsdriver.cfg` driver file.

Related tasks

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 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.

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,
    m_OracleService
)
values
(
    "NCIM",
    "oracle",
    "ORATEST",
    "ncim",
    "server1.location1.acme.com",
    "ncim",
    "ncim",
    "ncim",
    1521,
    "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=server1.location1.acme.com3)
(PORT=1521))(CONNECT_DATA=(SID=ORATEST)))",
    0,
    1
);
```

By using the `m_ConnectionString` attribute in this way you effectively replace the values of `m_DbName`, `m_Hostname` and `m_PortNum`. You must still provide these values; 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 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.

About this task

To set a custom connection URL to identify the primary and backup Db2 servers, or to identify the Oracle RAC servers, edit the relevant properties files and specify the URL connection to the servers. Specify the same URL connection in each of the properties files.

The following properties file is applicable to the Network Manager GUI:

- `$NMGUI_HOME/profile/etc/tnm/tnm.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:

Procedure

1. Open the \$NMGUI_HOME/profile/etc/tnm/tnm.properties and the \$NCHOME/precision/platform/java/lib/ncp_topoviz/etc/tnm/tnm.properties files for editing
2. 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: <pre>tnm.database.jdbc.url=jdbc:db2:// primary_db2_server: primary_db2_port_number/ dbname:clientRerouteAlternateServerName= backup_db2_server ;clientRerouteAlternatePortNumber= backup_db2_port;</pre> where: • <i>primary_db2_server</i> — Specifies the name of the primary server on which the Db2 database is running. • <i>primary_db2_port_number</i> — Specifies the port number of the primary server on which the Db2 database is running. • <i>dbname</i>: Specifies the name of the Db2 database. • <i>backup_db2_server</i> — Specifies the name of the backup server on which the Db2 database is running. • <i>backup_db2_port</i> — 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: <pre>tnm.database.jdbc.url=jdbc:oracle:thin: @Oracle_RAC_SCAN_hostname: Oracle_RAC_port_number/ Oracle_RAC_service_name</pre> where: • <i>Oracle_RAC_SCAN_hostname</i> — Specifies the Oracle Single Client Access Name (SCAN) address on which the Oracle RAC database is running. • <i>Oracle_RAC_port_number</i> — Specifies the port number on which the Oracle RAC database is running. • <i>Oracle_RAC_service_name</i> — Specifies the service name with which the Oracle RAC database is running.

3. Save and close the files.

Related tasks

[Configuring Network Manager to use Db2HADR or an Oracle RAC service](#)

Use this information to force the Network Manager core processes to use the Db2 alias or to connect to an Oracle RAC service name, depending on your database type.

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.

About this task

The Virtual Domain component uses two databases (config and state) 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 Reference*.

To change the default settings for the health check parameters:

Procedure

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_SocketKeepAlivePeriod,
    m_HealthCheckPeriod,
    m_FailoverTime,
    m_DirectoryScanPeriod,
    m_AutoTopologyDownload
)
values
(
    60,
    60,
    300,
    100,
    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](#)

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.

About this task

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.

Troubleshooting database errors after failover

If, after failover, you see errors in the GUI logs relating to the `NETWORKVIEWSUMR` or `networkViewSumr` table, you must drop and recreate this table.

About this task

The procedure for dropping and recreating the table differs on DB2 and Oracle.

Procedure

1. For DB2, complete the following steps:

- a) Enter the following commands at the DB2 command prompt.

```
SET SCHEMA ncpgui;  
DROP TABLE networkViewSumr;
```

- b) Find the section of `$PRECISION_HOME/scripts/sql/db2/createPrecisionGUIDb.sql` that creates `networkViewSumr` and copy it into the DB2 command line.
- c) Enter the following command at the DB2 command prompt:

```
COMMIT;
```

- d) Exit the DB2 command line.

2. For Oracle, complete the following steps:

- a) Enter the following commands at the Oracle command prompt.

```
ALTER SESSION SET CURRENT_SCHEMA = ncpgui;  
DROP TABLE networkViewSumr;
```

- b) Find the section of \$PRECISION_HOME/scripts/sql/oracle/createPrecisionGUIDb.sql that creates networkViewSumr and copy it into the Oracle command line.
- c) Exit the Oracle command line.

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 **Event Viewer**.
2. Stop the primary ObjectServer and check the ObjectServer log file (\$NCHOME/omnibus/log/PRIMARY_NAME.log) for failover messages.
3. Check the **Event Viewer** 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://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html>.

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.ncimCache.entityData.domain) in the \$NCHOME/var/precision directory in the backup domain, where *domain* is the name of the current domain.

Event generation for startup: Monitor the **Event Viewer** 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 **nbp_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 **nbp_poller** and **nbp_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.)

For further information about running OQL queries, see the *IBM Tivoli Network Manager 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 **Event Viewer** 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. The `Summary` field identifies the domain raising the event and the domain the event is about.

Tracking failover and fallback

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 **nbp_poller** and **nbp_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 **Event Viewer** 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.

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 Administration 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](#)

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.

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

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

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 and Linux
 - The Tivoli Netcool/OMNIBus **nco_objserv** command

For information about using the Tivoli Netcool/OMNIBus commands to start the ObjectServer, see the Tivoli Netcool/OMNIBus documentation at <http://www.ibm.com/support/knowledgecenter/SSSHTQ/landingpage/NetcoolOMNIBus.html>.

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 Dashboard Application Services Hub server, on which the Network Manager Web applications and the Tivoli Netcool/OMNIBus Web GUI are installed, starts automatically whenever the computer is started.

Configuring security

In order to protect your ITNM installation against malicious attacks by intruders you must perform the following tasks.

Configuring cookies

The Network Manager web applications use cookies to track users across requests. Although these cookies are not themselves sensitive, they could be used by an intruder to impersonate you on the system. Since network traffic often travels over untrusted networks, these cookies must be encrypted using SSL.

About this task

Configuring Dashboard Application Services Hub cookies

In the case of communications involving Dashboard Application Services Hub, the most important cookie is the HTTP session cookie; therefore it must be configured to be sent only over SSL.

About this task

To limit the HTTP session cookie to communicate using the HTTPS protocol only, perform the steps in the technote located at the following location: <https://www.ibm.com/support/pages/node/250915>

Configuring the WebSphere LTPA cookie

The Lightweight Third Party Authentication (LTPA) mechanism is associated with roles and authentication throughout your login session. If an intruder is able to intercept the LTPA cookie then they can impersonate you. To protect against this, you must ensure that the LTPA cookie is transmitted only over SSL.

About this task

Procedure

1. Click **Security** > **Global security**.
2. Click **Authentication** > **Web security** > **Single sign-on (SSO)**.
3. Click **Requires SSL**.
4. Click **OK**.
5. Restart the Dashboard Application Services Hub server.

Protecting against clickjacking

If you integrate Network Manager web applications into your own product, be aware that the integration will not be able to display the Database Access GUI and the Discovery Configuration GUI, due to a

protective filter implemented within Network Manager. These two GUIs contain sensitive information; preventing integration of these two GUIs protects you against clickjacking, whereby an intruder creates a GUI overlay to capture data. You can disable the filter; however, this is not recommended.

About this task

The filter is implemented using the `tnm.enableClickjackProtection` property in the `tnm.properties` file.

Note: If this property is not present in the file then filtering is enabled by default.

Procedure

1. Back up and edit the `$NMGUI_HOME/profile/etc/tnm/tnm.properties` file.
2. Find the entry `tnm.enableClickjackProtection=true`.
3. Change the entry to `tnm.enableClickjackProtection=false`.

Note: If this property is not present in the file then type:
`tnm.enableClickjackProtection=false`.

Changing the IP address and hostname of the Network Manager installation

If you change the IP address and hostname of the server where any of the components of Network Manager or integrated products are installed, you must configure Network Manager and associated components and products.

Changing the IP address and hostname for Network Manager

If you want to change the IP address and hostname for the server where the Network Manager core components are installed, you must perform some configuration tasks.

About this task

Complete the following steps to change the IP address and hostname on the Network Manager server.

Procedure

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 server; for example: `ncp=myhost`.
4. Save the `itnm.cfg` file.
5. Change to the following directory: `NCHOME/etc/precision/`.
6. Edit the file: `ServiceData.cfg`.
7. 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 server.
 - `Network_Manager_server_hostname` is the new hostname of the Network Manager server.
8. 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.

About this task

Complete the following steps to change the IP address and hostname on the Tivoli Netcool/OMNIBus server:

Procedure

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 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 to use the new IP address and hostname.

About this task

Complete the following steps to update Network Manager to make it aware of the changes to the Tivoli Netcool/OMNIBus server hostname:

Procedure

1. Update the Network Manager core components by editing the configuration file: `NCHOME/etc/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 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 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.

Updating the Dashboard Application Services Hub for a new Tivoli Netcool/OMNIBus IP address and hostname

If the Dashboard Application Services Hub 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 Dashboard Application Services Hub to use the new IP address and hostname.

About this task

Complete the following steps to configure the Dashboard Application Services Hub to use the new Tivoli Netcool/OMNIBus server hostname:

Procedure

1. Edit the following file:

```
$JazzSM_HOME/profile/config/cells/JazzSMNode01Cell/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.

Changing the IP address and hostname on the Dashboard Application Services Hub server

If you want to change the IP address and hostname of the Dashboard Application Services Hub, you must configure the Dashboard Application Services Hub.

About this task

Follow these steps to change the IP address and hostname on the Dashboard Application Services Hub server:

Procedure

1. Change to the following directory: \$JazzSM_HOME/profile/bin/.
2. Use the wsadmin command to change the Dashboard Application Services Hub server hostname and IP address:

```
wsadmin.sh -user smadmin -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 Nodename  
using SOAP connector;The type of process is: UnManagedProcess
```

3. Restart the Dashboard Application Services Hub server.

Updating Network Manager for changed hostname of the Dashboard Application Services Hub server

If you change the hostname of the Dashboard Application Services Hub server, you must configure Network Manager to use the new hostname.

About this task

To configure Network Manager to use the new hostname, complete the following steps:

Procedure

1. Update the Network Manager 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 Dashboard Application Services Hub server; for example:

```
tip=tiphost
```

3. Save the `itnm.cfg` file.

Configuring Network Manager 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 to use the new details.

About this task

Procedure

1. On the server where the Network Manager 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 web applications are installed, edit the following file:

```
$NMGUI_HOME/profile/logs/tnm/tnm.properties
```

6. 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 appropriate environment variables by running the environment scripts.

About this task

The environment scripts set the following required environment variables. The environment scripts are configured automatically with the correct locations where the components are installed. 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:

- `/opt/IBM/netcool/core`

\$NMGUI_HOME

The location where the Network Manager GUI components are installed. By default, this location is `/opt/IBM/netcool/gui/precision_gui`.

\$ITNMHOME and \$PRECISION_HOME

The Network Manager home location that defaults to `$NCHOME/precision`:

- `/opt/IBM/netcool/core/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.

\$DASH_HOME

The installation location of Dashboard Application Services Hub. By default, this location is `/opt/IBM/JazzSM/ui`.

\$JazzSM_HOME

The installation location of Jazz for Service Management. By default, this location is `/opt/IBM/JazzSM`.

To set the Network Manager environment variables, run the appropriate script for the components that you installed. There are different scripts on the server where the core components are installed and the server where the GUI components are installed.

Important: If you have installed the core components and the GUI components on one server, run both scripts.

Procedure

- Run the appropriate environment script:

On the server where the Network Manager core components are installed, the environment script is `installation_directory/netcool/core/env.sh`.

For example, on Bash, Bourne, and Korn shells, source the `env.sh` script using a command similar to the following:

```
. /opt/IBM/netcool/core/env.sh
```

On the server where the Network Manager GUI components are installed, the script is `installation_directory/nmgui_profile.sh`, for example, `/opt/IBM/netcool/nmgui_profile.sh`.

For example, on Bash, Bourne, and Korn shells, source the `nmgui_profile.sh` script using a command similar to the following:

```
. /opt/IBM/netcool/nmgui_profile.sh
```

What to do next

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 `netcool` subdirectory is created. The `netcool` directory in turn contains the following subdirectories:

- `core`: contains configuration files for the Network Manager back-end processes.
- `gui`: contains configuration files for GUI processes:
 - `omnibus_gui`: If present, contains Tivoli Netcool/OMNIBus Web GUI files.
 - `precision_gui`: contains Network Manager GUI 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`, 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.

Note: From version 4.2 onwards, `NCHOME` is `installation_directory/netcool/core`; for example, `opt/ibm/netcool/core`.

Table 14. Directories used by the installer	
Installation	Directories used for installation files
UNIX operating systems, root user	<code>/usr/ibm/common/acsi</code>
	<code>/var/ibm/common/acsi</code>
UNIX operating systems, non-root user	<code>~/.acsi_\${HOSTNAME}</code>
	<code>~/tivoli</code>
	<code>~/.cit</code> (that is, in the user's home directory)

Contents of the netcool directory

The following table describes the contents of the `netcool/core` 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:

- Linux – `linux2x86`
- AIX – `aix5`
- 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 15. 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.
license	Contains the text of the product license agreement in various languages.
log	Contains log files.
log/install	Contains log files for the installation.
log/precision	Contains log files created by Network Manager processes.
omnibus	If present, contains IBM Tivoli Netcool/OMNIBus files.
platform/arch	Contains the Java Development Kit (JDK) and Java Runtime Environment (JRE) files. Note: Dashboard Application Services Hub uses the WebSphere Application Server JRE.
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.
properties	Contains files used by the installation process. You should not need to alter the contents of this directory.
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:

- Linux – linux2x86
- AIX – aix5
- zLinux - linux2s390

Note: NCHOME/precision is the path set by default for PRECISION_HOME and ITNMMHOME.

Table 16. 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.
aoc	Contains the Active Object Class (AOC) files used by the dynamic class management and distribution system, CLASS.

Table 16. Directories in NCHOME/precision (continued)

Directory	Description
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.
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.
embeddedDb	Contains files for dNCIM.
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.
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.

Table 16. Directories in NCHOME/precision (continued)	
Directory	Description
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.
storm	Contains Apache Storm scripts.
system	Contains files for product operation.
systemApps	Contains files for Web applications.

Related reference

[Installation directory requirements](#)

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.

Configuring domains

You can configure network domains to match your environment.

Creating and configuring extra network domains

To add more network domains, configure process control for the domains and register the domains with the NCIM topology database. Configurations and polls can be copied from existing domains. Configure or reconfigure network views to show devices on the new domains.

About this task

Use one instance of **nbp_ctrl** process to run and manage each domain. If an **nbp_ctrl** process is not running for a domain, the domain cannot be configured on the GUI.

You can run the `domain_create.pl` script to copy configuration data from an existing domain. The script does not copy the topology from the original domain. For guidelines on the number of network domains that are required for a deployment, see the *IBM Tivoli Network Manager User Guide*.

Procedure

1. Back up the `$NCHOME/etc/precision/CtrlServices.cfg` file for the domain that was created during the installation of the product.
2. Make a copy of the `CtrlServices.cfg` file and rename it to `CtrlServices.DOMAIN.cfg`, where *DOMAIN* is the domain.

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

For example, `CtrlServices.MASTER.cfg`.

Then, edit the `CtrlServices.DOMAIN.cfg` file as required.

3. To configure a discovery for the domain:
 - a) Back up and create domain-specific versions of the discovery configuration files.
For example, `DiscoPingFinderSeeds.MASTER.cfg`
 - b) Configure the settings in the domain-specific files.
4. Back up and make a domain-specific version of the `$NCHOME/etc/precision/ConfigItnm.cfg` file.
For example, `ConfigItnm.MASTER.cfg`.
Then, specify the connection details for the ObjectServer in that file.
5. To register the new domain with the NCIM topology database, back up and create a domain-specific version of the `$NCHOME/etc/precision/DbLogins.cfg` file. Then, edit the database connection information in that file.
6. To connect to a different Tivoli Netcool/OMNIBus Web GUI data source:
 - a) Back up and make a domain-specific copy of the `$NCHOME/etc/precisionModelNcimDb.cfg` file.
For example, `ModelNcimDb.MASTER.cfg`
 - b) In the domain-specific file, change the **m_WebTopDataSource** property to the name of the data source.

7. To copy the configuration and network polls from an existing domain, run the `domain_create.pl` script.

The following example creates a domain that is called MASTER with the password PASSWORD.

```
$NCHOME/precision/bin/ncp_perl  
$NCHOME/precision/scripts/perl/scripts/domain_create.pl -domain MASTER  
-password PASSWORD
```

8. Start the Network Manager processes on the domain.

For example:

```
itnm_start ncp -domain MASTER
```

9. Create new network views in the new domain, or change your existing network views.

On the **Filter** tab, select the new domain. If you do not specify the new domain in network views, you cannot view the devices in that domain. If you previously ran auto-provision scripts to create network views automatically, you must rerun them, specifying the new domain. When a network discovery is run in the new domain, the new network views are populated with devices. For more information about network views, see the *IBM Tivoli Network Manager User Guide*.

10. Repeat the steps to set up all the domains.

What to do next

After **ncp_ctrl** is started on the domain, you can configure the domain. For example, configure the discovery on the **Network Discovery** GUI or edit configuration files, or configure network polling. Select the domain before you configure the discovery or poll.

For more information about configuring discovery, see the *IBM Tivoli Network Manager IP Edition Administration Guide*. For more information about configuring network polling, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Because network discovery is a resource-intensive process, discoveries are usually run one domain at a time. To run discoveries for several domains simultaneously, ensure that you have enough resources available. Typical checks are as follows:

- Ensure that enough database connections are configured.
- Ensure that network devices are not overloaded with traffic.
- Ensure that enough memory is available on the host to run the discovery, for example by check the memory usage of Network Manager processes.

Related concepts

[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.

Binding a domain to a network interface controller (NIC)

Binding different customer domains to different NICs can resolve issues with device addressing. For example, if your two of your customer' domains have overlapping IP addresses, and you are using Network Manager on a single server to manage both of these networks, then by binding these two customer domains to separate NICs, you enable Network Manager to uniquely address these IP addresses.

About this task

For example, assume that you have two customers A and customer B, and these two customers have overlapping IP address ranges. For example, assume that they both have a router with IP address 192.168.1.1. You are using Network Manager on a single server to manage both customers networks. The

problem is: how are Network Manager processes able to distinguish between these two devices. For example, if you ping the IP address 192.168.1.1 which customer router is pinged?

To resolve this and similar issues, perform the following steps:

Procedure

1. Install two separate NICs on the Network Manager server.

The cable from NIC A leads to customer A's network and the cable from NIC B leads to customer B's network.

Note: You might need to install more than two NICs. The steps given here are for illustrative purposes and apply to the example given earlier in this topic.

2. Assign NIC A to customer A's domain and NIC B to customer B's domain by adding the following lines to the \$NCHOME/etc/precision/ServiceData.cfg configuration file.

```
SERVICE: IPv4BindAddress DOMAIN: CUST_A_DOMAIN ADDRESS: NIC_A_IP_ADDR PORT: 0
SERVERNAME: itnmserver DYNAMIC: NO
SERVICE: IPv4BindAddress DOMAIN: CUST_B_DOMAIN ADDRESS: NIC_B_IP_ADDR PORT: 0
SERVERNAME: itnmserver DYNAMIC: NO
```

Where:

- *CUST_A_DOMAIN* is the domain name for customer A.
- *CUST_B_DOMAIN* is the domain name for customer B.
- *NIC_A_IP_ADDR* is the IP address of the NIC assigned to customer A's domain.
- *NIC_B_IP_ADDR* is the IP address of the NIC assigned to customer B's domain.

This ensures that each domain will use a different NIC and the packets from each domain will go to the appropriate customer.

3. Save the \$NCHOME/etc/precision/ServiceData.cfg configuration file.

Configuring a dNCIM database on Linux on IBM z Systems

On Linux on IBM z Systems, you need to make some configuration changes to the dNCIM database. By default, the dNCIM database is implemented using the SolidDB database. This database is automatically installed and there is no need to perform any setup tasks. However, SolidDB is not supported on Linux on IBM z Systems. If you are working on Linux on IBM z Systems and you want to use dNCIM, you must install an alternative database and configure it to work with the Discovery engine, **ncp_disco**.

About this task

To configure a dNCIM database on Linux on IBM z Systems complete the following tasks:

Procedure

1. Create an entry for the database in the DbLogins.*domain*.cfg file, where *domain* is the name of your domain.

For example:

```
insert into config.dbserver
(
    m_DbId,
    m_Server,
    m_DbName,
    m_Schema,
    m_Hostname,
    m_Username,
    m_Password,
    m_PortNum,
    m_EncryptedPwd
    m_EmbeddedProcess
    m_ScriptTimeoutSecs
)
```

```

values
(
    "DNCIM",
    "Db2",
    "ITNM",
    "dncim",
    "localhost",
    "user",
    "password",
    50000,
    1
    "ncp_disco"
    100
);

```

In this insert, the `m_ScriptTimeoutSecs` argument sets a timeout in seconds for any SQL scripts that run against this database. A timeout might be necessary if the dNCIM database is slow; for example, when the database is not embedded into **ncp_disco** or with a slow database server.

Note: In this example, the database is local to the Discovery engine, **ncp_disco**, and so the `m_Hostname` attribute is set to `localhost`. Keeping the database local to the discovery process ensures faster discoveries.

2. Populate the schema for the database by using the `$NCHOME/precision/scripts/sql/create_db_schemas.pl` Perl script.

For example:

```
./create_db_schemas.pl -server oracle|db2|| -dbname dbname -schema schema -
host hostName -username username -password password -port port -action ncim
```

Where:

- The `-server` attribute is the type of database.
 - The `dbname` attribute varies with the type of database.
 - On Oracle, use the SID value.
 - On Db2, use the value `m_DbId` from the `DbLogins.domain.cfg` insert.
 - The `schema` matches the `m_Schema` argument from the `DbLogins.domain.cfg` insert. For example, set `schema` to `dncim` to match the example insert in step 1.
- Note:** You can give the database schema any name. The value that you use for `m_Schema` in the `DbLogins.domain.cfg` insert must match the value you use for the `-schema` argument in the `create_db_schemas.pl` script.
- The `-action` attribute takes the value `ncim` because the dNCIM and NCIM databases are identical in format.

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.

About this task

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 Administration Guide*.
- For polling, see the *IBM Tivoli Network Manager IP Edition Administration 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 Administration Guide*.

Activating SNMP Helper throttling

You can activate SNMP Helper throttling.

About this task

To activate SNMP Helper throttling, perform the following steps:

Procedure

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 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.

About this task

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.

Procedure

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.

About this task

The SNMP Helper determines the value of the maximum number of repetitions for GetBulk requests (the max-repetitions parameter) based on the following calculation:

$$\text{max-repetitions} = \text{DefaultGetBulkMaxReps} / \text{\#varbinds}$$

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.

Procedure

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 authentication

You can configure different components of Network Manager to use different authentication methods.

About this task

For more information about single sign-on, see *Configuring Jazz for Service Management for SSO* on the Jazz for Service Management IBM Knowledge Center at <https://www.ibm.com/support/knowledgecenter/SSEKCU>.

Changing the user authentication method

When you install Network Manager you can choose to authenticate the Network Manager users in a file-based authentication system or in the Tivoli Netcool/OMNIbus ObjectServer.

About this task

If you want to change the authentication method after installation, for example to use LDAP, follow the same instructions as for changing the authentication method for Tivoli Netcool/OMNIbus. Refer to information about *Configuring user authentication*. See the topic *Configuring user authentication* within the *IBM Tivoli Netcool/OMNIbus Installation and Deployment Guide*.

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.

About this task

The OQL Service Provider authentication engine, `ncp_auth` is no longer used in Network Manager versions 3.9 and later. 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:

Procedure

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,
);
```

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: https://www.ibm.com/support/knowledgecenter/SSLVC/welcome/isa_welcome.html

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.

About this task

To install the ISA Lite collector, perform the following steps:

Procedure

1. Install Network Manager.
2. Open the following technote: <http://www.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.

Notices

This information applies to the PDF documentation set for IBM Tivoli Network Manager IP Edition.

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 17 on page 213](#) are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Table 17. IBM trademarks

AIX	Informix®	PR/SM
BNT	iSeries	System p
ClearQuest®	Lotus®	System z®
Cognos®	Lotus	Tivoli
Db2	Netcool	WebSphere
Db2 Universal Database	NetView®	z/OS®
developerWorks®	OMEGAMON®	z/VM®
DS8000	Passport Advantage	zSeries
Enterprise Storage Server®	PowerPC	
IBM	PowerVM®	

Adobe, Acrobat, Portable Document Format (PDF), PostScript, and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

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 may collect IP addresses, user names and passwords for the purpose of performing network discovery. Failure to enable the collection of this information would likely eliminate important functionality provided by this Software Offering. You as customer should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

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> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details>, and the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www.ibm.com/privacy>.



Part Number:

Printed in the Republic of Ireland

2021-4213-01



(1P) P/N: