Network Manager IP Edition
Version 3 Release 9

Network Visualization Setup Guide

IBM

SC27-2764-04

Network Manager IP Edition
Version 3 Release 9

Network Visualization Setup Guide

SC27-2764-04

Note

Before using this information and the product it supports, read the information in "Notices" on page 115.

This edition applies to version 3.9 of IBM Tivoli Network Manager IP Edition (product number 5724-S45) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this publication

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

The *IBM Tivoli Network Manager IP Edition Network Visualization Setup Guide* describes how to use Network Manager IP Edition to visualize your discovered network.

Intended audience

This publication is intended for network operators who are responsible for monitoring the health of the network.

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

What this publication contains

This publication contains the following sections:

- Chapter 1, “Administering the Web console,” on page 1

  Describes how to use the functions of the Web console to administer pages, folders, views, portlets, and console preference profiles.
- Chapter 2, “Administering network views,” on page 33

  Describes how to create new views or change existing network views to help network operators visualize devices.
- Chapter 3, “Configuring tools and menus,” on page 83

  Describes how to create and edit context menus, configure user access to menu items, define the context in which menus are available, and create tools that can be run from the context menus.
- Chapter 4, “Editing network topology,” on page 101

  Describes how to edit the discovered network topology by performing the following actions: adding network devices, adding connections between network devices, removing devices from the domain, and removing connections between network devices.

Publications

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

Your Network Manager library

The following documents are available in the Network Manager library:

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

  Gives important and late-breaking information about IBM Tivoli Network Manager IP Edition. This publication is for deployers and administrators, and should be read first.
- *IBM Tivoli Network Manager Getting Started Guide*, GI11-9353-00

  Describes how to set up IBM Tivoli Network Manager IP Edition after you have installed the product. This guide describes how to start the product, make sure it is running correctly, and discover the network. Getting a good network discovery is central to using Network Manager IP Edition successfully. This guide describes how to configure and monitor a first discovery, verify the results of the discovery, configure a production discovery, and how to keep the network topology up to date. Once you have an up-to-date network topology, this guide describes how to make the network topology available to Network Operators, and how to monitor the network. The essential tasks are covered in this short guide, with references to the more detailed, optional, or advanced tasks and reference material in the rest of the documentation set.
- *IBM Tivoli Network Manager IP Edition Product Overview*, GC27-2759-00

  Gives an overview of IBM Tivoli Network Manager IP Edition. It describes the product architecture, components and functionality. This publication is for anyone interested in IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition Installation and Configuration Guide*, SC27-2760-00

  Describes how to install IBM Tivoli Network Manager IP Edition. It also describes necessary and optional post-installation configuration tasks. This publication is for administrators who need to install and set up IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition Administration Guide*, SC27-2761-00

  Describes administration tasks for IBM Tivoli Network Manager IP Edition, such as how to administer processes, query databases and start and stop the product. This publication is for administrators who are responsible for the maintenance and availability of IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition Discovery Guide*, SC27-2762-00

  Describes how to use IBM Tivoli Network Manager IP Edition to discover your network. This publication is for administrators who are responsible for configuring and running network discovery.
- *IBM Tivoli Network Manager IP Edition Event Management Guide*, SC27-2763-00

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

- *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*, GC27-2765-00

  Describes how to use IBM Tivoli Network Manager IP Edition to troubleshoot network problems identified by the product. This publication is for network operators who are responsible for identifying or resolving network problems.
- *IBM Tivoli Network Manager IP Edition Network Visualization Setup Guide*, SC27-2764-00

  Describes how to configure the IBM Tivoli Network Manager IP Edition network visualization tools to give your network operators a customized working environment. This publication is for product administrators or team leaders who are responsible for facilitating the work of network operators.
- *IBM Tivoli Network Manager IP Edition Management Database Reference*, SC27-2767-00

  Describes the schemas of the component databases in IBM Tivoli Network Manager IP Edition. This publication is for advanced users who need to query the component databases directly.
- *IBM Tivoli Network Manager IP Edition Topology Database Reference*, SC27-2766-00

  Describes the schemas of the database used for storing topology data in IBM Tivoli Network Manager IP Edition. This publication is for advanced users who need to query the topology database directly.
- *IBM Tivoli Network Manager IP Edition Language Reference*, SC27-2768-00

  Describes the system languages used by IBM Tivoli Network Manager IP Edition, such as the Stitcher language, and the Object Query Language. This publication is for advanced users who need to customize the operation of IBM Tivoli Network Manager IP Edition.
- *IBM Tivoli Network Manager IP Edition Perl API Guide*, SC27-2769-00

  Describes the Perl modules that allow developers to write custom applications that interact with the IBM Tivoli Network Manager IP Edition. Examples of custom applications that developers can write include Polling and Discovery Agents. This publication is for advanced Perl developers who need to write such custom applications.
- *IBM Tivoli Monitoring for Tivoli Network Manager IP User's Guide*, SC27-2770-00

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

Prerequisite publications

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

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

  Includes installation and upgrade procedures for Tivoli Netcool/OMNIbus, and describes how to configure security and component communications. The publication also includes examples of Tivoli Netcool/OMNIbus architectures and describes how to implement them.
- *IBM Tivoli Netcool/OMNIbus User's Guide*, SC23-9683

  Provides an overview of the desktop tools and describes the operator tasks related to event management using these tools.
- *IBM Tivoli Netcool/OMNIbus Administration Guide*, SC23-9681

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

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

  Contains introductory and reference information about probes and gateways, including probe rules file syntax and gateway commands.
- *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide* SC23-9682

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

Accessing terminology online

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

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

Accessing publications online

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

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

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

Ordering publications

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

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

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

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

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

Accessibility

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

Accessibility features

The following list includes the major accessibility features in Network Manager:

- The console-based installer supports keyboard-only operation.
- The console-based installer supports screen reader use.
- Network Manager provides the following features suitable for low vision users:
  - All non-text content used in the GUI has associated alternative text.
  - Low-vision users can adjust the system display settings, including high contrast mode, and can control the font sizes using the browser settings.
  - Color is not used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.
- Network Manager provides the following features suitable for photosensitive epileptic users:
  - Web pages do not contain anything that flashes more than two times in any one second period.

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

Extra steps to configure Internet Explorer for accessibility

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

To enable high contrast mode, complete the following steps:

1. Click **Tools** > **Internet Options** > **Accessibility**.
2. Select all the check boxes in the Formatting section.

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

IBM® and accessibility

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

Tivoli technical training

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

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

Support information

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

Online

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

IBM Support Assistant

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

Conventions used in this publication

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

Typeface conventions

This publication uses the following typeface conventions:

Bold

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

Italic

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

`Monospace`

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

Operating system-dependent variables and paths

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

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

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

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

Chapter 1. Administering the Web console

Use the functions of the Web console to administer pages, folders, views, portlets, and console preference profiles.

Tip: If you do not find the information that you require in this publication, see the IBM Websphere Application Server Information Center at the following Web address:

http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.zseries.doc/info/welcome_nd.html

Note: The default ports for logging into the application server are different across versions. The nonsecure access redirects you to the secure port unless you configured it otherwise (see Configuring access for HTTP and HTTPS). The default ports for the Network Manager V3.9 release are as follows:
- `https://`*`localhost`*`:16311/ibm/console` (secure access).
- `http://`*`localhost`*`:16310/ibm/console` (nonsecure access).

Console layout

The layout of the console user interface has these major elements.

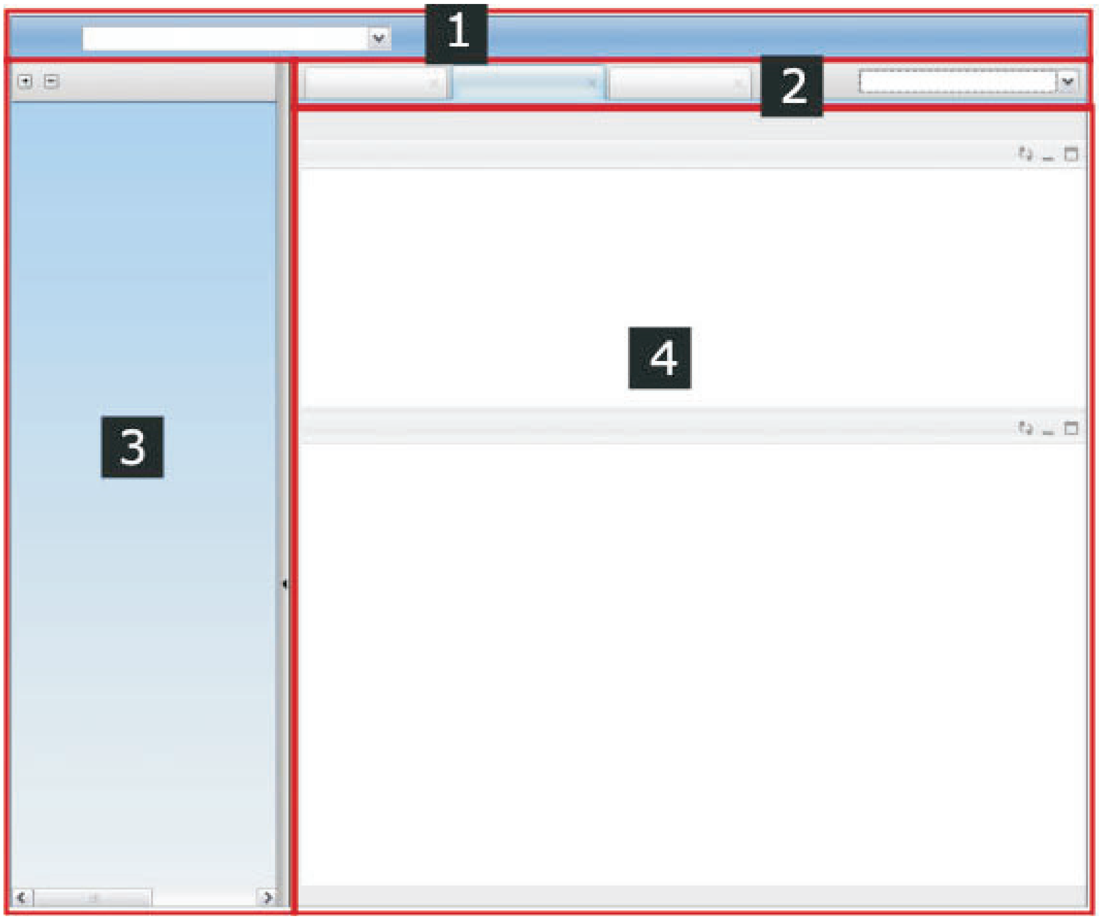


Figure 1. Console layout

1 Banner
Displays a common image across all console installations. The banner includes a greeting to the user as well as links to log out of the console and to open console help. The **View** selection list in the banner controls which nodes are displayed in the navigation as well as pages that are opened when the view is selected.

2 Page bar
Displays tabs to select between open pages. The page bar allows you to work on different pages without closing the page or losing unsaved data. For example, if you are working on an application on Page A, you can open an application on another page to gather information about a resource that you need to finish the form on Page A without losing any unsaved data you have already entered. Multiple pages can be opened at one time, but only one of the open pages is in focus (*current page*). The page bar also contains a **Select Action** drop-down list for performing actions on the current page.

3 Navigation pane
Displays a set of navigation nodes used for accessing content. The nodes shown in the navigation pane are only those to which you have access.

4 Work area
Displays the current page that you are working on. The page contains one or more Web applications or *portlets*, each in its own portlet window with a title bar.

Setting up the console

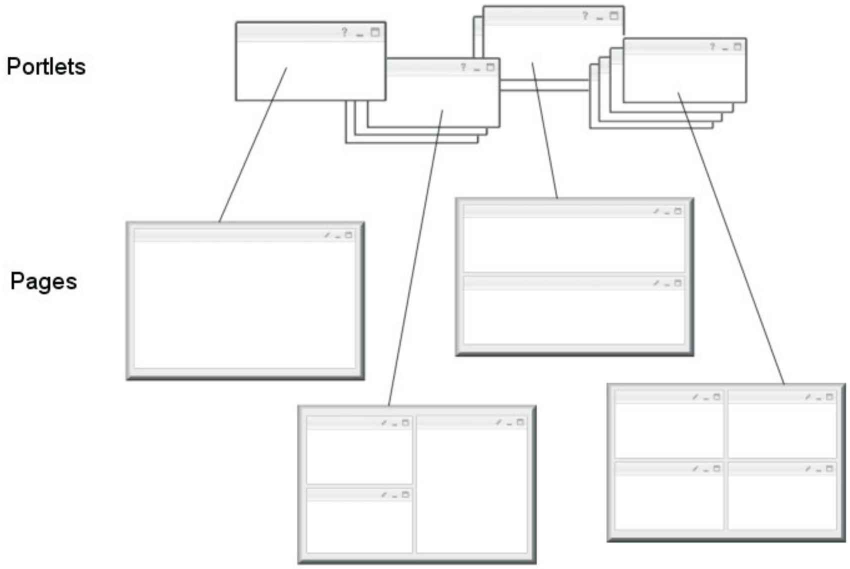
For a new console installation, the console administrator needs to create the experience for users when they log into the console. This task involves working through the console content from the basic building blocks to the high level organization and presentation of these resources so that users can quickly find what their way around and perform their tasks efficiently.

To get started setting up the console, you should already be familiar with the concepts and characteristics of the console layout. You should take time navigating through the console to become familiar with the portlets, pages, views, roles, and preference profiles that are provided. As you work with the console, you will create some of these resources to suit your organization's needs.

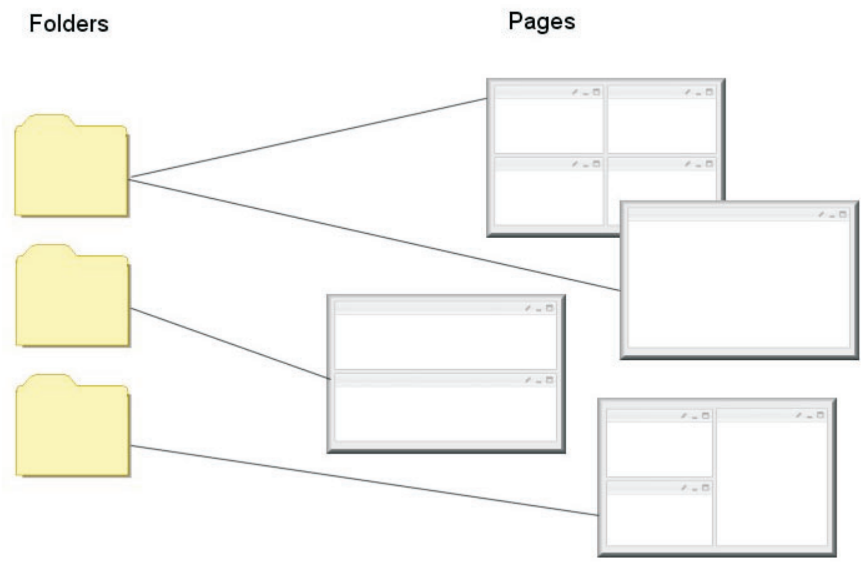
Understanding the structure of the console

Access to each level in the console organization is assigned based on the users' roles. Keep each role in mind when planning how to structure the console.

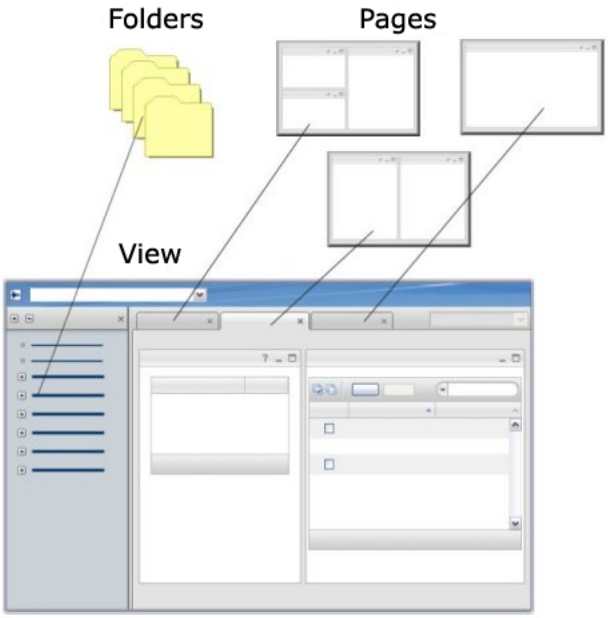
Content in the console is composed of portlets. The following figure shows how portlets are arranged on a page using a row and column layout. Access to each page, and to each portlet on each page, is assigned to users based on their defined role.



Each page is accessed from the console navigation, either from the console root or they can be grouped into folders. The hierarchical structure of the navigation affects how quickly users can find a page and work with the portlets on that page.



Folders and pages can be assembled into views that the user can select from the View drop-down list in the banner. Each view can include pages that are initially launched when the view is selected.



Finally, you can define a set of preferences, called a *preference profile*, that determines what views are available to each role, and whether the navigation should be displayed.

Process for planning and setting up the console

Setting up the console is an iterative process. While you should initially start with organizing pages, roles, and portlets and work your way up to setting up views and preference profiles, over time you will need to come back to any of these steps to make changes.

1. Define your console users and what tasks they perform. Console users are assigned to roles, which are used to determine what tasks they can perform in the console. As you assess the users' tasks, think about how these roles will be defined. Consider how the community of console users will be assigned to different roles and whether there are any existing roles that you can use, or if you need to create new roles.

   Roles can be created without assigning access to any resources. This step can be performed later.
2. Review the content. Users' tasks are performed using portlets on console pages. You need to understand what portlets are available and how they will be used to perform these tasks. For each portlet, determine which roles should have access and which roles should be restricted.
3. Create a navigation structure of pages and folders. Determine which pages are currently used to access the portlets. Are these pages sufficient for the roles that you have defined, or do you need to create new pages? For existing pages, do you need to add or remove any portlets or change the way they are arranged on the page? Consider that multiple roles can access a page with different access to the portlets on that page.

   Review the folders in the navigation and the pages that are contained in these folders. Do these folders help the users find their content? Do you need to edit existing folders or create new folders? Should you move any pages between folders? What folders or pages should be hidden for each role?
4. Organize the content and navigation into views. Determine which navigation folders and pages have a related purpose for each role. You can define one or more views for each role, and even make a single view appear differently between roles based on access control. Each view can also include one or more pages that are launched when the view is selected. Each of these options is provided to help remove other content and pages that can distract users.
5. Define the presentation for each role Determine which views should be available to users in a role. For some roles, you can remove the navigation bar and just provide a set of startup pages. You can assign exactly one preference profile per role.
6. Test the console for each role. Create a test user for each role. Log into the console as each user and verify the use cases.
   - The navigation is shown or not, depending on the setting in the console preference profile.
   - The view selection list shows only the views to which the role has access and as defined by the preference profile.
   - Each view shows only the navigation nodes and startup pages allowed for that role.
   - Each folder shows only the pages allowed for that role.
   - Each page launched in the navigation shows only the portlets allowed for that role.
   - If the role has Editor access to a page, the **Edit Page** option is available in the **Page Actions** selection list. This option is not showing if the user's role does not have Editor access.

- Each page shows only the portlets allowed for that role.
- The portlet title bar provides an **Edit Options** icon that provides access to two options, a **Personalize** option, and an **Edit Shared Settings** option. The **Personalize** option is available, if the user's role has Privileged User access. The **Edit Shared Settings** option is available if the user's role has Editor access. Otherwise, neither of these options are available.

Go back and make corrections as indicated by the results of your testing.

7. Move the console to production use. Assign roles to actual users and notify the user community that the console server is ready for use.

Working with pages

Console content is composed of pages, folders, and external URLs. Each of these resources is represented in the navigation pane as a node. Click **Settings** > **Page Management** to create, edit, and delete pages and folders for the console navigation. You can also edit external URLs that are launched from the navigation pane. You cannot create URLs in the console. Instead, URLs are created when an application is deployed to the console that includes the URL node in its descriptors.

Field descriptions

This section describes the fields and controls in the main panel of Page Management.

Select all icon
Selects all items displayed in the table for deletion. If you are displaying only a filtered set of items, only those items are selected. You can deselect specific items before actually deleting.

Deselect all icon
Deselects all items displayed in the table.

New Page
Opens a panel for creating a new page.

New Folder
Opens a panel for creating a new folder.

Delete Immediately deletes all selected items in the list. Only Custom resource types can be deleted.

Filter Type in this field to quickly find an item in the table. This field is useful when there are a large number of items to look through.

Select Selects or deselects a single item in the table.

Name Displays the title of the page as it is shown in the navigation.

Type Displays the type of page.

Unique Name
Displays the string used by the system to uniquely identify the page or folder.

Creating pages

To create a page, you must first select content for the page and specify the layout of the portlet window. You must then set the properties of the page, including the page name and its location in the navigation pane. All pages that are created in the console have a resource type of “Custom”.

To create a page for testing purposes:

1. To display the Create New Work Page portlet:
   - In the taskbar, click the **Create page** tab.
   - In the navigation pane, click **Settings** > **Page Management** and in the Page Management portlet, click **New Page**.

   A Page Settings page is displayed.
2. In the **Page name** field, provide a descriptive name for the page and in the **Page location** field indicate where you want the page to be displayed in the navigation pane. Consider the content on the page and how users will find that content by looking for the page name in the navigation pane.
3. Optional: Click the **Optional Setting** label and associate one or more roles with the new page and set the level of access for each role.
4. Click **Save**. The taskbar tab is updated with the name of the new page and a Choose a Portlet window is displayed.
5. To add a portlet, scroll through the list and select a portlet or use the **Filter** field to find the portlet you want to add.
6. Optional: Use the the **Horizontal split** icon or the the **Vertical split** icon to add more portlet containers to the page and select a portlet for each section.
7. Click **OK** in the Choose a Portlet window. The selected portlet is displayed.
8. Click **Save** to commit your changes.

The new page is displayed. Users with “editor” access to the page can add more content, arrange the content using horizontal and vertical layouts, and replace and remove content.

Make sure that the roles with access to this page also have access to the portlets that are on the page. You can also edit the new page to customize its page persistence settings and text direction settings.

Editing page content and layout

Pages are an arrangement of one or more portlets in the work area and contain the portlets needed to complete tasks. Users whose roles have “Editor” access to a page can edit a page's layout and content using the **Edit Page** option in the page action list. After saving changes to the layout and content, you can change a page's properties, including it's name and location in the navigation.

Note: User's with “Privileged User” access can change the size of portlet windows on the page.

1. Locate the page you want to edit in the navigation pane and open it.
2. In the page bar, select **Edit Page** from the page actions selection list. The page is changed to show buttons at the top. Each portlet title bar displays new icons for creating horizontal and vertical layouts and replacing and removing portlet content.
3. Optional: To add more portlets to the page, follow these steps.

   a. Create a window for the new portlet by splitting one of the windows displayed.
      - Use the **Horizontal split** icon to create a window below an existing window.
      - Use the **Vertical split** icon to create a window to the right of an existing window.

      The Portlet Picker is displayed within the new portlet window for selecting the portlet content.
   b. Scroll through the list or use the **Filter** field to find the portlet you want to add.
   c. Click **OK**. The portlet is added to the window.
4. Optional: To replace a portlet in a window, follow these steps.
   a. Click the **Replace content** icon in the title bar where you want to replace the portlet content. The Portlet Picker is displayed within the new window.
   b. Scroll through the list or use the **Filter** field to find the portlet you want to add.
   c. Click **Add Portlet**. The portlet is added to the window.
5. Optional: To remove a portlet and its window, click the **Delete** icon in the title bar. The content is removed immediately without a warning prompt.
6. Optional: To create wires between portlets so they can share information and updates, click **Show Wires**. Before working with wires, make sure that you have enough information about the events that a portlet supports.
7. Click **Page settings**. The page settings are displayed.
8. Optional: Make changes to the page's settings as required.
   a. Click the **General** tab.
   b. In the **Page name** field, provide a descriptive name for the page and in the **Page location** field indicate where you want the page to be displayed in the navigation pane. Consider the content on the page and how users will find that content by looking for the page name in the navigation pane.
   c. Use the **Navigation visibility** list to indicate whether or not you want the page to be listed in the navigation pane.
   d. From the **Page persistence** list, make one of the following selections:
      - Client side (default setting) - This setting preserves any changes that the user makes on the page when the user navigates away from the page. Changes include not only form data, but any state changes to portlets, for example, opening edit mode, switching to another panel in the portlet, or minimizing a portlet. Page data and page state are maintained on the client side until the user closes the page or logs out of the console.
      - None
      - Server side - This setting maintains unsubmitted or unsaved form data from a page when the user navigates away from the page. The data is saved on the server and fetched when the user returns to the page. Unsaved data is saved until the user closes the page or logs out of the console.

        Note: The Server side setting only applies to forms on a page. Any user interaction outside of a form is not maintained.
   e. Use the **Page tasking** radio buttons to indicate whether multiple instances of the page can be launched.

f. In the **Component direction** drop-down list, you can accept the **Default** setting to allow the component direction to be governed at console level or select one of the other settings to indicate whether you want to display page components from left-to-right or from right-to-left. If you select a setting other than **Default**, it will override any component direction setting that may be set at console or browser level.

g. In the **Text direction** drop-down list, you can accept the **Default** setting to allow the text direction to be governed at console level or select Left-to-Right or from Right-to-Left to indicate the direction that you want the page text to display. You can also select **Contextual Input** so that for pages that include text entry fields, the direction of text is dependent on the language used to enter data. If you select a setting other than **Default**, it will override any text direction setting that may be set at console or browser level.

9. Optional: Click the **Roles** tab to update the list of roles with permissions to the page and their access level. A list of all roles with access to the page is displayed.

Option	Description
To remove access for a role	Select a role and click **Remove**. The role is removed immediately from the access list without a warning prompt.
To add access for a role	Click **Add**. Select one or more of the roles displayed and click **OK**. The roles you added are included to the list.
To change the access level for a role	Select one of the options under **Access Level** for the role.

Attention: Make sure that the roles with access to a page also have access to the portlets that are on the page.

10. Optional: Click the **View Membership** tab to update the list of views that include this page.

Option	Description
To add this page to a view	Click **Add** and select one or more views.
To remove this page from a view	Select one or more views in the list and click **Remove**.

11. If you accessed the Page settings window and made changes, click **Save** to commit your changes and return to the main edit page window.
12. When you are satisfied with your updates, click **Save** to commite your changes.

You are returned to the page with your changes displayed.

Related reference:

"List of Network Manager portlets" on page 28
You can use Network Manager portlets for creating pages.

Arranging portlets using the drag-and-drop feature

When editing a page, you can drag portlets to any window on the page. The portlet must already be placed in a window on the page, and the target window must already exist.

The target window can be an empty window or it can already contain a portlet.

- If you drag a portlet into an empty window, the original window becomes empty after the portlet has been moved.
- If you drag a portlet into a window that already contains another portlet, the two portlets exchange windows.

1. Locate the mouse over the portlet title in the title bar. You cannot drop a portlet into another window by dragging from any other location in the portlet window or title bar. The portlet must be dragged using the title.
2. Drop the portlet in the target window when the target window displays a blue, dotted outline around the frame. The outline is the only indication that the portlet can be dropped into this location.

Creating folders

Folders are used to group nodes in the console navigation. All folders that are created in the console have a resource type of "Custom".

1. Click **Settings** > **Page Management** in the navigation pane. A Page Settings page is displayed.
2. Click **New Folder**. The properties panel for the new folder is displayed.
3. Complete the fields in the properties panel.
4. Click **Save** to save your changes and return to Page Management.

The new folder is displayed in the summary table. The folder is also displayed in the navigation pane once you have added page content to it. Add other nodes to the folder by editing their location properties.

Editing the properties of a page, folder, or external URL

You can edit the properties of custom and system navigation nodes, which include pages, folders, and external URLs. Properties of a node include its display name and its location in the navigation. You can also indicate whether multiple or only single instances of a page node can be launched in the console.

When changes are made to a system node, the updated system node is saved as `System - Customized`. You cannot delete a system node. Instead, you can restore the system node, which deletes the custom copy of it.

You can perform the following tasks when you edit a node's properties.

- Define who can access a page or external URL and the level of access
- Determine which view should include the node. When the view is selected, the page, folder, or URL is included in the navigation pane for that view.
- Change the name that is displayed in the navigation pane for a node.
- Change the location of a node in the navigation pane. For example, you can group pages into folders.

Attention: You cannot create URLs in the console. Instead, URLs are created when an application is deployed to the console that includes the URL node in its descriptors.

1. Click **Settings** > **Page Management** in the navigation pane. Page Management is opened displaying console navigation nodes in a summary table.
2. Locate the node that you want to edit in the table provided. Use the filter in the table to type in the node name and quickly display it.
3. Click the link for the node provided in the **Name** column. The properties panel for the node is displayed.
4. Make your changes to the node's Page, Folder, and External URL properties.
5. Click **Save** when you have finished.

The changes you made are reflected in the navigation pane.

Deleting custom pages and folders

You can delete only pages with the resource type of `Custom`. These are nodes created using the console.

System nodes that have been customized can be restored.

Attention: Before deleting a page or folder, consider whether any users are actively using the resource and any impacts this might have on services. If necessary, notify users in advance of any plans for changes that could affect their work.

1. Click **Settings** > **Page Management** in the console navigation. Page Management is opened displaying console navigation nodes in a summary table.
2. Locate the node that you want to delete in the table provided. Use the filter in the table to type in the node name and quickly display it.
3. Check the box in the **Select** column for the node. You can select more than one custom page or folder for deletion.
4. Click **Delete**. A message is displayed at the top prompting you to confirm the deletion.
5. Click **OK**.

The page or folder is deleted and removed from the navigation pane.

Restoring system pages, folders, and external URLs

System nodes are always preserved with their original settings. After making changes to a system node, the changes are saved in a customized copy of the page, folder, or URL. When you restore a system node, the customized copy is deleted and the original system node is restored in its place.

To delete the customized copy and restore the system node, follow these steps.

1. Click **Settings** > **Page Management** in the console navigation. Page Management is opened displaying console navigation nodes in a summary table.
2. Locate the node that you want to edit in the table provided. Use the filter in the table to type in the node name and quickly display it.
3. Click the link for the node provided in the **Name** column. The properties panel for the node is displayed.
4. Scroll to the bottom of the panel and click **Restore**.
5. Click **OK** to save your changes.

You are returned to the main panel of Page Management. The resource type of the node is displayed as `System`.

Working with views

Views are a defined set of tasks that are displayed in the console navigation pane. Views also can include one or more pages that are launched when the view is selected.

For example, if you find a set of tasks related to obtaining sales and cost reports from retail stores throughout a region, you could create a view called “Reports” that includes all of the pages associated with those tasks in the navigation. Each page, along with the folders that include them, would be added to the view. You could then set some of the most important pages to launch when the view is selected. In this way, views can make your experience with the console more productive than sorting through all of the navigation tasks that are displayed by default.

If you have sufficient access, you can create your own custom views. You can only edit system views.

To access View Management in the console, click **Settings** > **View Management** in the navigation.

Field descriptions

This section describes the fields and controls in the main panel of View Management.

Select all icon
Selects all items displayed in the table for deletion. If you are displaying only a filtered set of items, only those items are selected. You can deselect specific items before actually deleting.

Deselect all icon
Deselects all items displayed in the table.

New Opens a panel for creating a new view.

Delete Immediately deletes all selected items in the list. Only Custom resource types can be deleted.

Filter Type in this field to quickly find an item in the table. This field is useful when there are a large number of items to look through.

Select Selects or deselects a single item in the table.

View Name
Displays the name of the view as it is shown in the **View** selection list in the banner. Click the name to edit the view.

Type Displays the type of view. The actions you can perform on a view depend upon its type.

Role Count
Displays the number of roles that have access to this view..

Page Count
Displays the number of pages that are available in the console when the view is selected.

Creating views

Views determine what pages are listed in the navigation pane as well as which pages are launched when the view is selected. All views that are created in the console have a resource type of `Custom`. This procedure walks you through the task of creating a view for testing purposes. After completing these steps, you can remove or edit this view for production use.

You should understand the Console layout before starting this task.

1. Click **Settings** > **View Management** in the navigation pane. The View Management page is displayed with the list of system and custom views in the console.
2. Click **New**. The properties panel for the new view is displayed.
3. Enter a descriptive name for the view. This name is displayed in the **View** selection list in the banner.
4. Expand the **Roles with Access to This View** section and click **Add**. The **Add Roles** panel is displayed with a list of available roles. For this task, add a role that can be used to test the view before adding access for other roles.

   Attention: Granting access to the view does not grant access to the pages within the view.
5. Select your role in the table. You can use the filter to quickly find your role if the list of roles is very large.
6. Click **Add** after making your selection. You are returned to the view properties. The next step is to determine the pages that make up the view.
7. Expand the **Pages in This View** section and click **Add**. The **Add Pages** panel is displayed with a list of available pages.
8. Select several folders or pages in the list. Selecting a folder also selects all of the pages contained in that folder. You can individually deselect pages in a folder if necessary.
9. Click **Add** after making your selections. You are returned to the view properties.
10. Select the **Launch** option for two or three of the pages and select one of the launch pages as the default.
11. Click **Save** to save the new view and return to View Management.

Select the new view from the **View** drop down list located above the navigation pane. Verify that all pages and folder that you selected are displayed in the navigation, that the pages selected to launch are available is the page bar, and that the default selection has focus in the work area.

Editing views

Views provide a limited set of nodes in the console navigation and optional set of startup pages to help users focus on their tasks. If you have sufficient authorization in the console, you can change the view name, navigation content, and access permissions for system and custom views. You can delete only custom views. Changes you make to a system view are saved as *System Customized*.

1. In the navigation pane, click **Settings** > **Views**. The View Management page is displayed with the list of system and custom views in the console.
2. Click the view name in the list displayed in View Management. This displays the view's properties.

3. Optional: Expand **Roles with Access to This View** to update the list of roles with permissions to the view and their access level. A list of all roles with access to the view is displayed.

Option	Description
To remove access for a role	Select a role and click **Remove**. The role is removed immediately from the access list without a warning prompt.
To add access for a role	Click **Add**. Select one or more of the roles displayed and click **OK**. The roles you added are included to the list.
To change the access level for a role	Select one of the options under **Access Level** for the role.

   Note: Granting access to the view does not grant access to the pages within the view.

4. Optional: Expand **Pages in This View** to change which pages are displayed in the navigation when the view is selected.

Option	Description
Add a page to the view	Click **Add** to add a page to the view.
Remove a page from the view	Select the page in the **Select** column and click **Remove**. You can select multiple pages to remove.
Change the launch options for a page	Select **Launch** for each page that should be opened when the view is selected. Only one page can be in focus (current) when the view is selected. When multiple pages are set to launch, set the current page in the **Default** column.

5. Click **Save** to save your changes and return to the main view panel.

For customized versions of a system view, you can retrieve the system view settings by editing the system customized view and clicking **Restore**. The “system customized” version of the view is removed and replace by the original system view.

Deleting custom views

You can delete only views with the resource type of `Custom`. These are views created using the console.

Customized versions of system views can be restored. Restoring a `System Customized` view deletes the custom copy and replaces it with the original system view.

Attention: Before deleting a view, consider whether any users are actively using the view and any impacts this might have on services. If necessary, notify users in advance of any plans for changes that could affect their work.

Follow these steps to delete a custom view.

1. Click **Settings** > **View Management** in the console navigation. The View Management page is displayed with the list of system and custom views in the console.
2. Select the custom view that you want to delete. You can select more than one custom view.
3. Click **Delete**. A message is displayed at the top prompting you to confirm the deletion.
4. Click **OK**.

The custom view is removed from the view list.

Working with roles

Console users are granted access to resources based on the role to which they have been assigned. In the console navigation, click **Users and Groups** > **Role Management** to add and remove roles and to assign access to portlets, pages, and views.

To manage users and groups and assign them to roles, click **Users and Groups**.

After the console is installed, there are some roles already defined to the server.

Attention: The "suppressmonitor" role is used to hide the tasks associated with the application server, including the tasks in the Security, Troubleshooting, and Users and Groups folders.

Access levels

The access level that a role has to a resource determines the actions that users within that role can perform on the resource.

Table 1. Access rights to console resources based on access level

	Access Level		
Resource	**"User"**	**"Privileged User"**	**"Editor"**
Portlet	View and interact with the portlet and access portlet help	View and interact with the portlet, edit personal settings, and access portlet help	View and interact with the portlet, edit personal settings, edit global settings, and access portlet help
Page	Launch the node from the navigation		Launch the node from the navigation and edit the content and layout
Folder	**Note:** Folders are always available in the navigation if the user has access to at least one of its pages.		
External URL	Launch the node from the navigation		
View	Select the view		

For a given resource, if a role does not have one of these access level settings, then the role has no access to the resource.

Only users with “adminsecuritymanager” and “Administrator” role can create, delete or change the properties of a role. If you assign access for any other role to the Role Management portlet, users in that role will only be able to view roles and change access to views and pages.

Note: The access control settings are not observed when using the administrative portlets under the **Settings** node. Users with access to these pages and portlets will be able to create, edit, and delete all custom pages, portlets, and views. For example, if a user has no access to “Page Two”, but has access to Page Management, that user can edit all of the properties of “Page Two” and change access control settings. Keep this in mind when granting access to the **Settings** portlets for a role.

If a user is assigned to multiple roles, the user acquires the highest access level between these roles for a resource. For example, if a user belongs to the manager role with “Privileged User” access to a portlet and also belongs to the communications role with no access to the portlet, then the user has “Privileged User” access to the portlet.

Tasks

You can grant access for multiple roles while creating or editing a resource, such as a page or a portlet. You can also grant access to multiple pages or views while creating or editing a role.

Creating roles

Console users are granted access to resources based on the role to which they have been assigned. All roles that are created in the console have a resource type of `Custom`. This procedure walks you through the task of creating a role for testing purposes. After completing these steps, you can remove or edit this role for production use.

1. Click **Users and Groups** > **Role Management** in the navigation. A list of all roles in the console is displayed.
2. Click **New**. The properties panel for the new role is displayed.
3. Enter a descriptive name for the role.
4. Expand the **Access to Views** section. Use this section to grant access to one or more custom views for users who are assigned to the new role. If you have already created a custom view, follow these steps.
   a. Click **Add**. A list of available views is displayed.
   b. Select one or more views and click **OK**.
   c. To make sure the role has access to all of the pages within the view, click **Grant to All**.
5. Expand the **Access to Pages** section. A list of pages that the role can access is displayed. However, this list is empty if you did not add a view and grant access to all of the pages within the view.
6. Optional: Click **Add** to grant access to additional pages.
7. For each page that is listed, verify that the **Access Level** is set correctly.
8. Click **Save** to save your changes and return to Role Management.

The new role is created with access to the views and pages that you indicated. To grant access to the portlets on those pages you must edit the portlets.

Editing roles

Console users are granted access to resources based on the role to which they have been assigned. If you have sufficient authorization in the console, you can change the name of custom roles. For all roles, you can change access to views and pages and set the access level to pages.

1. In the navigation pane, click **Users and Groups** > **Role Management**. A list of all roles in the console is displayed.
2. Click the name of the role that you want to edit. The properties panel for the role is displayed. If this is a custom role, the only field you can edit is **Role Name**. For all other resource types, you cannot edit any of the role properties.
3. Expand the **Access to Views** section. Use this section to grant access to one or more custom views for users who are assigned to the new role. If you have already created a custom view, follow these steps.
   a. Click **Add**. A list of available views is displayed.
   b. Select one or more views and click **OK**.
   c. To make sure the role has access to all of the pages within the view, click **Grant to All**.
4. Expand the **Access to Pages** section. A list of pages that the role can access is displayed. However, this list is empty if you did not add a view and grant access to all of the pages within the view.
5. Optional: Click **Add** to grant access to additional pages.
6. For each page that is listed, verify that the **Access Level** is set correctly.
7. Click **OK**.

Your changes are saved and you are returned to the Role Management page.

For any pages that you added for the role, you should ensure that the role also has access to the portlets on the page..

Deleting custom roles

You can delete only roles with the resource type of `Custom`. These are roles created using the console.

Attention: Before deleting a role, consider whether any users are actively using the role and any impacts this might have on services. If necessary, notify users in advance of any plans for changes that could affect their work.

Follow these steps to delete a custom role.

1. Click **Users and Groups** > **Role Management** in the navigation pane. The Role Management page is displayed with the list of roles in the console.
2. Select the custom role that you want to delete. You can select more than one custom role.
3. Click **Delete**. A message is displayed at the top prompting you to confirm the deletion.
4. Click **OK**.

The custom role is removed from the list.

Working with portlets

Portlets are web applications that display information or provide a service in a console page. You can only work with portlets that have been deployed to the console. Use Portlet Management to create, edit, and delete portlet from a page.

To access Portlet Management in the console, click **Settings** > **Portlet Management** in the navigation. The main panel displays a list of all of the portlets in the console. Within the list, the portlets are grouped into the pages and folders as they are located in the console navigation. The group `Uncategorized portlets` indicates portlets that are not placed on a page within the navigation. To place a portlet on a page, you have to edit the page.

A delete icon to the right of a portlet indicates that it is a copy.

Field descriptions

This section describes the fields and controls in the main panel of Portlet Management.

Select all icon
Selects all items displayed in the table for deletion. If you are displaying only a filtered set of items, only those items are selected. You can deselect specific items before actually deleting.

Deselect all icon
Deselects all items displayed in the table.

Copy Creates a copy of all selected portlets and updates the table. Copied portlets are placed in the `Uncategorized portlets` folder with the name `Copy of` *`Original Portlet Name`*.

Filter Type in this field to quickly find an item in the table. This field is useful when there are a large number of items to look through.

Select Selects or deselects a single item in the table.

Portlet Name
Displays the title of the portlet as it is shown on the page.

Unique Name
Displays the name used by the console to uniquely identify this portlet.

Delete For portlet copies only, shows the **Delete** icon to remove the portlet from the system. Clicking this icon removes the portlet copy immediately without a warning prompt.

Creating portlets

You can create a new copy of an existing portlet. You can create many different portlet copies, or *portlet entities*, of a single portlet, each entity with a different name. The portlet must already be installed to the console for you to create a copy of it.

Note: If you are creating a new copy of a portlet, add your own role to the portlet access list so that you can view the portlet when it is placed on a page.

Follow these steps to create a copy of a single portlet.

1. Click **Settings** > **Portlet Management** in the navigation pane. A list of all of the console portlets is displayed in a scrollable table.

2. Browse through the list or use the **Filter** field to locate the portlet you want to copy. To use the filter field, start typing the portlet name. The list is reduced to portlets whose names match the characters you enter.
3. Check the box next to the portlet and click **Copy**. The portlet properties panel is opened. The **Portlet Entity Title** field displays the original portlet's title prefixed with `Copy of`.
4. Click the new portlet name.
5. Enter a new, descriptive name for **Portlet Entity Title**. In most circumstances, the entity title becomes the display name.
6. Click **Roles with Access to This Portlet**. The list of roles with access is based on the access list of the original portlet.
7. Use the **Add** and **Remove** buttons to update the list. For each role, verify their access level is set correctly.

   Attention: You must add your own role to this list to access the portlet copy on any page it is placed.
8. Click **Save** to save your changes and return to Portlet Management.

Now that you have finished creating your portlet copy, use Page Management to place the portlet on a page.

To create copies of multiple portlets, follow these steps, but select multiple portlets from the list before you click **Copy**. This adds each new portlet copy to the list under `Uncategorized portlets`. Click each portlet in the list to change the title.

Editing portlets

Portlets provide content on a console page, for example, viewing system information or submitting reports. If you have sufficient authorization in the console, you can change access permissions to a portlet. For copies of portlets that have been created, you can also change the display name of the portlet. If you want to place a portlet on a page, you have to edit the page and select the portlet from the displayed list.

1. Click **Settings** > **Portlet Management** in the console navigation. A list of all of the console portlets is displayed in a scrollable table.
2. Browse through the list or use the **Filter** field to locate the portlet you want to edit. To use the **Filter** field, start typing the portlet name. The list is reduced to portlets whose names match the characters you enter.
3. Click the name of the portlet that you want to edit. The portlet properties are displayed.
4. Optional: Enter a descriptive name for the portlet. The portlet name can be changed only if this is a copy of a portlet.
5. Optional: Expand **Roles with Access to This Portlet** to update the list of roles with permissions to the portlet and their access level. A list of all roles with access to the portlet is displayed.

Option	Description
To remove access for a role	Select a role and click **Remove**. The role is removed immediately from the access list without a warning prompt.
To add access for a role	Click **Add**. Select one or more of the roles displayed and click **OK**. The roles you added are included to the list.

Option	Description
To change the access level for a role	Select one of the options under **Access Level** for the role.

6. Optional: Use the **Component direction** and **Text direction** fields to set the direction to display portlet content and text. For both portlet content and text, the **Default** option allows the portlet to inherit the display direction that is set at page level. You can set the text and content direction at portlet level to either left-to-right or right-to-left. Additionally, in the **Text direction** list, you can also select **Contextual Input** so that for portlets that include text entry fields, the direction of text is dependent on the language used to enter data.
7. Click **Save** to save your changes and return to the main portlet panel.

Editing portlet shared settings

Some portlets include an *Edit Shared Settings* mode that allows users with “Editor” access level to configure common settings for other users of the portlet. Once shared settings are configured, users with “Privileged User” level of access can change these values for their own personal use of the portlet. Default settings cannot be changed by users with “User” level of access. Follow these steps to set the shared settings for a portlet.

You must have “Editor” access to the portlet to perform this task.

1. Navigate to the page where the portlet is located.
2. Click the **Edit options** icon in the portlet title bar. Two options are displayed: **Personalize** and **Edit Shared Settings**.

   Attention: If this icon is not available in the portlet title bar, then either the portlet does not support *Edit Shared Settings* mode, or you do not have “Editor” access for the portlet.
3. Select **Edit Shared Settings**. The portlet displays shared settings that can be changed.
4. Make any changes to the settings and submit them when you are finished. The portlet might provide a **Save**, **OK**, or **Submit** button. Once you have submitted your changes, you should be returned to the main panel for the portlet. If not, click the **Back** icon in the title bar.

The shared settings for using this portlet are saved. If the portlet is located on more than one page, the updated settings will be observed on the other pages as well.

The updated settings configuration only affect settings that have not been personalized by users. To verify that the a user's preferences have been preserved, log in with a test user name and verify that the shared settings are set as intended.

Related reference:

“Editable portlet parameters” on page 29
Use this information to understand which parameters are associated with each Network Manager portlet and how each of these parameters affects the appearance of the portlet.

Deleting portlets

You can use the console to delete only a copy of a portlet. To remove the original portlet, the console administrator must undeploy the console module application to which the portlet belongs.

1. Click **Settings** > **Portlets** in the console navigation. A list of all of the console portlets is displayed in a scrollable table.
2. Browse through the list or use the Filter field to locate the portlet you want to remove. To use the filter field, start typing the portlet name. The list is reduced to portlets whose names match the characters you entered.
3. Click the **Delete** icon.

The portlet is removed immediately without a warning prompt.

Portlet events and wires

You can create connections, or *wires*, between portlets so that they can exchange messages with each other. When an action occurs in a source portlet, it creates an *event*, which contains information that can be sent to other portlets.

Before working with wires on a page, you must first open the page for editing.

Not all portlets support wires and events. Portlets must use specific code to process events that are sent or received through a wire. Each portlet is designed to process certain events. You should have thorough knowledge of the portlets and the events that they support before creating or editing wires. To determine if a portlet supports an event, click the **Events** icon to view a list of all events that the portlets subscribes to or publishes.

Some target portlets are capable of processing events after they have been transformed to match certain criteria. For example, an event that sends the cost of a transaction in one currency might need to be transformed to a different currency before the target portlet can receive it. When you create a wire, you have the option of selecting a transformation for the event, if the target portlet requires it. The console provides the Simple String Transformation to transform from one event to another. Other transformations might be available from other applications in the console.

The target portlet can be on the same or on a different page from the portlet that is the source of the event. A page can also be the target of a wire. In this case, all portlets on the target page can receive the event. In response to the event, the target portlet can update its content.

You can work with wires using the wire summary panel or the drag-and-drop feature.

Related reference:

"Inter-portlet actions" on page 29
Use this information to understand how Network Manager portlets communicate with each other when placed on the same page.

Using the wire summary panel

These steps describe how to create a new wire. You can also edit and delete wires using this panel.

1. Click **Show Wires**. The Summary of wires panel is displayed. The Wire Type column indicates whether the existing wires are system or custom.
   - System wires are created by applications in the console. You cannot create, edit, or delete system wires.
   - Custom wires are created by console users with “Editor” access to a page. You can also edit and delete these wires as necessary.
2. Click **New Wire**. A dialog is displayed that allows you to select an event provided by a source portlet on the page. If no events are listed, then you cannot create a wire from this page. You can select from the events listed to read a description of each event.
3. Select one of the available source events for the new wire and click **OK**. A dialog is opened that allows you to select the target for the new wire. You can browse through the pages and folders listed to select a target portlet or page, or use the search field to find the target.
4. Select a target for the new wire.
5. Optional: If the target is on another page, select from the following options.
   - **Load the selected target page**

     This option opens the target page if it is not already opened when the event is launched.
   - **Switch to the selected target page**

     This option makes the target page the current page when the event is launched.
6. After you have finished making your selections, click **OK**. A dialog is opened that allows you to select from a list of transformations. Transformations are used to change event names or parameters so that the target can process them. You should be familiar with the transformation and target before defining a transformation for the wire. You can select from the list of transformations to read a description.
7. Select the transformation for the new wire, or select `None` if no transformation is needed, and click **OK**. If you selected “Simple String Transformation”, select a target event from the list and select the source parameter names for each target parameter in the list. When the original event is sent, it is transformed into this target event before it is received by the target portlet.

The new wire is created and added to the wire summary for the page.

When you are finished making changes to the page, click **Save**.

Using the drag-and-drop feature

Portlets register the events that they support to the console. If it is a subscribed event, the portlet can be a target of the event and receive the event message. If it is a published event, the portlet is the source of the event and sends the event message. When editing a page, some portlets might display the **Events** icon in the title bar. Click this icon to view the events that the portlet has registered with the console.

You can create wires by dragging the events from the source portlet to another portlet on the page. Wires to other pages must be created using the **Summary of wires** table.

1. In the portlet title bar, click the **Events** icon. The portlet window replaces the portlet with a list of events supported by the portlet.

   Note: There is an **Enable** checkbox next to each event in the list. Unchecking this box disables all custom and system wires associated with the event and source portlet. Your selection to enable or disable the event overrides preceding selections for the same event that could have been made for other custom wires with other portlets.
2. To create a wire from a source portlet, drag an event listed under **Published Events** to another portlet on the page. The target portlet must be capable of processing the selected event. A dialog is opened that allows you to select from a list of transformations. Transformations are used to change event names or parameters so that the target can process them. You should be familiar with the transformation and target before defining a transformation for the wire. You can select from the list of transformations to read a description.
3. To create a new custom wire from a source portlet to a target on another page, drag the event to the target listed in the **Summary of wires** panel.
4. Select the transformation for the new wire, or select **None** if no transformation is needed, and click **OK**. If you selected "Simple String Transformation", select a target event from the list and select the source parameter names for each target parameter in the list. When the original event is sent, it is transformed into this target event before it is received by the target portlet.

The new wire is created and added to the wire summary for the page.

When you are finished making changes to the page, click **Save**.

Working with console preference profiles

Preference profiles are a collection of console behavior preferences for using the console that are created by the console administrator. These preferences include the visibility of the navigation tree, contents of the view selection list, and the default view. Assign preference profiles to roles to manage how the navigation area and view selections are displayed to the users in the role.

Attention: Each role is limited to one preference profile.

Field descriptions

This section describes the fields and controls in the main panel of Console Preference Profiles.

Select all icon
Selects all items displayed in the table for deletion. If you are displaying only a filtered set of items, only those items are selected. You can deselect specific items before actually deleting.

Deselect all icon
Deselects all items displayed in the table.

New Opens a panel for creating a new preference profile.

Delete Immediately deletes all selected items in the list. Only Custom resource types can be deleted.

Filter Type in this field to quickly find an item in the table. This field is useful when there are a large number of items to look through.

Select Selects or deselects a single item in the table.

Profile Name
Indicates the name of the profile. You can sort the list of names by clicking the column heading.

Role Count
Indicates the number of roles assigned to a preference profile. Each role is limited to one preference profile. However, multiple roles can be assigned to any single preference profile.

Creating preference profiles

Preference profiles are a collection of console behavior preferences for using the console that are created by the console administrator. Follow these steps to create a preference profile and assign it to a role.

1. Click **Settings** > **Console Preference Profiles** in the console navigation. The Console Preference Profiles page is displayed with the list of preference profiles that have already been created in the console.
2. Click **New**. The properties panel for the new preference profile is displayed.
3. Enter a descriptive name for the preference profile. Consider how the name reflects the roles that have been assigned to it or the console settings that are defined.
4. Indicate whether the navigation tree should be hidden. This might be preferable when the user has few pages to access and display space in the console is better reserved for page content.
5. Optional: Use the Console Bidirection Options to set the direction to display console content and text. The default option lets the browser dictate the text and content direction, for example, for Arabic and Hebrew, the text is displayed right-to-left, whereas for other languages it is displayed left-to-right. Alternatively, you can decide to set the text and content direction to either left-to-right or right-to-left. In the **Text direction** list, you can also select **Contextual Input** so that for portlets that include text entry fields, the direction of text is dependent on the language used to enter data.
6. Select which view options should be available for users in the role.
7. Expand the section **Roles Using this Preference Profile**.
8. Click **Add** and select one or more roles to use this preference profile. When assigning roles, you might notice some roles missing from the list. This means they are assigned to another preference profile. The role must be removed from the other profile before it can be assigned to this one.
9. Select the default console view for this preference profile. The default view is the one that is selected when users in this role log in to the console. This field is enabled when at least one role has been added for this preference profile.
10. Click **Save** to save your changes and return to Console Preference Profiles.

The new preference profile is created and listed on the main panel for Console Preference Profiles.

Editing console preference profiles

Preference profiles are a collection of console behavior preferences for using the console that are created by the console administrator. Follow these steps to change the properties or roles assigned to a preference profile.

1. in the navigation pane, click **Settings** > **Console Preference Profiles**. The Console Preference Profiles page is displayed with the list of preference profiles that have already been created in the console.
2. Click the name of the preference profile that you want to edit. The properties panel for the preference profile is displayed.
3. Optional: Enter a descriptive name for the preference profile. Consider how the name reflects the roles that have been assigned to it or the console settings that are defined.
4. Optional: Indicate whether the navigation tree should be hidden. This might be preferable when the user has few pages to access and display space in the console is better reserved for page content.
5. Optional: Use the Console Bidirection Options to set the direction to display console content and text. The default option lets the browser dictate the text and content direction, for example, for Arabic and Hebrew, the text is displayed right-to-left, whereas for other languages it is displayed left-to-right. Alternatively, you can decide to set the text and content direction to either left-to-right or right-to-left. In the **Text direction** list, you can also select **Contextual Input** so that for portlets that include text entry fields, the direction of text is dependent on the language used to enter data.
6. Optional: Select which view options should be available for users in the role.
7. Expand the section **Roles Using this Preference Profile**.

Option	Description
To add roles	Click **Add** and select one or more roles to add to the list. Click **OK** when you have made all of your selections. **Note:** If a role is not listed, it likely means that it has been assigned to another preference profile.
To remove roles	Select one of more roles in the list and click **Remove**. Be certain of your selections. When you delete, there is no warning prompt and the action cannot be undone.
To assign a default view	Select from the **Default console view** section to the side of the role list.

8. Click **Save** to save your changes.

The preference profile is updated and you are returned to the main panel for Console Preference Profiles.

Deleting console preference profiles

Preference profiles are a collection of console behavior preferences for using the console that are created by the console administrator. Follow these steps to delete a preference profile.

1. Click **Settings** > **Console Preference Profiles** in the navigation pane. The Console Preference Profiles page is displayed with the list of preference profiles that have already been created in the console.
2. Locate the preference profile that you want to delete in the table provided. You can use the filter in the table to type in the preference profile name and quickly display it.
3. In the **Select** column select one or more preference profiles.
4. Click **Delete**. A message is displayed at the top prompting you to confirm the deletion.
5. Click **OK**.

The preference profile is removed.

Resource types

You can use the console to create pages, roles, and views. All of these resources that you create using the console are assigned a resource type of `Custom`. With other resource types, a more limited set of actions are available.

The type of resource is determine by how it was created.

Core
This resource type is central to the operation of the console. Core resources cannot be created or deleted in the console, and you cannot edit its properties. However, you can make other changes that do not alter the nature of the resource, for example, including a core page in a custom view.

System
This resource type is created by products and applications that deploy the resource to the console. For example, when an application is installed to the console environment, it can define certain pages, roles, and views needed to administer the application through the console. All of these have a resource type of `System`. Like core resources, system resources cannot be created or deleted. However, for views, pages, and folders, you can create copies of system resources, which are explained under `System Customized`. And like core resources, you can perform actions on a system resource, like changing access to the resource, without modifying its properties.

System Customized
This is a copy of a system resource with properties, such as the name of the resource, that have been changed in the console. The original system resource is always maintained, but the system customized version of the resource is used until the original is restored. When the system resource is restored, the system customized copy is deleted.

You can create system customized pages, folders, and views, but not roles, wires, or external URLs.

Custom
These are resources that you create using the console. Custom resources can be created, edited, and deleted by any user whose role has access to the **Page Management**, **View Management**, **Portlet Management**, and **Role Management** portlets under the **Settings** folder in the navigation.

Manage Global Refresh

Console administrators use Manage Global Refresh to configure portlet refresh settings for all users of the console. Portlet refresh is used to refresh the content of a single console module without reloading the entire console page. As a result, your experience with the console interface is quicker and more interactive. Use these settings to fine tune how each portlet refreshes its content individually on the page.

Using Manage Global Refresh

Use this module for the following tasks:

- Giving permission to console users to edit their own portlet refresh options.
- Configuring default refresh settings for console modules. Administrators can set values for refresh mode, refresh interval, and show timer settings. These settings become the default values for Configure Portlet Refresh.
- Setting the minimum refresh interval for each console module. Use this setting to prevent the performance impacts of too many calls to the server to refresh content.

Portlet refresh settings

Restore Default Configuration
Changes all of the displayed field values to the values that were last saved. At least one portlet must be selected to enable this button. To save the changes displayed by this button, select the portlets that you want to restore to the default settings and click **Apply** or **OK**.

Select all Select all icon
Selects all of the portlets displayed. A maximum of 10 refreshable portlets can be displayed and selected at a time.

Deselect all Deselect all icon
Deselects all of the portlets displayed.

Select Use the checkbox to select individual portlets that you want to restore to the default settings.

Portlet
Indicates the name of the portlet or console module which can be refreshed.

Refresh Mode
Select one of the following options:

- **No Refresh**

  Indicates that the portlet content will not be refreshed automatically. The refresh timer is not displayed in the portlet title bar, but the portlet can still be refreshed manually.
- **Timed Refresh**

  Indicates that the portlet content is refreshed automatically based on the value of the refresh interval.
- **Smart Refresh**

  Indicates that after the refresh interval has timed out, the client should query the portlet on the server to determine if it should refresh the content. If the portlet has updates to provide, then the content is updated on the client. Otherwise, no change is made and the timer is started again.

- `Unregister`

  Disables portlet refresh capabilities for this portlet. The portlet still displays in Manage Global Refresh. Portlet refresh can be subsequently restored by setting this value to one of the other settings.

Refresh Interval
Indicate a value in seconds after which the portlet's content can be refreshed from the server without reloaded the entire console page. This value must be greater than or equal to the minimum refresh interval.

Minimum Refresh Interval
Indicates the minimum value for the refresh interval. This value is determined by the administrator.

User Configurable
Indicates whether users can change refresh setting in Configure Portlet Refresh.

Show Timer
Indicates whether to display a timer in the portlet title bar showing the number of seconds remaining until the next refresh can take place.

Network Manager portlets

Use this reference information to help you configure customized Network Manager pages.

The following topics provide more information on Network Manager portlets.

List of Network Manager portlets

You can use Network Manager portlets for creating pages.

The following Network Manager portlets are available to add to a page. You might also see portlets from other products, as well as the Tivoli® Integrated Portal administrative portlets.

- AEL (the Active Event List)
- Configure Historical Polling Database Access
- Configure NCIM Database Access
- Configure Poll Definitions
- Configure Poll Policies
- Management Database Access
- Network Discovery Configuration
- Network Discovery Status
- Network Hop View
- Network Views
- Path Views
- Path View Administration
- SNMP MIB Browser
- SNMP MIB Graph
- Structure Browser
- Work with reports (configures Tivoli Common Reporting)

Inter-portlet actions

Use this information to understand how Network Manager portlets communicate with each other when placed on the same page.

The following table describes the inter-portlet communication when the user clicks on a device, component, or event in the transmitting portlet.

Table 2. Inter-portlet actions

Transmitting portlet	**Receiving portlet**			
	Network Hop View	**Network Views**	**AEL**	**Structure Browser**
Network Hop View User clicks on a device	Not applicable	No interaction	No interaction	In the default Hop View, or in a custom page, displays structure of the selected device.
Network Views User clicks on a device	No interaction	Not applicable	In a custom page, displays alerts relating to the selected device.	In a custom page, displays structure of the selected device.
AEL User clicks on an event	In the default Fault finding view only, displays the Network Hop View using the corresponding device as the pivot device.	No interaction	Not applicable	No interaction

Editable portlet parameters

Use this information to understand which parameters are associated with each Network Manager portlet and how each of these parameters affects the appearance of the portlet.

To modify the portlet parameters, click **Edit** ✏.

Important: The Network Views, Hop View, and Structure Browser portlets refresh themselves. There is no need to set a global refresh on these portlets.

The editable parameters for the Network Manager portlets are as follows.

"Database Configuration" on page 30
"Discovery Configuration" on page 30
"Discovery Status" on page 30
"MIB Browser" on page 30
"Monitor Configuration Poll Policy" on page 30
"Monitor Configuration Template" on page 30
"Management Database Access" on page 30
"Structure Browser" on page 30

"Topology HopView" on page 31
"NetworkViews" on page 31
"Path Views" on page 32

Database Configuration

There are no editable parameters for this portlet.

Discovery Configuration

There are no editable parameters for this portlet.

Discovery Status

There are no editable parameters for this portlet.

MIB Browser

MIB Browser

Domain
Name of the domain that the portlet presents as default

Object ID
SNMP Object ID of the node for which MIB information is requested

Host Name of the host that has where the Helper Server is running

Show Results Only?
Indicates whether only the results of the MIB query are displayed. The default value is False.

Monitor Configuration Poll Policy

There are no editable parameters for this portlet.

Monitor Configuration Template

There are no editable parameters for this portlet.

Management Database Access

Management Database Access

Domain
Name of the domain that the portlet presents as default

Query SQL query

Service
Name of management database on which the query is run

Show Results Only?
Indicates whether only the results of the query are displayed. The default value is False.

Structure Browser

Structure Browser

Entity ID
Entity ID of the device whose structure is being requested.

View Mode
Specifies which mode the portlet loads: tree or table.

Note: Table mode is only available when the Structure Browser is displayed as a portlet.

Topology HopView

Topology HopView

Domain
Name of the domain that the portlet presents as default

Seed device
Pivot device around which the Network Hop View must be displayed

Hops Number of hops to display from the pivot device

Connectivity
Type of connectivity to display in the network map; options are IP Subnets, Layer 3, or Layer 2

Default value: IP Subnets

Layout
Layout style of the network map; options are Symmetric, Hierarchical, Orthogonal, and Circular

Default value: Symmetric

Show End Nodes?
Indicates whether to display end nodes in the map. The default value is False.

NetworkViews

Topology Network Views

Show Network Views Tree?
Indicates whether to display the network view navigation tree.

Map ID
ID of the network view to be displayed

Width Indicates the width of the column.

Hidden Columns
Indicates whether a column should be hidden. Master columns can not be hidden.

Locked Columns
Prohibits scrolling. Master columns can not be locked.

Sort Column
Specifies how the master column is to be sorted

Sort Order
Indicates whether columns should be sorted in ascending or descending order. Parent rows are sorted first, then child rows.

Path Views

Show Path Views Tree?
Indicates whether to display the path views navigation tree.

Map ID
ID of the path view to be displayed.

Width Indicates the width of the column.

Hidden Columns
Indicates whether a column should be hidden. Master columns can not be hidden.

Locked Columns
Prohibits scrolling. Master columns can not be locked.

Sort Column
Specifies how the master column is to be sorted

Sort Order
Indicates whether columns should be sorted in ascending or descending order. Parent rows are sorted first, then child rows.

Chapter 2. Administering network views

Network Views shows logical groupings of devices that you may need to monitor within your network. Create new views or change existing views to help network operators visualize devices.

About network views

Use this information to understand what a network view is, the different types of network view, and the types of user access to network view collections.

Use a network view to create a custom grouping of any set of devices, sub-nets, VLANs or other device collections for monitoring.

Network views can also be created based on device events. For example, you can create a network view that displays all devices on which a Critical severity event has occurred.

Standard network views

Create a standard network view to group any set of devices, sub-nets, VLANs or other device collections for monitoring. Standard network views are also referred to as *network views*.

For example, if you need to monitor the status of two specific sub-nets, you can group them in a standard network view. Once created, this network view appears in the Navigation Panel, with a name and in a position in the navigation tree that you specify.

For example you can create a new `My Views` container node in the navigation tree, name your new network view `My Subnets` and place this new view in the `My Views` container.

As the network changes and the topology is updated following discoveries, the content of the network view changes accordingly. For example, if new devices are added to the subnet, then these devices are automatically added to the network view after they have been discovered.

Usage considerations

Standard network view are useful for operators who monitor a part of the large network and need to focus on the devices, subnets or other device collections within their part of the network.

Create a standard network view if:

- You want to create views of particular device collections only, rather than all device collections of a specific type.
- You want to create a view that contains more than one device collection, rather than one view for each device collection.

Related tasks:

"Creating standard network views" on page 38
Network Manager has two types of views: standard and dynamic. You can create these standard views.

Dynamic network views

Dynamic network views are based on the devices or collections that you specify and based on all the network topology data. Dynamic network views are also referred to as *dynamic views*

If you create a dynamic view of VLANs, multiple VLAN network views are created, one for each VLAN. The result is therefore a node in the Navigation Panel for each VLAN in the network.

As the network changes and the topology is updated following discoveries, the VLAN nodes in the Navigation Panel might appear or disappear. For example, if any VLANs are removed from the network, then after another discovery, the corresponding VLAN network views automatically disappear.

Usage considerations

The dynamic view option is useful for keeping track of all the devices and device collections in your network. This option is therefore of greater use to an administrator who needs to keep track of device changes across the entire network. This option is also useful for operators of smaller networks who monitor an entire network.

Do not create a dynamic view if:

- You want to create views of particular device collections only, rather than all device collections of a specific type.
- You want to create a view that contains more than one device collection, rather than one view for each device collection.

If you want to achieve either of the above results, create a standard network view.

Related tasks:

"Creating dynamic network views" on page 55
Network Manager has two types of views: standard and dynamic. You can create these dynamic views.

Access configuration for network view collections

Use groups and role assignments to administer read-write and read-only access to network view collections, and administer privileges to copy and move network views between network view collections.

Network view collections

A network view collection is a grouping of network views accessible to a single user, a restricted set of users, or all users. You configure user access to network view collections by assigning roles to users and assigning users to groups.

Types of network view collection

TopoViz categorizes network view collections as follows:

Group views
Network views that are assigned to the group or groups to a user belongs. For example, divide users into geographical groups. Access to network views can then be restricted based on membership of the groups.

User views
Network views created by a user. Only the user and certain administrators can see these views.

Global views
Network views that are accessible to all users regardless of the group or groups to which they belong.

Types of user access to network view collections

User access to network views falls into the following two categories:

Read-write access
Enables the user to create, edit, delete, and partition network views. A user with this type of access can also copy and move network views between group, user and global view collections. Administrator access also enables users to display network views. To give users read-write access, you must assign the user the `netcool_rw` role, in addition to the Network Views administrative roles.

Read-only access
Enables the user to only display network views.

Example

The following table shows an example of assignment of roles to enable read-write or read-only access for different users within the "London" and "New York" groups.

The user "bob" is a member of both the "London" and "New York" groups and has read-write access across both groups. In addition to the group views, user can access their own user views and the global views.

Table 3. Configuring user access to network view collections

Group	Users	Roles	Accessible view collections	Access Level
London	ben (London)	ncp_networkview netcool_ro	London Views Global Views	read-only
	betty (London)	ncp_networkview netcool_rw ncp_networkview_admin_user	betty Views	read-write
			London Views Global Views	read-only
	barbara (London)	ncp_networkview netcool_rw ncp_networkview_admin_user ncp_networkview_admin_group	barbara Views London Views	read-write
			Global Views	read-only
New York	bob (London and New York)	ncp_networkview netcool_rw ncp_networkview_admin_all_users ncp_networkview_admin_group ncp_networkview_admin_global	ben Views, betty Views, barbara Views bob Views jerry Views, judy Views, jonas Views London Views New York Views Global Views	read-write
	jerry (New York)	ncp_networkview netcool_rw ncp_networkview_admin_user ncp_networkview_admin_group	jerry Views New York Views	read-write
			Global Views	read-only
	judy (New York)	ncp_networkview netcool_rw ncp_networkview_admin_user	judy View	read-write
			New York Views Global Views	read-only
	jonas (New York)	ncp_networkview netcool_ro	New York Views Global Views	read-only

Creating network view containers

Create a container to group together network views and store them in a single node in the Network View navigation panel.

To create a network view container:

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `Container`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Background Image
   Click **Browse** ... to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

   Line Status
   Specify how the lines that represent the links between devices should be rendered.

   You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.
3. Click **OK**.

The new container node is displayed in the Network View Tree.

Now, create new view within the container, or move existing views to the container.

Related tasks:

"Creating network views"
Create network views to show only those parts of the network that you need to monitor. There are two types of network views: standard views and dynamic views.

"Copying or moving views" on page 66
Move network views if you want to make private views available on a group-wide or global basis. Copy network views into your private collection if you want to change a group or global view without any impact on the original view.

Creating network views

Create network views to show only those parts of the network that you need to monitor. There are two types of network views: standard views and dynamic views.

Both standard views and dynamic views provide a custom grouping of any set of devices, sub-nets, VLANs or other device collections for monitoring.

Certain types of network view can be created based on device events. For example, you can create a network view that displays all devices on which a Critical severity event has occurred. To create network views based on device events, you must create a network view with an event filter.

Creating standard network views

Network Manager has two types of views: standard and dynamic. You can create these standard views.

Certain types of network view can be created based on device events. For example, you can create a filtered network view that displays all devices on which a Critical severity event has occurred.

Creating network views of device collections

To monitor collections of devices, such as subnets, VPNs, and MPLS VPNs, in a part of a large network, create a standard network view of a device collection. Standard views of device collections are changed automatically as the topology changes after a discovery.

If you want to store the view in a custom container, you must create the container before you begin this task.

You can create the following device collections:

- Border Gateway Protocol (BGP) Autonomous Systems (AS), clusters, and networks
- Generic collections
- Global Virtual Local Area Networks (VLANs)
- Hot Standby Routing Protocol (HSRP) groups
- Internet Group Membership Protocol (IGMP) groups
- Internet Protocol (IP) paths
- IPM Route Multicast Distribution Trees (MDT)
- ISIS levels
- ITNM Services

- Logical collections
- MPLS Traffic Engineered (TE) tunnels
- Open Shortest Path First (OSPF) areas and routing domains
- Protocol Independent Multicast (PIM) groups
- Stacks
- Subnets
- Virtual Private Networks (VPNs)
- VLAN Trunking Protocol (VTP) domains

To create a standard network view of one or more device collections in your network:

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `Collection`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Tree Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Background Image
   Click **Browse** ... to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

   Line Status
   Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Click the **Filter** tab. Complete the tab as follows:

   Domain
   Select your network domain.

   Type Select the required device collection. The **Available Collections** list is automatically populated based on your selection.

   Connectivity
   Select `Default`. The network view is displayed using the most appropriate connectivity for the type of collection you selected. You also have the option of specifying one of the other following connectivity options:

   - Layer 2
   - Layer 3
   - IP Subnets
   - OSPF
   - PIM
   - IPMRoute

   connectivity options.

   SubGraph
   If the visualization of logical groups has been enabled by the administrator, this menu is available. Select **Enable** to display entities in logical groups surrounded by a boundary (cloud), which can be expanded and collapsed. Select **Disable** to display entities in logical groups connected to a ring, which cannot be expanded or collapsed.

   Available Collections
   Select the device collections that you want to display in the network view and click **Select** > to move them to the **Selected Collections** list.

4. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Related tasks:

"Creating dynamic views of subnets" on page 58
To create network views for each of the subnets in your network, create a *dynamic view* of the subnets.

"Creating dynamic views of MPLS VPNs" on page 60
To create a view of the customer VPNs in your network, and have the option of showing customer-edge (CE) devices, create a dynamic view of MPLS VPNs.

Creating network views of MPLS VPNs

To have the option of showing or hiding CE (customer edge) devices, create a network view of MPLS VPNs.

You can also create an MPLS VPN view by creating a network view of device collections. However, you do not have the option to show or hide CE devices.

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `MPLS VPN`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Tree Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Background Image
   Click **Browse** ... to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

   Line Status
   Specify how the lines that represent the links between devices should be rendered.

   You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.
3. Click the **Filter** tab. Complete the tab as follows:

Domain
Select your network domain.

CE Devices
Select the `Hide` or `Show`.

Available MPLS VPNs
Select the MPLS VLANs that you want to display in the network view and click **Select** > to move them to the **Selected MPLS VPNs** list.

4. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Creating network views of VPLS VLANS

To monitor Virtual Private LAN Service Virtual Private Networks (VPLS VPNs), you can create network views of specific VPNs.

VPLS VPN network views are created automatically. You can also create them manually. To create a network view of a particular VPLS VPN, complete the following steps.

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

Name Type a name for the network view, dynamic view, or network view container.

Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

Type Select `VPLS VPN`.

Layout
Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

Map Icon
If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

Tree Icon
If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

Background Image

Click **Browse** ... to browse for an image to use as the background for the view.

Background Style

Specify whether the background image is to be centered or tiled.

Line Status

Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Click the **Filter** tab. Complete the tab as follows:

   Domain

   Select your network domain.

   CE Devices

   Select `Hide` or `Show`.

   Available VPLS VPNs

   Select the VPLS VLANs that you want to display in the network view and click **Select** > to move them to the **Selected VPLS VPNs** list.

4. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Creating network views to manually add devices

The custom view groups any set of devices, sub-nets, VLANs or other device collections in a domain for monitoring. Create a custom view to manually add devices. Custom views are empty when they are first created. Devices can be added from any network view in the domain for which the custom view was created.

Custom views do not use SQL filters because they are manually created. The view is updated as you add and remove devices.

Note: When you add an unassigned device to a custom view, the Unassigned view is automatically updated to remove the device.

An administrator can set the value of the **`topoviz.customview.enable`** property in the `etc/tnm/topoviz.properties` file to enable or disable custom views. This property is also used to enable or disable Unassigned views.

Complete these steps to create a custom view.

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .

2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

Type Select `Custom`.

Layout
Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

Map Icon
If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

Tree Icon
If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

Background Image
Click **Browse** ... to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Add devices, including unassigned devices, to the custom view.

Adding devices to a custom view:

After you create a custom view, the view is empty. You can manually add devices from any network view to the custom view.

Devices from any other network view can be added to a custom view. If you add an unassigned device to a custom view, the device is automatically removed from the unassigned view.

Complete these steps to add one or more devices to a custom view.

1. From an existing view, select one or more devices.

2. Right click the selected device or devices and select **Add To View** from the context menu.
3. From the **Add View** window, under **Add devices to custom view**, specify a value for these fields:**To** and **View**.
4. First, choose a view from the **To** drop-down menu. This designates the category of view, for example itnmadmin views, to add the device to.
5. Next, click the **View Tree** button. A tree is displayed that contains the custom views that are available for the **Type** you selected. The custom views in the tree are highlighted in bold and italics.
6. Select a custom view from the tree, and then click **OK**.

   Note: You must click **OK** below the tree, before clicking **OK** for **Add selected nodes to**. If you do not click **OK** below the tree, an error message is displayed.
7. Click **OK** to add the selected devices to the custom view.

Removing devices from a custom view:

Remove one or more devices from a custom view if you no longer want the device to be assigned to the custom view.

Network Manager automatically updates network views to add or remove devices. The custom view is the only view that is not automatically updated. If you want to remove a device from a custom view, you must manually remove the device. Complete these steps to remove one or more devices from a custom view.

Note: If an unassigned view exists for a domain, any devices removed from the custom view are automatically added to the unassigned view if they do not exist in any other network view.

1. Navigate to the custom view from which you want to remove one or more devices.
2. From the custom view, select the devices.
3. Right-click to access the context menu and then select **Remove from view**.
4. When the confirmation window displays, click **Yes** to remove the selected devices from the custom view.

Creating network views for unassigned devices

Create a network view for unassigned devices. The Unassigned view groups all devices in a domain that are not currently assigned to a network view. The view is updated dynamically as devices are added and removed from views in the domain.

The Unassigned view acts as a placeholder for network devices that do not belong to other views. From the Unassigned view, an operator can assign devices to a network view.

Unassigned views do not use SQL filters because they are automatically created by querying the network for unassigned devices. The view is updated dynamically as devices are added and removed from views in the domain.

An administrator can set the value of the **`topoviz.customview.enable`** property in the `etc/tnm/topoviz.properties` file to enable or disable unassigned views. This property is also used to enable or disable custom views.

Complete these steps to create an Unassigned view.

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `Unassigned`.

   Layout
   Select Grid or Tabular.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Tree Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Background Image
   Click **Browse** ... to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

   Line Status
   Specify how the lines that represent the links between devices should be rendered.

   You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.
3. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

The Unassigned view is created when devices that are not in another view are automatically added to the unassigned view.

You can select an unassigned device and right-click to add the device to a network view.

Creating filtered views

Use a filtered view to view parts of the network based on topology database filters; for example, a network view showing all Cisco devices on a given subnet.

If you want to store the view in a custom container, you must create the container before you begin this task.

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `Filtered`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Tree Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Background Image
   Click **Browse** ... to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

   Line Status
   Specify how the lines that represent the links between devices should be rendered.

   You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.
3. Set up the filter:
   a. Click the **Filter** tab.

   b. From the **Domain** list, select your network domain.
   c. In the **Table** column, select the attribute table that you want to use in the filter.
   d. In the **Filter** column, type an SQL WHERE clause.

   To set up the filter using the Filter Builder click **Edit** .

4. Optional: In the Filter Builder, under **Basic**, use the lists and fields to build the required query:
   a. Select a field, comparator, and value from the lists. Use percent sign (%) as a wildcard.
   b. Use a Boolean relationship to combine multiple filters:

      All Only network entities that match all the specified filters are generated in the view. For example, if you create two filters, a network entity must match both filters.

      Any Network entities that match either of the specified filters are generated in the view.
5. From the **End nodes** list, specify whether you want end nodes, such as printers and workstations, to be displayed in the view.
6. From the **Connectivity** list, select the required connectivity:

Option	Description
IP Subnets	Displays device membership by subnet. To simplify the view and make subnet membership clear, this type of connectivity does not show all connections.
Layer 2	Displays all datalink connections. No logical connections are displayed.
Layer 3	Displays all logical connections. Routers are displayed. Switches are not displayed, unless they have an active connection that involves a layer 3 interface. Connections between layer 3 devices are displayed. Connections between a layer 3 and a layer 2 interface are displayed between the layer 3 interface and the subnet to which the layer 2 interface belongs.
OSPF	Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.
PIM	Displays connections based on PIM adjacency information.
IPMRoute	Displays connections based on IP Multicast upstream and downstream routing information.
No connections	Does not present any of the discovered connections for the nodes shown in the view.

7. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Sample filters

The following examples show the different ways to build a typical filter. The filter retrieves all Cisco devices on subnet 172.20.10.

To build a filter by typing SQL WHERE statements:

1. On the **Filter** tab, from the **Table** list, select `ipEndPoint`. In the **Value** field, type `subnet like '172.20.10.%'`.
2. Click **Add new row** ➕ .
3. From the **Table** list, select `chassis`. In the **Value** field, type `className like 'Cisco'`.
4. Click **OK**.

To build a filter by using the Filter Builder:

1. On the **Filter** tab, from the **Table** list, select `ipEndPoint`. Click . The Filter Builder is displayed.
2. On the **Basic** tab, select `subnet` from the **Field** list.
3. From the **Comparator** list, select `=`.
4. In the **Value** field, type `172.10.10.6` and click **OK**.
5. On the **Filter** tab, from the **Table** list, select `chassis`. Click . The Filter Builder is displayed.
6. Click **Add new row** ➕ .
7. From the **Field** list, select `className`.
8. From the **Comparator** list, select `=`.
9. In the **Value** field, type `Cisco`.
10. Click **OK**.

Example topology filter: all Cisco devices on a subnet:

When creating a filtered network view, create a topology filter to filter the parts of the topology to show in the network view. For example, as part of the filtered network view you can create a filter to show all Cisco devices on a given subnet.

This task shows you how to create an example topology filter for a filtered network view.

Before you begin this task, you need to follow the instructions described in the task "Creating filtered views". When you reach the step in which you set up the filter for the network view, perform the following steps.

1. Click the **Filter** tab.
2. From the **Domain** list, select your network domain.
3. Set up the subnet part of the filter. In the **Table** column, select the ipEndPoint NCIM topology table.
4. Open the Filter Builder, by clicking **Open Filter Builder** .
5. In the Filter Builder, under **Basic**, use the lists and fields to build the required query:
   a. From the **Field** list select subnet.
   b. From the **Comparator** list select like.

   c. In the **Value** field type a subnet identifier. For example, to specify the subnet 172.20.100.0, type the text 172.20.100%. The percent sign (%) is a wildcard.
   d. Click **OK** to complete the definition of the subnet part of the filter. The **Filter** column value for ipEndPoint now reads as follows: subnet like '172.20.100%'.
6. Set up the part of the filter that filters by device type. Click **Add new row** to add a new row to the Filter table.
7. In the **Table** column, select the chassis NCIM topology table.
8. Open the Filter Builder, by clicking **Open Filter Builder** .
9. In the Filter Builder, under **Basic**, use the lists and fields to build the required query:
   a. From the **Field** list select className.
   b. From the **Comparator** list select like.
   c. In the **Value** list type Cisco%.
   d. Click **OK** to complete the definition of the device type part of the filter. The **Filter** column value for chassis now reads as follows: className like 'Cisco%'.
10. Ensure that the Boolean relationship used to combine the two filters that you just defined is **All**.

Now, complete the remaining steps in the task "Creating a filtered network view".

Example event filter: all devices with Critical events:

When creating a filtered network view, create an event filter to filter topology based on events. For example, as part of the filtered network view you can create a filter to show all devices with events of Critical severity.

This task shows you how to create an example event filter for a filtered network view.

Before you begin this task, you need to follow the instructions described in the task "Creating a filtered network view". When you reach the step in which you set up the filter for the network view, perform the following steps.

1. Click the **Filter** tab.
2. From the **Domain** list, select your network domain.
3. In the **Table** column, select the activeEvent table.
4. Open the Filter Builder, by clicking **Open Filter Builder** .
5. In the Filter Builder, under **Basic**, use the lists and fields to build the required query:
   a. From the **Field** list select Severity.
   b. From the **Comparator** list Select =.
   c. From the **Value** list select Critical.
   d. Click **OK** to complete the definition of the filter. The **Filter** column value for the activeEvent table now reads as follows: Severity = Critical.

   Note: The activeEvent table contains a subset of fields from the Tivoli Netcool/OMNIbus alerts.status table. For information on the fields in the alerts.status table, see the *IBM Tivoli Netcool/OMNIbus Administration Guide*.

Now, complete the remaining steps in the task "Creating a filtered network view".

Creating filtered views using variables

Use a variable in a filtered view to create complex views. For example, create a view of all devices with events older than one hour.

If you want to store the view in a custom container, you must create the container before you begin this task.

You can use a variable in the filter. The variable is replaced by the appropriate value retrieved from the server. The variable name must be in the form `{%variable}`.

Restriction:

The only variable supported is {%serverTime}. The {%serverTime} variable is replaced with the current time on the Network Manager server, expressed as a UNIX epoch time (seconds after midnight on 1 January 1970 UTC).

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `Filtered`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Tree Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Background Image
   Click **Browse** ... to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

Line Status

Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Set up the filter:
   a. Click the **Filter** tab.
   b. From the **Domain** list, select your network domain.
   c. In the **Table** column, select the database table that contains the variable you want to use. For the `{%serverTime}` variable, select the **activeEvent** table.
   d. In the **Filter** column, type an SQL WHERE clause that includes the variable you want to use. For example, to create a view that contains devices with events older than one hour, use the following clause:

      ```
      {%serverTime} – FirstOccurrence > 3600
      ```
4. From the **End nodes** list, specify whether you want end nodes, such as printers and workstations, to be displayed in the view.
5. From the **Connectivity** list, select the required connectivity:

Option	Description
IP Subnets	Displays device membership by subnet. To simplify the view and make subnet membership clear, this type of connectivity does not show all connections.
Layer 2	Displays all datalink connections. No logical connections are displayed.
Layer 3	Displays all logical connections. Routers are displayed. Switches are not displayed, unless they have an active connection that involves a layer 3 interface. Connections between layer 3 devices are displayed. Connections between a layer 3 and a layer 2 interface are displayed between the layer 3 interface and the subnet to which the layer 2 interface belongs.
OSPF	Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.
PIM	Displays connections based on PIM adjacency information.
IPMRoute	Displays connections based on IP Multicast upstream and downstream routing information.
No connections	Does not present any of the discovered connections for the nodes shown in the view.

6. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Creating IP filtered views

You can create network views for IP addresses (devices and subnets) based on IP filter criteria. For example, you can create a network view for all devices and subnets that either have a specific IP address or contain a specific fragment of an IP address. You can specify multiple IP filters.

If you want to store the view in a custom container, you must create the container before you begin this task.

To create an IP-filtered network view:

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `IP Filter`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Tree Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Background Image
   Click **Browse** ... to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

   Line Status
   Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Click the **Filter** tab. From the **Domain** list, select your network domain.
4. In the **Address Patterns** field, specify an IP address pattern that you want to match.

   Tip: You can specify as many IP address patterns as you want. The resulting network view shows the union of all IP address retrieved by the different address patterns.
5. From the **End nodes** list, specify whether you want end nodes, such as printers and workstations, to be displayed in the view.
6. From the **Connectivity** list, select the required connectivity:

Option	Description
`IP Subnets`	Displays device membership by subnet. To simplify the view and make subnet membership clear, this type of connectivity does not show all connections.
`Layer 2`	Displays all datalink connections. No logical connections are displayed.
Layer 3	Displays all logical connections. Routers are displayed. Switches are not displayed, unless they have an active connection that involves a layer 3 interface. Connections between layer 3 devices are displayed. Connections between a layer 3 and a layer 2 interface are displayed between the layer 3 interface and the subnet to which the layer 2 interface belongs.
OSPF	Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.
PIM	Displays connections based on PIM adjacency information.
IPMRoute	Displays connections based on IP Multicast upstream and downstream routing information.
No connections	Does not present any of the discovered connections for the nodes shown in the view.

7. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Sample IP address patterns

To match all IP addresses that begin with 192.168, type the address pattern `192.168`.
To match IP addresses that begin with 172.18, 172.19, and 172.20, type the address pattern `172.18-20`.

IP filter syntax:

Use this reference information to understand how to model the syntax of an IP filter.

When searching for specific IP addresses, you can use ranges for the last octet. You can also assume wildcards for the last octet.

See the following examples to understand the use of ranges and wildcards.

The following examples show different options for using ranges and wildcards to filter for IP addresses:

- `172.18-20` matches any IP address that has 172.18, 172.19, or 172.20 as the first two octets.
- `172.20.36-38` matches any IP address that has 172.20.36, 172.20.37, or 172.20.38 as the first three octets.
- `192.168` matches all IP addresses that have the value of 192.168 as the first two octets.

  Note: When used in the last octet, the asterisk (*) wildcard is optional. For example, entering 192.168 and 192.168.* produce the same results. However, the asterisk can be used to filter within octets, for example 192.0.2.1* only matches addresses that have 192.0.2.1* as their first characters.

Creating dynamic network views

Network Manager has two types of views: standard and dynamic. You can create these dynamic views.

Certain types of network view can be created based on device events. For example, you can create a dynamic distinct network view that categorizes devices by location, and within each location, categorizes the devices by the event severity on each device.

Creating dynamic views of device collections

To view and keep track of changes to device collections in your network, create dynamic views of device collections. Use dynamic network views to monitor changes to the network. If the topology has changed after a discovery, the nodes in the Navigation Panel are updated automatically.

Use a dynamic network view to monitor which devices have been added to the network, and which devices have been removed. If the topology has changed after a discovery, the nodes in the Navigation Panel are updated automatically.

If you want to store the view in a custom container, you must create the container before you begin this task.

You can create the following device collections:

- Border Gateway Protocol (BGP) Autonomous Systems (AS), clusters, and networks
- Generic collections
- Global Virtual Local Area Networks (VLANs)
- Hot Standby Routing Protocol (HSRP) groups
- Internet Group Membership Protocol (IGMP) groups

- Internet Protocol (IP) paths
- IPM Route Multicast Distribution Trees (MDT)
- ISIS levels
- ITNM Services
- Logical collections
- MPLS Traffic Engineered (TE) tunnels
- Open Shortest Path First (OSPF) areas and routing domains
- Protocol Independent Multicast (PIM) groups
- Stacks
- Subnets
- Virtual Private Networks (VPNs)
- VLAN Trunking Protocol (VTP) domains

The following table describes specific requirements for which a dynamic view of device collections is not suitable. In each case, follow the alternative course of action:

Table 4. Strategies for creating dynamic views of device collections

Requirement	**Action**
You want a dynamic view of subnets and want to avoid creating large numbers of view of class C subnets	Create a dynamic view of subnets. Typically, networks contain large numbers of class C subnets, which result in large numbers of views. By creating a dynamic view of subnets, you can restrict the number of views to class A and class B subnets.
You want a dynamic view of MPLS VPNs but want to restrict the views to customer VPNs only, and want the option of showing customer-edge (CE) devices in those views	Create a dynamic view of MPLS VPNs. For MPLS VPNs, a dynamic view of device collections results in views for both the customer VPNs and the MPLS core network. Additionally, the customer VPNs do not show customer edge (CE) devices.

To create a dynamic view of one or more device collections in your network:

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `Dynamic Views – Collection`.

Layout
Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

Map Icon
If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

Tree Icon
If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

Background Image
Click **Browse** ... to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Click the **Filter** tab. Complete the tab as follows

Domain
Select your network domain.

Type
Select the required device collection. The **Preview** list is automatically populated based on your selection.

SubGraph
If the visualization of logical groups has been enabled by the administrator, this menu is available. Select **Enable** to display entities in logical groups surrounded by a boundary (cloud), which can be expanded and collapsed. Select **Disable** to display entities in logical groups connected to a ring, which cannot be expanded or collapsed.

4. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Related tasks:

"Creating dynamic views of subnets" on page 58
To create network views for each of the subnets in your network, create a *dynamic view* of the subnets.

"Creating dynamic views of MPLS VPNs" on page 60
To create a view of the customer VPNs in your network, and have the option of showing customer-edge (CE) devices, create a dynamic view of MPLS VPNs.

Creating dynamic views of subnets

To create network views for each of the subnets in your network, create a *dynamic view* of the subnets.

If you want to store the view in a custom container, you must create the container before you begin this task.

Typically, networks contain large numbers of class C subnets, which result in large numbers of views. By creating a dynamic view of subnets, you can restrict the number of views to class A and class B subnets.

Tip: If you want to create network views that contain more than one subnet, then do not create a dynamic view. Instead, create a *standard network view* for device collections.

To create a dynamic view of the subnets in your network:

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `Dynamic Views – Subnet`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Tree Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Background Image
   Click **Browse** ... to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

Line Status

Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Click the **Filter** tab. Select your network domain from the **Domain** list.
4. Select the required option from the **Subnet** list:

Option	Description
A & B	Creates network views for each of the class A and class B subnets in your network
A, B & C	Creates network views for each of the class A , class B, and class C subnets in your network. Typically, this option automatically creates a large number of subnet network views because most networks contain many class C subnets.

The **Preview** list is automatically populated based on your selection.

5. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Related tasks:

"Creating dynamic views of subnets" on page 58
To create network views for each of the subnets in your network, create a *dynamic view* of the subnets.

"Creating dynamic views of MPLS VPNs" on page 60
To create a view of the customer VPNs in your network, and have the option of showing customer-edge (CE) devices, create a dynamic view of MPLS VPNs.

"Creating dynamic views of device collections" on page 55
To view and keep track of changes to device collections in your network, create dynamic views of device collections. Use dynamic network views to monitor changes to the network. If the topology has changed after a discovery, the nodes in the Navigation Panel are updated automatically.

"Creating network views of device collections" on page 38
To monitor collections of devices, such as subnets, VPNs, and MPLS VPNs, in a part of a large network, create a standard network view of a device collection. Standard views of device collections are changed automatically as the topology changes after a discovery.

Creating dynamic views of MPLS VPNs

To create a view of the customer VPNs in your network, and have the option of showing customer-edge (CE) devices, create a dynamic view of MPLS VPNs.

If you want to store the view in a custom container, you must create the container before you begin this task.

Restriction: The dynamic view of MPLS VPNs does not create a network view for the MPLS core network. To create a view for the core network, create a dynamic view of device collections.

Tip: If you want to create a view that contains more than one customer VPN, do not create a dynamic view. Instead, create a network view of MPLS VLANs.

To create a dynamic view of the customer VPNs in your network:

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `Dynamic Views – MPLS – VPN`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Tree Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Background Image
   Click **Browse** ... to browse for an image to use as the background for the view.

   Background Style
   Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Click the **Filter** tab. Complete the tab as follows:

   Domain
   Select your network domain.

   CE Devices
   Select `Hide` or `Show`. The **Preview** list is automatically populated based on your selection.
4. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Related tasks:

"Creating dynamic views of device collections" on page 55
To view and keep track of changes to device collections in your network, create dynamic views of device collections. Use dynamic network views to monitor changes to the network. If the topology has changed after a discovery, the nodes in the Navigation Panel are updated automatically.

"Creating network views of device collections" on page 38
To monitor collections of devices, such as subnets, VPNs, and MPLS VPNs, in a part of a large network, create a standard network view of a device collection. Standard views of device collections are changed automatically as the topology changes after a discovery.

"Creating dynamic views of subnets" on page 58
To create network views for each of the subnets in your network, create a *dynamic view* of the subnets.

Creating distinct dynamic views

To create a network view that has custom categories and subcategories, create a *distinct dynamic view*.

For example, you can use the distinct dynamic view to categorize devices by location and within each location organize by the network administrator who is responsible for maintaining the devices. For example, you can use this option to categorize devices by location, and within each location, list the different device classes, such as Cisco 2600 devices or 3ComSuperStack devices.

To create an IP-filtered network view:

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

Type Select `Dynamic Views – Distinct`.

Layout
Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

Map Icon
If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

Tree Icon
If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

Background Image
Click **Browse** ... to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Click the **Filter** tab. From the **Domain** list, select your network domain.
4. In the **Fields** list, select the topology database tables and fields that correspond to the categories and subcategories that you want to define. Make sure you define the categories and subcategories in the correct order.
   a. Click **Add...**.
   b. From the **Table** list, select the required database table. The **Field** list is automatically populated based on your selection.
   c. Select the required field from the **Field** list.
   d. Repeat steps 4a to 4c.

   See “Sample topology database fields for categories” on page 63 for more information on how to specify the fields. As you select fields, the **Preview** list is updated to show the relationships between the categories that you selected.
5. From the **End nodes** list, specify whether you want end nodes, such as printers and workstations, to be displayed in the view.
6. From the **Connectivity** list, select the required connectivity:

Option	Description
IP Subnets	Displays device membership by subnet. To simplify the view and make subnet membership clear, this type of connectivity does not show all connections.
Layer 2	Displays all datalink connections. No logical connections are displayed.
Layer 3	Displays all logical connections. Routers are displayed. Switches are not displayed, unless they have an active connection that involves a layer 3 interface. Connections between layer 3 devices are displayed. Connections between a layer 3 and a layer 2 interface are displayed between the layer 3 interface and the subnet to which the layer 2 interface belongs.
OSPF	Displays connections based on discovered OSPF information that includes router roles, area membership, and connectivity.
PIM	Displays connections based on PIM adjacency information.
IPMRoute	Displays connections based on IP Multicast upstream and downstream routing information.
No connections	Does not present any of the discovered connections for the nodes shown in the view.

7. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Sample topology database fields for categories

The following example helps you complete the fields in step 4 on page 62.

To categorize devices by location, and within each location categorize by the responsible network administrator, define the following categories, in the following order:

1. Location of the device: This data is held in the sysLocation field of the chassis database table.
2. Contact person associated with the device: This data is held in the sysContact field of the chassis database table.

This order ensures that location is the main category and contact person is the subcategory.

Creating template-based dynamic views

Use a template-based dynamic view to generate a pre-configured set of dynamic views that are predefined by the network administrator.

If you want to store the view in a custom container, you must create the container before you begin this task.

The required templates must have been defined and stored in the `ITNMHOME/profiles/TIPProfile/etc/tnm/dynamictemplates` directory. If a template is not stored in this directory, it cannot be selected for generating dynamic views.

A template is a set of preconfigured views that are defined in an XML file. The network administrator can preconfigure different sets of views for different network operators by defining these preconfigured views in separate templates. The network operators select the template that is relevant to them and generate the views.

To create a template-based dynamic view:

1. Click **Availability** > **Network Availability** > **Network Views**. Click **New View** .
2. Complete the **General** tab as follows:

   Name Type a name for the network view, dynamic view, or network view container.

   Important: It is best practice to use network view names containing Latin characters only. Network views names containing non-Latin characters (for example Cyrillic characters) are not supported as they cannot be imported and exported when migrating to a new version of Network Manager.

   Parent Select the node under which the view appears in the hierarchy in the Navigation Tree. To display the view on the top level, select `NONE`.

   Type Select `Dynamic Views - Template`.

   Layout
   Select `Orthogonal`, `Circular`, `Symmetric`, `Hierarchical`, or `Tabular` layout.

   Map Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Tree Icon
   If you want a different icon than the default cloud icon to represent the view, click **Browse** ... to browse for an icon.

   Background Image
   Click **Browse** ... to browse for an image to use as the background for the view.

Background Style
Specify whether the background image is to be centered or tiled.

Line Status
Specify how the lines that represent the links between devices should be rendered.

You can choose not to display any status, or to display the system default. Alternatively, lines can be colored based on the associated AEL event with the highest severity, and can appear with an additional severity icon.

3. Click the **Filter** tab. From the **Domain** list, select your network domain.
4. From **Template**, select the template that want to use to generate the dynamic view. The **Preview** list is automatically populated with the list of network views based on your selection.
5. Click **OK**. The new view is added to the navigation tree in the Navigation Panel. If you added the view to a container, expand the container node to see the new view in the tree.

Changing network views

You can change any of the properties of an existing view.

To edit a view:

1. In the navigation panel, navigate to the view you want to edit and click **Edit**. A dialog box is displayed.
2. Edit the properties of the view. When you have finished, click **OK** to apply your changes.
3. Click **Save** .

Deleting network views

Delete existing network views if they are no longer required.

To delete an existing view:

1. Click **Availability** > **Network Availability** > **Network Views**.
2. Navigate to the required network view and select the view. Then click **Delete View** . The Delete View dialog is displayed.
3. Select one of the following options:

Option	Description
Delete view and all its sub-views	Deletes both the selected view and any subviews that it might have.
Delete view and move sub-views to new parent	Deletes only the selected view and moves any sub-views to the node that you select from the list. To move the subviews to the top level of the hierarchy, select `NONE`.

4. Click **Delete** > **OK**.

Copying or moving views

Move network views if you want to make private views available on a group-wide or global basis. Copy network views into your private collection if you want to change a group or global view without any impact on the original view.

To copy or move views to a container, you must be a member of that contain, or you must have administration rights for the container.

To move a view, you must have the appropriate administration rights. If you do not have the administration rights to move a view, you can only copy a view. For many of these operations you must have read-write access.

For the available options when copying or moving views, see "Possible copy and move actions."

To copy or move a view:

1. Click **Availability** > **Network Availability** > **Network Views**.
2. Navigate to the required view, select the view, and click **Copy or Move View** .
3. Under **Action**, select an option:
   - **Copy**: Creates a copy of the view in the selected target.
   - **Move**: Moves the view to the selected target.
4. Complete the other fields as follows:

   To Select the view collection to which you want to copy or move the view.

   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`.
5. Click **OK**.

Possible copy and move actions

The following table describes the copy and move operations that you can perform, and shows source and target view collections for these copy and move operations.

Table 5. Copying and Moving Network Views between Network View Collections

Source	Target	Result
Own user view collection	Within same user view collection	Places the network view in a required position within the user view collection
Own user view collection	Group view collection	Makes a private network view available on a group-wide basis
Own user view collection	Global view collection	Makes a private network view available on a global basis
Group view collection	Own user view collection	Enables you to copy a group view into your own user view collection and modify the view there
Group view collection	Within same group view collection	Places the network view in a required position within the group view collection
Group view collection	Another group view collection	Enables sharing of network views between groups

Table 5. Copying and Moving Network Views between Network View Collections (continued)

Source	Target	Result
Group view collection	Global view collection	Makes a network view formerly available only to users within a single group available on a global basis
Global view collection	Own user view collection	Enables you to copy a global view into your own user view collection and modify the view there
Global view collection	Group view collection	Enables you to copy a global view into a group view collection where group members can display the view and modify it if they have read-write access
Global view collection	Another point within the Global view collection	Places the network view in a required position within the global view collection

Related reference:

"Access configuration for network view collections" on page 34
Use groups and role assignments to administer read-write and read-only access to network view collections, and administer privileges to copy and move network views between network view collections.

Roles required to copy and move network views

To enable users to copy and move network views between network view collections you must assign the users to certain roles and groups.

The ability to copy and move network views between view collections varies depending on which roles are assigned to a user and which group or groups of which the user is a member.

The following table describes that you must assign to users so that they can copy and move views.

Table 6. Roles for copying and moving network views between network view collections

Operation	From	To	Roles required	Group membership required
Copy or move	Own user view collection	Within same user view collection	ncp_networkview ncp_networkview_admin_user netcool_rw	None
Copy	Own user view collection	Group view collection	ncp_networkview ncp_networkview_admin_group netcool_rw	Must be member of the target group
Move view collection	Own user view collection	Group view collection	ncp_networkview ncp_networkview_admin_user ncp_networkview_admin_group netcool_rw	Must be member of the target group

Table 6. Roles for copying and moving network views between network view collections (continued)

Operation	From	To	Roles required	Group membership required
Copy	Own user view collection	Global view collection	ncp_networkview ncp_networkview_admin_global netcool_rw	None
Move	Own user view collection	Global view collection	ncp_networkview ncp_networkview_admin_user ncp_networkview_admin_global netcool_rw	None
Copy	Group view collection	Own user view collection	ncp_networkview ncp_networkview_admin_user netcool_rw	Must be member of the source group
Move	Group view collection	Group view collection	ncp_networkview ncp_networkview_admin_user ncp_networkview_admin_group netcool_rw	Must be member of the source group
Copy or move	Group view collection	Within same group view collection or to another group view collection	ncp_networkview ncp_networkview_admin_group netcool_rw	Must be member of the source and target groups
Copy	Group view collection	Global view collection	ncp_networkview ncp_networkview_admin_global netcool_rw	Must be member of the source group
Move	Group view collection	Global view collection	ncp_networkview ncp_networkview_admin_global ncp_networkview_admin_group netcool_rw	Must be member of the source group
Copy	Global view collection	Own user view collection	ncp_networkview ncp_networkview_admin_user netcool_rw	None
Move	Global view collection	Own user view collection	ncp_networkview ncp_networkview_admin_user ncp_networkview_admin_global netcool_rw	None

Table 6. Roles for copying and moving network views between network view collections (continued)

Operation	From	To	Roles required	Group membership required
Copy or move	Global view collection	Another point within the Global view collection	ncp_networkview ncp_networkview_admin_global netcool_rw	None
Copy	Global view collection	Group view collection	ncp_networkview ncp_networkview_admin_group netcool_rw	Must be member of the target group
Move	Global view collection	Group view collection	ncp_networkview ncp_networkview_admin_global ncp_networkview_admin_group netcool_rw	Must be member of the target group

Configuring connectivity types

You can create or edit connectivity types for use in the Hop View and the Network Views.

You can display different types of connectivity in the Hop View and the Network Views. By default, you can display Layer 2, Layer 3, or IP subnet connectivity. You can also define your own connectivity types.

To configure a connectivity type, complete the following steps:

1. On the server where the Network Manager Web components are installed, back up and edit the appropriate file:
   - For US English, edit the file `ITNMHOMEprofiles/TIPProfile/etc/tnm/locale/ncp_layertypes.properties`.
   - For other languages, edit the file `ITNMHOMEprofiles/TIPProfile/etc/tnm/locale/ncp_layertypes_`*`lang_country`*`.properties`, where *lang* is the two-latter language code, and *country* is the two-letter country code.

   For example, to define a new layer type in Brazilian Portuguese, edit the file `ncp_layertypes_pt_BR.properties`.
2. Add a line to create a new connectivity type, or edit or delete the line for an existing connectivity type. To create a new layer of type "Pseudo Wire":

   ```
   connectivity.77:Pseudo Wire
   ```

   In this example, the number 77 is the value of the `entityType` field from the `ncim.entityType` topology database that corresponds to Pseudo Wire Topology. You can choose a different entityType, as long as it has a metaClass of Topology. Pseudo Wire is the name that will be displayed in the **Connectivity** menu.

   Important: Do not delete or modify the default connectivity types Layer 2. Layer 3, or IP Subnet.

3. Save and close the file.

Enabling custom or unassigned views

Enable custom and unassigned views if you want to create a custom or unassigned view type. You must create a custom view if you want to manually add a collection of devices to a view. Create an unassigned view to automatically collect all unassigned devices for a domain in the unassigned view.

Complete these steps to enable custom and unassigned views.

1. Back up the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` file.
2. Add or edit the following property: **`topoviz.customview.enable`**. Set the value to `true` to enable both custom and unassigned views.

   Note: Set the value to `false` to disable custom and unassigned views.
3. Save and close the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` file.
4. Ensure that the `addToView.xml` and `removeFromView.xml` files are present in the `ITNMHOME/profiles/TIPProfile/etc/tnm/tools` directory. If they are not present, copy them from the `ITNMHOME/profiles/TIPProfile/etc/tnm/tools/default/` directory.
5. Ensure that the following lines are present in the `ITNMHOME/profiles/TIPProfile/etc/tnm/menus/ncp_topoviz_device_menu.xml` file:

```
<tool id="addToView"/>
<tool id="removeFromView"/>
```

Enabling visualization of logical groups

If you enable this feature, logical groups such as subnets can be expanded and collapsed in the Network Views.

If the **SubGraph** property of a Network View is disabled, membership of logical groups is shown by dashed lines connecting entities to a blank oval, which represents the logical group. If the **SubGraph** property of a Network View is enabled, entities in logical groups are shown surrounded by a rectangular border, which can be collapsed into a cloud.

The **SubGraph** property can only be set on Network Views of type Collection.

The **SubGraph** property of a Network View can be enabled or disabled when creating or editing a network view. The option to enable or disable the **SubGraph** property only appears in the GUI if the visualization of logical groups has first been enabled by an administrator.

To enable the visualization of logical groups, complete the following tasks.

1. Run the following script: `ITNMHOME/scripts/sql/`*`database type`*`/updatePrecisionGUIDb.sql`.
2. Back up the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` file.
3. Add or edit the following line: `topoviz.collection.subgraph.enable=true`.
4. Save and close the file.

Deploying pre-configured network views

To configure network views for use by network operators, create a template that specifies pre-configured network views. The template can be deployed either by the operators, or globally for specific sets of operators.

The network views in the template can be created in two ways:

- Network operators generate the network views from the Network Views GUI by create a new template-based dynamic network view and specifying the template.
- You generate the network views specified in the template and assign the generated views to a specific user or group.

Making a pre-configured template available to operators

Provide a template of pre-configured network views to network operators so that they can use the template to generate dynamic network views from the Network Views GUI themselves.

To provide the template:

1. Define the template in an XML file. Give the XML file the following name: `*template_name*.xml` , where *template_name* is the name of the template on which network operators base their dynamic network views.
2. Save the template to the `ITNMHOME/profiles/TIPProfile/etc/tnm/dynamictemplates` directory.

Related concepts:

"About network view templates" on page 72
A network view template is a set of preconfigured network views that is defined in an XML file. Network administrators use templates to automatically generate network views.

Deploying pre-configured network views automatically

Use automatic deployment to make pre-configured network views globally available to specific network operators or groups of operators.

To deploy the templates, you must create an auto-provision script. This script must perform the following tasks:

- Create a top-level dynamic view node in the Network Views Navigation Panel, using a specified name
- Generate a set of network views using a specified template, and put the template in the top-level dynamic view node in the Navigation Panel
- Assign the network views generated to a specified user or user group.
- Use a specified domain.

Every 60 seconds the `ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision` directory is monitored for new auto-provision scripts. When a new auto-provision script is found, the script is read and processed, and the dynamic network view is created and assigned to the specified user or user groups.

To deploy pre-configured network views automatically:

1. Define the template as an XML file and save the template to the `ITNMHOME/profiles/TIPProfile/etc/tnm/autoprovision` directory.
2. Create the auto-provision script in XML. See "Sample auto-provision script" on page 72 for an example.

Sample auto-provision script

The following sample auto-provision script creates a view called NCOMS View and creates a set of views underneath using the dynamic view template ipdefault. These views are assigned to the itnmadmin user and use the domain NCOMS.

```
<autoProvision name="NCOMS View" domain="NCOMS" accessLevel="user"
accessId="itnmadmin">
        <dynamicViewTemplate id="ipdefault" />
</autoProvision
```

Network view templates

Read about network view templates and use this reference information to create new network view templates for Network Manager.

About network view templates

A network view template is a set of preconfigured network views that is defined in an XML file. Network administrators use templates to automatically generate network views.

The XML files that are used to define the templates are stored in the ITNMHOME/profiles/TIPProfile/etc/tnm/dynamictemplates directory.

Network administrators create templates based on the needs of network operators. The templates can be made available to operators in the following ways:

By saving the templates to a specified location
The operator can then choose to generate the preconfigured set of network views from the Network Views GUI, as one of the options available when creating a network view.

By assigning the templates to specified users or user groups
The administrator deploys the preconfigured views defined in one or more templates and assigns these views to a specific user, group or at a global level. Depending on how the templates have been assigned, operators find the preconfigured views automatically available in their Network Views Navigation Panel.

Related tasks:

"Creating template-based dynamic views" on page 64
Use a template-based dynamic view to generate a pre-configured set of dynamic views that are predefined by the network administrator.

"Making a pre-configured template available to operators" on page 71
Provide a template of pre-configured network views to network operators so that they can use the template to generate dynamic network views from the Network Views GUI themselves.

"Deploying pre-configured network views automatically" on page 71
Use automatic deployment to make pre-configured network views globally available to specific network operators or groups of operators.

Related reference:

"Default Network Manager dynamic network view template" on page 73
Network Manager is shipped with the ip_default.xml template. It consists of a set of the dynamic views that creates a dynamic view for each item available on the network.

Default Network Manager dynamic network view template

Network Manager is shipped with the `ip_default.xml` template. It consists of a set of the dynamic views that creates a dynamic view for each item available on the network.

Note: Do not use the `ip_default.xml` template if you have large or very large networks. The `ip_default.xml` template is intended mainly for educational purposes to demonstrate how the topology can be displayed. Running this template against a large or very large production topology could have a serious impact on the memory and performance of your Network Manager installation, particularly on displaying and using network views. Create network views manually if you have large or very large networks. For more information about network sizes, see Deployment scenarios.

Dynamic views are created for the following items:

- Alert views. The following alert views are presented:
  - All devices with PingFailRootCause events
  - All devices with SnmpLinkInDiscards events
  - Alert views based on event severities
  - Monitoring views: network views resulting from Network Manager polling and used by the adaptive polling scenarios
- ASMs running on devices. An ASM agent running on a device corresponds to a commercial server or database product running on that device. These network views group devices within a network based on the commercial server or database products running on those devices.
- BGP networks
- Customer MPLS VPNs
- Device classes
- HSRP groups
- IGMP
- IPMROUTE
- NAT address spaces
- OSPF routing domains
- Subnets
- VLANs
- VPLS
- VTP domains

No dynamic view is created for an item if no item of that type exists on the network. For example, if your network has no HSRP groups, then no dynamic view is generated for HSRP groups.

Complete Network Manager network view template

This template example uses all of the elements available from the template hierarchy. It includes network views based on user-defined filters and all the dynamic views.

Example

The following sample template XML file is provided for illustration purposes and uses all of the elements available from the template hierarchy.

```
<dynamicViewTemplate id="complete_template" label="Complete Template" manager="PrecisionIP">

<!--  "Classic" Class Partition -->

<!-- VPLS -->
<container id="vpls" label="VPLS">
 <dynamicMplsVpn id="vpls_vpns" label="VPLS VPNs" ceDevices="true"/>
</container>

<!-- IP Multicast Routing View -->
 <dynamicCollection id="ipMRoutingMdts" label="Multicast Routing MDTs" entityType="46" connectivity="ipMRoute"/>

<!-- IGMP View -->
 <dynamicCollection id="igmpGroups" label="IGMP Groups" entityType="121"/>

<dynamicDistinct id="device_classes" label="Device Classes" connectivity="ipsubnets" endNodes="false">
        <tableField table="chassis" field="className" />
    </dynamicDistinct>

<!--  BGP Networks -->
    <collection id="bgp_networks" label="BGP Networks" entityType="30">
        <entity name="BGP Networks" />
    </collection>

<!-- PIM Network -->
 <collection id="pim_network" label="PIM Network" entityType="42">
  <entity name="PIM Network"/>
 </collection>

<!-- Unassigned view-->
 <unassigned id="unassigned_view" label="Unassigned_View" />

<!-- Custom view (previously known as a manual view)-->
 <custom id="custom_view" label="Custom_View" connectivity="ipsubnets"/>

<!--  Global VLANs -->
    <dynamicCollection id="global_vlans" label="Global VLANs" entityType="16" />

<!--  HSRP Groups -->
    <dynamicCollection id="hsrp_groups" label="HSRP Groups" entityType="18" />

<!--  OSPF Routing Domains -->
    <dynamicCollection id="ospf_routing_domains" label="OSPF Routing Domains" entityType="21" />

<!--  VTP Domains -->
    <dynamicCollection id="vtp_domains" label="VTP Domains" entityType="24" />

<!--  Subnets -->
    <dynamicSubnet id="subnets" label="Subnets" classes="ab" />

<!--  MPLS -->
    <container label="mpls" label="MPLS">
        <collection id="mpls_core" label="MPLS Core" entityType="17">
            <entity name="VPN_CONTAINER_MPLS Core" />
        </collection>
        <dynamicMplsVpn id="mpls_vpns" label="MPLS VPNs" ceDevices="false" />
    </container>

<!-- MPLS TE -->
 <dynamicCollection id="mpls_te" label="MPLS TE" entityType="36"/>

<!-- Static MPLS -->
    <mplsVpn id="mpls_vpn" label="Static MPLS VPN" ceDevices="true">
        <entity name="VPN_CONTAINER_1104"/>
    </mplsVpn>

<!--  NAT Address Spaces -->
    <dynamicDistinct id="nat_address_spaces" label="NAT Address Spaces" connectivity="ipsubnets" endNodes="false">
        <tableField table="ipEndPoint" field="addressSpace" />
    </dynamicDistinct>

<!--  Discovered ASMs -->
    <dynamicDistinct id="discovered_asms" label="Discovered ASMs" connectivity="ipsubnets" endNodes="false">
       <tableField table="netcoolAsmsRunning" field="ASMName" />
    </dynamicDistinct>

<!-- Wildcard IP Filter -->
    <ipFilter id="ipfilter1" label="Filtered IPs 1" endNodes="true">
       <addressPattern pattern="192.*.*.*"/>
    </ipFilter>

<!-- Ranged IP Filter -->
    <ipFilter id="ipfilter2" label="Filtered IPs 2">
      <addressPattern pattern="192.168.3-4"/>
    </ipFilter>

<!-- Filtered for two class names -->
```

```
    <filtered id="filtered1" label="Network Devices/Linux Machines" endnodes="true" condition="or">
      <filter table="chassis" filter="className = 'NetworkDevice'"/>
      <filter table="chassis" filter="className = 'Linux'"/>
    </filtered>

<!-- Filtered for particular network devices -->
    <filtered id="filtered2" label="Network Devices: Main Node < 2000" endnodes="true" condition="and">
      <filter table="chassis" filter="className = 'NetworkDevice'"/>
      <filter table="chassis" filter="mainNodeEntityId < 2000"/>
    </filtered>

<!-- Devices that have been manually added with the topology editor -->
<!-- connectivity defaults to IP subnets -->
  <filtered id="ManuallyAdded" label="Manually Added Devices" endNodes="true">
    <filter schema="ncim" table="entity" filter="manual = 1" />
  </filtered>

<!-- All routers -->
  <filtered id="AllRouters" label="All Routers" connectivity="layer3">
    <filter schema="ncim" table="classMembers" filter="classId in (select classId from {%schema_ncim}entityClass where classType='Router')" />
  </filtered>

<!-- All switches -->
<filtered id="AllSwitches" label="All Switches" connectivity="layer2">
  <filter schema="ncim" table="classMembers" filter="classId in (select classId from {%schema_ncim}entityClass where classType='Switch')" />
  </filtered>

<!-- default event filtered type views based on severities -->
    <container id="alert_views" label="Alert views">

        <container id="acknowledged_alerts"  label="Acknowledged Alerts">
            <filtered id="Critical" label="Critical" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=5 and Acknowledged=1"/>
            </filtered>

            <filtered id="Major" label="Major" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=4 and Acknowledged=1"/>
            </filtered>

            <filtered id="Minor" label="Minor" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=3 and Acknowledged=1"/>
            </filtered>
        </container>

        <container id="Unacknowledged_alerts"  label="Unacknowledged Alerts">
            <filtered id="Critical" label="Critical" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=5 and Acknowledged=0"/>
            </filtered>

            <filtered id="Major" label="Major" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=4 and Acknowledged=0"/>
            </filtered>

            <filtered id="Minor" label="Minor" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="Severity=3 and Acknowledged=0"/>
            </filtered>
        </container>

<!-- Filter using the current time as a variable -->
  <filtered id="OldCriticalPingFail" label="Critical Ping Fail Events at least 1 hour old" connectivity="ipsubnets" endNodes="true">
    <filter schema="ncmonitor" table="activeEvent" filter="EventId = 'NmosPingFail' and Severity=5 and {%serverTime} - FirstOccurrence &gt;= 3600"/>
  </filtered>

<!-- default event filtered type view -->
    <filtered id="ping_fail_root_cause" label="PingFailRootCause" connectivity="ipsubnets" endNodes="true">
        <filter schema="ncmonitor" table="activeEvent" filter="EventId='NmosPingFail' and NmosCauseType='Root Cause'"/>
    </filtered>
<filtered id="snmppollfail" label="SNMP Poll Fail" connectivity="ipsubnets" endNodes="true">
  <filter schema="ncmonitor" table="activeEvent" filter="EventId='NmosSnmpPollFail'" />
  </filtered>

<!-- default event filtered type view -->
    <filtered id="SnmpLinkInDiscards" label="SnmpLinkInDiscards" connectivity="ipsubnets" endNodes="true">
        <filter schema="ncmonitor" table="activeEvent" filter="EventId='NmosSnmpLinkInDiscards'"/>
    </filtered>

<!-- Monitoring views -->
        <container id="Monitoring_views"  label="Monitoring Views">

            <filtered id="InitialPingFail" label="Initial Ping Fail Events" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="EventId = 'NmosPingFail' and Tally <= 18"/>
            </filtered>

            <filtered id="HighDiscardRate" label="Devices that have at least one interface event for HighDiscardRate" connectivity="ipsubnets" endNodes="true">
                <filter schema="ncmonitor" table="activeEvent" filter="EventId = 'Poll-HighDiscardRate'"/>
            </filtered>
        </container>

    </container>

</dynamicViewTemplate>
```

Network view template elements

Use this information to understand the elements that are used to create an XML template for a network view.

The following table describes the elements that are used to create a template.

Note: Each element can take the attributes `id` and `label`, in addition to the attributes listed in the table.

Table 7. Elements in the template XML

Element	Description	Attributes
addressPattern	Specifies an address pattern to filter device IP addresses.	pattern
collection	Generates a network view of a device collection.	entityType subgraph
container	Generates a container to group network views. Containers can also group other containers.	
dynamicCollection	Generates a dynamic view of a device collection.	entityType connectivity subgraph
dynamicDistinct	Generates a distinct dynamic view.	connectivity endNodes
dynamicMplsVpn	Generates a dynamic view of MPLS VPNs.	ceDevices
dynamicSubnet	Generates a subnet dynamic view.	classes
dynamicViewTemplate	Defines a template.	manager
entity	Specifies a device collection to display in the network view.	name
filter	Specifies a custom filter on the chosen table and fields within it. The filter is performed on an inner join between the "entity" table and the specified table.	schema table filter
filtered	Generates a network view of a device collection, filtered based on other tables and fields.	endNodes connectivity condition
ipFilter	Generates a network view of a device collection, filtered by the IP address of each. A device must pass at least one child addressPattern filter to be shown.	endNodes connectivity
manual	Generates an empty manual view.	
mplsVpn	Generates a network view of MPLS VPNs.	ceDevices
tableField	Specifies a topology database table and field to use as a category.	table field

Table 7. Elements in the template XML (continued)

Element	Description	Attributes
unassigned	Generates an empty unassigned view.	

Network view template attributes

Use this information to understand the attributes that are used to create an XML template for a network view.

The following table describes the attributes that are used to create a template.

Note: Attributes must be enclosed within quotation marks; for example, `id="device_classes"`.

Table 8. Attributes in the template XML

Element	Description
ceDevices	Specifies whether to display customer-edge (CE) routers in a dynamic view of MPLS VPNs. Options are the following: • `false`: do not display CE routers • `true`: display CE routers
classes	Specifies which types of subnets to display in a subnet dynamic view. Options are the following: • `ab`: class A and B subnets • `abc`: class A, B, and C subnets
condition	The operator to combine multiple filters. Options are the following: • and • or
connectivity	Specifies the type of connectivity to use to display the network views. Options are: • `layer1` • `layer2` • `layer3` • `ipsubnets`
endNodes	Specifies whether to display end nodes, such as workstations and printers, in the network view. Options are as follows: • false: do not display end nodes (default) • true: display end nodes
entityType	Specifies the type of the device collection to display. For example, to display VLANs, set this attribute to `16`, which is the entityType field value for VLANs in the topology database.
field	Specifies a topology database field to use in a distinct dynamic view.

Table 8. Attributes in the template XML (continued)

Element	Description
filter	SQL filter to use. Any strings within the SQL filter must be coded within single quotation marks. It is necessary to use XML escape sequences for certain symbols. Examples of filters are: • "className = 'NetworkDevice'" • "mainNodeEntityId &gt; 2000" **Note:** If filtering using entityId, you must specify the corresponding table attribute as entity.The filter string can use variables in the form `{%`*`variable`*`}`. For example, the following filter shows events that are older than an hour: `<filter schema="ncmonitor" table="activeEvent" filter="{%serverTime} - FirstOccurrence &gt; 3600">`. In Network Manager 3.9, the only supported variable is `{%serverTime}`.
id	Contains a template identifier. If you deploy pre-configured views automatically using a template, use the id identifier to use in the auto-provision script in the dynamicViewTemplate attribute.
label	Contains the label used to identify a template in the Network Views GUI. The operator sees this label in the New View dialog box when the operator creates a template-based dynamic view.
manager	Contains the name of the network management system that manages the devices to be visualized in the generated network views; for example, `PrecisionIP` for Network Manager.
name	Contains the name of the device collection to display. You can also use this attribute to specify the name of a container node and of dynamic views.
pattern	Specifies a filter pattern for IP addresses; for example, 192.*.*.8, or 192.168.3–4.
subgraph	Provides the option, within the network view, to display entities in logical groups surrounded by a boundary (cloud), which can be expanded and collapsed. This attribute can take the following values: • `subgraph = "False"`: enable display of entities in logical groups surrounded by a boundary (cloud). • `subgraph = "True"`: enable display of entities in logical groups connected to a ring, which cannot be expanded or collapsed.

Table 8. Attributes in the template XML (continued)

Element	Description
schema	Specifies a database schema within the NCIM database. By default the value of the schema attribute is set to `ncim`. You do not need to specify the schema attribute if you want to reference a table in the `ncim` schema. However, if you want to reference a table in a different schema, then you must set the value of the schema attribute. For example, to reference the activeEvent table in the `ncmonitor` schema, set `schema = ncmonitor`.
table	Specifies a topology database table to use in a distinct dynamic view.

Entity types

The entityType table contains all the entity types that are available in the NCIM topology database.

The following table lists the entity types available in the topology database.

Table 9. Summary of the information in the entityType table

Value (entityType)	Entity type name (typeName)	Category (metaClass)
0	Unknown	Element
1	Chassis	Element
2	Interface	Element
3	Logical Interface	Element
4	Local VLAN	Element
5	Module	Element
6	PSU	Element
7	Logical Collection	Collection
8	Daughter Card	Element
9	Fan	Element
10	Backplane	Element
11	Slot	Element
12	Sensor	Element
13	Virtual Router	Element
15	Subnet	Collection
16	Global VLAN	Collection
17	VPN	Collection
18	HSRP Group	Collection
19	Stack	Element
20	VRF	Element
21	OSPF Routing Domain	Collection
22	OSPF Service	Service

Table 9. Summary of the information in the entityType table (continued)

Value (entityType)	Entity type name (typeName)	Category (metaClass)
23	OSPF Area	Collection
24	VTP Domain	Collection
25	Other	Element
26	BGP Service	Service
27	BGP AS (Autonomous System)	Collection
28	BGP Route	Attribute
29	BGP Cluster	Collection
30	BGP Network	Collection
31	ISIS Service	Service
32	ISIS Level	Collection
33	OSPF Pseudo-Node	Element
34	ITNM Service	Collection
35	MPLS TE Service	Service
36	MPLS TE Tunnel	Element
37	MPLS TE Resource	Element
38	MPLS LSP	Element
40	IP Connection	Element
41	PIM Service	Service
42	PIM Network	Collection
43	IPMRoute Service	Service
44	IPMRoute Upstream	Element
45	IPMRoute Downstream	Element
46	IPMRoute MDT	Collection
47	IPMRoute Source	Element
48	IPMRoute Group	Element
49	IP Path	Collection
50	IP Endpoint	Protocol Endpoint
51	VLAN Trunk Endpoint	Protocol Endpoint
52	Frame Relay Endpoint	Protocol Endpoint
53	OSPF Endpoint	Protocol Endpoint
54	ATM Endpoint	Protocol Endpoint
55	VPWS Endpoint	Protocol Endpoint
56	BGP End Point	Protocol Endpoint
57	ISIS End Point	Protocol Endpoint
58	MPLS Tunnel End Point	Protocol Endpoint
59	TCP/UDP End Point	Protocol Endpoint
60	PIM End Point	Protocol Endpoint
61	IPMRoute End Point	ProtocolEndPoint

Table 9. Summary of the information in the entityType table (continued)

Value (entityType)	Entity type name (typeName)	Category (metaClass)
62	IGMP End Point	ProtocolEndPoint
70	Topology	Topology
72	Layer 2 Topology	Topology
73	Layer 3 Meshed Topology	Topology
75	MPLS TE Topology	Topology
77	Pseudo Wire Topology	Topology
78	OSPF Topology	Topology
79	BGP Topology	Topology
80	IP Path Topology	Topology
81	PIM Topology	Topology
82	Local VLAN Topology	Topology
83	IPMRoute Topology	Topology
84	VPLS Pseudo Wire Topology	Topology
110	Generic Collection	Collection
120	IGMP Service	Service
121	IGMP Groups	Collection
122	VSI (Virtual Switch Instance)	Element

Chapter 3. Configuring tools and menus

You can create and edit context menus, configure user access to menu items, define the context in which menus are available, and create tools that can be run from the context menus.

About context menus

Context menus are opened by right-clicking on devices, events, or subnets. You can run tools from context menus. You apply filters to menus and tools.

As an administrator, you can create context menus that enable operators to run tools on devices, events, or subnets. You can configure which users can access the tools, and where the tools and menus can be used from.

About filters

Filters are pieces of XML code that form part of an XML menu definition or an XML tool definition. There are two types of filter: *context filters* and *security filters*.

Filter characteristics are inherited by submenu and tools. For example if the `My Tools...` menu has context or security restrictions, then these restrictions are applied to all menus and tools within the `My Tools...` menu.

If no filter is present then the menu or tool will always appear in the context menu.

Related tasks:

"Defining context filters for tools and menus" on page 97
You can specify the views in which a menu or tool is available, and which devices it can be run on, using context filters.

"Defining user access for tools and menus" on page 99
You can specify the users, roles, and groups authorized to display a tool or menu using security filters.

About tools

Tools are defined in XML files in the `ITNMHOME/profiles/TIPProfile/etc/tnm/tools` directory. You can associate the following types of tools with a menu option: URL tools and local tools.

Related tasks:

"Creating tools for context menus" on page 86
You can create tools for operators to use and add them to context menus on a network map.

Configuring context menus

You can add a menu item to, or edit the menu items in, the context menus that are displayed when you right-click a device or subnet from a topology map.

You can associate tools with menu items to enable network operators to right-click a device and run a script or a third-party Web application. Any new menu items you define appear after the default menu items.

To add or edit an item for a device or subnet in a context menu, complete the following steps.

1. Edit an XML file in the `ITNMHOME/profiles/TIPProfile/etc/tnm/menus` directory.
2. Configure the elements and attributes of the menu definition to define the name, filters, label, and other properties of the menu item. Use the reference information about the XML elements and attributes available for menu items and the example provided to help you define the menu item.
3. Add the menu item that you have defined to the appropriate menu type in the `ITNMHOME/profiles/TIPProfile/etc/tnm/topoviz.properties` file:

   Menus launched from devices

   `topoviz.menu.device =` *`menu-id`*

   Menus launched from subnets

   `topoviz.menu.subview =` *`menu-id`*

   Where *menu-id* is an identifier that points to the top level of a menu hierarchy defined in an XML file in the `ITNMHOME/profiles/TIPProfile/etc/tnm/menus` directory. Subnets require a separate menu because the tools executed on subnets are executed for all nodes contained within the subnet.

   The following example defines a menu item for devices with the identifier "mytools":

   ```
   topoviz.menu.device = mytools
   ```

XML elements and attributes for defining context menus

Understand the different XML elements and attributes that define context menu items.

Sample menu item definition

The following example shows the format of an XML file that defines a menu item. Elements are highlighted in bold for clarity.

```
<ncp_menu id="mytools" label="My Tools" key="key">
<context>
<!-- This section of the xml file is a context filter. -->
<!-- Context filters specify the device and view conditions -->
<!-- under which this menu is displayed. -->
</context>
<security>
<!-- This section of the xml file is a security filter. -->
<!-- Security filters specify the users, roles and groups -->
<!-- authorized to display this menu. -->
</security>
<definition>
<tool id="ncp_dns"/>
<separator/>
```

```
<menu id="ncp_cisco"/>
<menu id="ncp_juniper"/>
</definition>
</ncp_menu>
```

XML elements and attributes

The following table describes the elements and attributes used to define context menus, with reference to the above example.

Table 10. Elements and Attributes in the menu XML definition file

Element or attribute	Type	Description
`ncp_menu`	Element	Introduces the definition of a menu.
`context`	Element	Defines the views and devices that the menu items is available from. Use the reference information about defining context filters to define this attribute.
`security`	Element	Defines the users, groups and roles that are allowed to view the menu item. Use the reference information about defining user access filters to define this attribute.
`id`	Attribute	Contains an alphanumeric identifier for this menu.
`label`	Attribute	Contains the actual text of the menu option that appears in the context menu.
`key`	Attribute	Used as a lookup into the `ITNMHOME/profiles/TIPProfile/etc/tnm/locale/ ncp_menus(_xx_XX).properties` file. This allows you to specify translations of the menu label for users with different locale settings.
`tool`	Element	Inserts a tool with the specified `id` into the menu. In this example, a tool with the id ncp_dns is inserted into the menu. The associated menu text for this tool is **DNS Lookup**. The ncp_dns tool is defined in a separate XML file stored in `ITNMHOME/profiles/TIPProfile/etc/tnm/tools`.
`separator`	Element	Inserts a separator into the menu.
`menu`	Element	Inserts a submenu with the specified `id` into the menu. In this example, two submenus are defined: • The `ncp_cisco` submenu. The associated menu text for this submenu is `Cisco Tools....` • The `ncp_juniper` submenu. The associated menu text for this submenu is `Juniper Tools....` Each of these submenus is defined in a separate `.xml` file stored in `ITNMHOME/profiles/TIPProfile/etc/tnm/menus`. These `.xml` files are formatted according to the rules defined in this section.

Creating tools for context menus

You can create tools for operators to use and add them to context menus on a network map.

Related concepts:

"About tools" on page 83
Tools are defined in XML files in the ITNMHOME/profiles/TIPProfile/etc/tnm/tools directory. You can associate the following types of tools with a menu option: URL tools and local tools.

Adding reports to context menus

You can add existing reports to context menus. Operators can run the reports from devices in any network map.

There are several reports available by in the context menu by default. You can add additional reports to the context menu.

To add a report to a context menu, complete the following steps.

1. On the server where the Tivoli Integrated Portal is installed, create or edit a tool definition XML file in the following directory: ITNMHOME/profiles/TIPProfile/etc/tnm/tools. Create a separate file for each menu item and give each file a meaningful name.
2. In the tool definition file, define the parameters for the report. Some parameters, such as the domain and entity name, are retrieved from the environment and embedded in the report URL. Default values are used for report parameters that are not defined. If no default values exist, you are prompted for a value. The following example tool definition defines a tool called ifInDiscards, which launches a generic trend analysis report using the poll policy ifInDiscards.

```
<?xml version="1.0"?>
<ncp_tool id="ncp_ifindiscards_report" key="ncp_ifindiscards_report" label="IfInDiscards Report" type="url">
        <url value="../../../tarf/servlet/component" target="_blank" windowFeatures="ScrollBars=yes,
Resizable=yes,Width=1280,Height=1024" method="GET">
        <parameter name="b_action" valueType="text" text="cognosViewer"/>
        <parameter name="ui.action" valueType="text" text="run"/>
        <parameter name="ui.object" valueType="text" text="/content/package[@name='Network Manager']
/folder[@name='Performance Reports']/report[@name='Generic Trend Analysis']"/>
        <parameter name="ui.name" valueType="text" text="ifInDiscards Usage"/>
        <parameter name="run.outputFormat" valueType="text" text="HTML"/>
        <parameter name="run.prompt" valueType="text" text="false"/>

        <parameter name="p_Domain" valueType="domainName" />
        <parameter name="p_PollDefinition" valueType="text" text="ifInDiscards"/>
        <parameter name="p_Hostname" valueType="ncim" table="entityData" column="entityName"
runOnMainNode="true"/>

  </url>
</ncp_tool>
```

3. Edit the file ITNMHOME/profiles/TIPProfile/etc/tnm/menus/ncp_reports.xml and add a menu entry that references the tool definition file. The following example defines context menu options for several reports, including the ncp_ifindiscards_report defined in the previous example, under a menu titled **Reports**.

```
<ncp_menu id="ncp_reports_menu" key="ncp_reports_menu" label="Reports">
 <definition>
  <tool id="ncp_bandwidth_in_report"/>
  <tool id="ncp_bandwidth_out_report"/>
  <tool id="ncp_availability_report"/>
```

```
    <tool id="ncp_ifindiscards_report"/>
    <tool id="ncp_memory_usage_report"/>
    <tool id="ncp_cpu_usage_report"/>
    <tool id="ncp_cisco_device_dashboard"/>
    <tool id="ncp_monitored_policies_report"/>
   </definition>
  </ncp_menu>
```

You can define which reports are available to run on which kinds of devices by using context filters.

URL tools

A URL tool opens a new browser window and applies a specified URL.

Examples of URL tools that you can configure to extend the right-click tools include the following:

- Third-party applications.
- Custom CGI scripts.
- Web sites: Use an absolute URL, for example http://www.any_company.com.

URL tools are defined in an XML file that is located in the `ITNMHOME/profiles/TIPProfile/etc/tnm/tools` directory.

You can specify the features of the window in which the tool opens. You can specify window features either by specifying the most common features using a parameter per feature, or by specifying any feature using a common parameter.

Example

The following example shows a URL tool that traces a route from the server to a selected device or component, and shows the format of the XML file used to define the URL tool. Elements and attributes are highlighted in bold for explanatory purposes only.

```
<ncp_tool id="server_traceroute" label="Trace route from server" type="url" runforeach="false" runonlist="true"
key="key">
<url value="/webtop/cgi-bin/traceroute.cgi" target="_blank">
<parameter name="host" valueType="ncim" table="chassis" column="accessIPaddress" runOnMainNode="true"/>
</url>
<context>
<!-- This section of the xml file is a context filter. -->
<!-- Context filters specify the device and view conditions -->
<!-- under which this tool is displayed.-->
</context>
<security>
<!-- This section of the xml file is a security filter. -->
<!-- Security filters specify the users, roles and groups -->
<!-- authorized to display this tool. -->
</security>
</ncp_tool>
```

Sample URL tool

Use this example information to understand the XML attributes and elements that are used to define a URL tool.

The following XML code shows the use of the `parameter` attribute.

```
<ncp_tool id="url_tool_id" label="My URL Tool" type="url"
<url value="/mytool/doSomething.do" target="_blank">
<parameter name="domain" valueType="domainName"/>
<parameter name="webtopds" valueType="webtopDataSource"/>
<parameter name="host" valueType="ncim" table="chassis"
column="accessIPaddress" runOnMainNode="true"/>
<parameter name="retries" valueType="text" text="3"/>
<parameter name="userId" valueType="cookie" cookieName="userId"/>
```

```
</url>
<context>
......
</context>
<security>
......
</security>
</ncp_tool>
```

This example, when executed against a device, produces a URL that has the following form:

```
https://server:port/ibm/console/mytool/doSomething.do?domain=NCOMS
&webtopDataSource=NCOMS&host=1.2.3.4&retries=3&userId=fred
```

Sample Window features for URL tools

Use these examples to help you specify the features of the window in which a URL tool opens.

In the following examples, attributes are highlighted in **bold** for explanatory purposes only.

Example 1

The following example shows how to specify the most common features using a parameter per feature.

```
<ncp_tool id="url_tool_id" label="My URL Tool" type="url"
<url value="/mytool/doSomething.do" target="_blank" width="500" height="500"
status="no" resizable="no">
</url>
......
</ncp_tool>
```

Example 2

The following example shows how to specify any window feature using a common `windowFeatures` parameter.

```
<ncp_tool id="url_tool_id" label="My URL Tool" type="url"
<url value="/mytool/doSomething.do" target="_blank" windowFeatures="width=500,
height=500, menubar=no, toolbar=no,
location=no, status=no, resizable=no">
</url>
......
</ncp_tool>
```

Local tools

A local tool runs a command on the client workstation.

Examples of commands that can be run in this way include `traceroute.exe` and `ping.exe`.

“Example 1: Solaris” on page 89
“Example 2: Windows” on page 89
“Elements and attributes” on page 89

Examples

The following examples show a URL tool that traces a route from the local workstation to a selected device or component, and shows the format of an XML file used to define this local tool. The XML code generates the command for the operating system on which the client is running. Elements are highlighted in bold for explanatory purposes only. The XML code can be extended for other operating systems.

Example 1: Solaris

Solaris The following example shows the code that is required to generate the command on Solaris operating systems:

```
<ncp_tool id="local_traceroute" label="Trace route from local machine" type="local" runForEach="true"
runOnList="false">
<command platform="Solaris" enabled="true">
<commandElement valueType="text" text="xterm -e /bin/sh -c '/usr/sbin/traceroute" />
<commandElement valueType="ncim" table="entity" column="entityName" runOnMainNode="true"
noTrailingSpace="true" />
<commandElement valueType="text" text="; read a'" />
</command>
 </ncp_tool>
```

This example, when executed against a selected device, produces a command that traces the route from the local host to the selected device. This command takes the following form:

```
xterm -e /bin/sh -c '/usr/sbin/traceroute my_entity; read a'
```

Where *my_entity* is the name of the device returned by the NCIM topology database query.

Example 2: Windows

Windows The following example shows the code that is required to generate the command on Windows operating systems:

```
<ncp_tool id="local_traceroute" label="Trace route from local machine" type="local"
runForEach="true" runOnList="false">
<command platform="windows" enabled="true">
<commandElement valueType="text" text="start cmd /k %WINDIR%\\SYSTEM32\\TRACERT.EXE" />
<commandElement valueType="ncim" table="entity" column="entityName" runOnMainNode="true" />
</command>
 </ncp_tool>
```

Elements and attributes

The following table describes the XML elements and attributes used to define a local tool.

Table 11. Elements and attributes in the tool XML definition file

Element or attribute	Type	Description
ncp_tool	Element	Introduces the definition of a tool.
id	Attribute	Contains an alphanumeric identifier for this tool.
label	Attribute	Contains the actual text of the menu option for this tool that appears in the context menu.
type	Attribute	The following types of tool are supported: • url: use this option to define a URL tool. • local: use this option to define a local tool.

Table 11. Elements and attributes in the tool XML definition file (continued)

Element or attribute	Type	Description
runforeach	Attribute	If set to the value true, then this tool is run once for each selected node.
runonlist	Attribute	If set to the value true, then this tool is run once only. The selected nodes are are passed to the tool as a comma-separated list.
command	Element	Builds up the command by adding together one or more commandElement elements. Each commandElement element adds a string of text to the command. The string of text added varies according to the value of the valueType attribute.
platform	Attribute	Operating system for which the command applies. The following are valid values: • Windows • Solaris • Linux • HPUX • AIX
enabled	Attribute	Indicates whether the tool is available for a specified operating system.
commandElement	Element	Defines a string of text to be added to the command. By default, a space is added to the command after the output of each commandElement, unless you supply a noTrailingSpace attribute with the value set to true.
valueType	Attribute	Indicates how to create the string of text specified in the commandElement element. This attribute can take one of the following values: • domainName: name of the Network Manager IP Edition domain containing the device or devices against which the tool is executing. • webtopDataSource: name of the Tivoli Netcool/OMNIbus Web GUI data source mapped to the Network Manager IP Edition domain containing the device or devices against which the tool is executing. • ncim: retrieves the value of a field in the NCIM topology database. Use the table and column parameters to specify the topology database field. Set the runOnMainNode attribute to true in order to use the entityId field associated with the main node containing a selected interface. • cookie: obtains the value of the cookie specified using the cookieName attribute. • text: specified text attribute is added to the command.
text	Attribute	Specifies a text string to add to the command.

Adding CGI scripts to context menus

To make additional tools available when network operators right-click a device, extend the context menu to include a custom CGI script. User-defined tools are accessed by right-clicking a device.

Restriction: You cannot launch a user-defined tool on a device of type `Subnet`.

You must store all CGI scripts in `NCHOME/omnibus_webgui/etc/cgi-bin`

You must register CGI tools in the Tivoli Netcool/OMNIbus Web GUI.

CGI script parameters

When you write a CGI script for use in an extended context menu, you must use the script parameters to reference the device from which the script is called.

To reference the device, use the following fixed parameters, which are automatically passed to user-defined scripts by TopoViz.

Attention: The parameters are provided only when no parameters are specified in the URL tool definition. Otherwise, the parameters passed to the CGI script are as specified in the tool.

$selected_rows.ServerName
This value defines the name of the ObjectServer that corresponds to the current Network Manager domain. This value is defined in the `ncp.domains` table when the topology database is created.

$selected_rows.NmosObjInst
This value is a unique identifier for the device. It is equivalent to the ObjectId field in the mainNodeDetails table of the topology database.

$selected_rows.Node
This value is from the ObjectServer. The value is usually equivalent to the IpAddress field in the mainNodeDetails table of the topology database.

These values refer to the device that was selected when the context menu was used. Topoviz uses an HTTP `Get` request to call the script and passes the above parameters in the URL. The URL is encoded into x-www-form-urlencoded format. Non-alphanumeric characters are converted into the 3-character string *%xy*, where *xy* is the two digit hexadecimal representation of the lower 8-bits of the character.

Example

If a script named `traceroute.cgi` is run on the host `192.168.21.35`, and the script is passed the following variables:

- *ServerName=Primary_01*
- *NmosObjInst=1477*
- *Node=192.168.0.7*

A new browser window is opened with the following URL:

```
https://192.168.21.35:16316/ibm/console/webtop/cgi-bin/traceroute.cgi?
%24selected_rows.ServerName%3DPrimary_01%26%24selected_rows.NmosObjInst
%3D1477%26%24selected_rows.Node%3D192.168.0.7
```

CGI support

Use the initialization parameters to control the behavior of CGIServlet.

CGIServlet

CGI scripts run on a Web server and use the Common Gateway Interface (CGI) to perform tasks. The support for CGI in Tivoli Integrated Portal is provided by *CGIServlet*, extracted from Apache Tomcat. The Tomcat CGI support is largely compatible with the Apache HTTP Server but there are some limitations (such as only one cgi-bin directory). To change the configuration, edit `web.xml` in the directory where the CGI application is installed.

Servlet initialization parameters

Several initialization parameters are available for configuring the behavior of the CGIServlet.

cgiPathPrefix
The CGI search path will start at the Web application root directory + File.separator + this prefix. Default setting: `cgiPathPrefix` is `Web-INF/cgi`.

debug
Determines the level of debugging detail for messages that are logged by the servlet. Default setting: `0`.

executable
This is type of the program to be used to run the script. Default setting: `perl`.

parameterEncoding
Names the parameter encoding to be used with the CGI servlet. Default setting: `System.getProperty("file.encoding","UTF-8")`.

passShellEnvironment
Determines whether shell environment variables, if there are any, shall be passed to the CGI script. Default setting: `false`.

Registering tools in the Tivoli Netcool/OMNIbus Web GUI

After you have created the CGI script, and defined the appropriate tool, you must register the tool in the Web GUI so that you can use the tool in Topoviz.

The Tivoli Netcool/OMNIbus Web GUI was known as Netcool/Webtop in versions 2.2 and below. Registering your tool makes it available in Topoviz only.

From the CGI Registration window you can configure settings and properties for the tool. See the *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide* for more details.

To register a tool in the Web GUI:

1. Click **Content**. From the **Menus & Tools** list, select **CGI Registration** > **Register**. The CGI Registration page is displayed.
2. Type the name of the tool and the file name of the script.

To make the tool available in the Web GUI, you must add the tool to the main Web GUI client.

Making tools available in the Tivoli Netcool/OMNIbus Web GUI

In addition to registering the tool in the Web GUI, you must also make the tool available in the main Web GUI client.

The Tivoli Netcool/OMNIbus Web GUI was known as Netcool/Webtop in versions 2.2 and below.

From the Tools Editor window you can configure settings and properties for the tool. See the *IBM Tivoli Netcool/OMNIbus Web GUI Administration and User's Guide* for more details.

To create a tool in the Web GUI:

1. Click the **Content** tab. From the **Menus & Tools** list, select **Tools**. The Tools Editor page is displayed.
2. Click **Create**. The Create New Tool page is displayed.
3. Type the name and type of the tool.

Configuring scope of the Show Connectivity Information tool

You can specify which interface types to display when the **Show Connectivity Information** tool is run on a device in Network Hop View or Network Views. By default, all interface types are displayed.

Before performing this task you must determine the appropriate interface types IDs. You can do this by performing the following SQL query on the NCIM topology database.

```
SELECT * FROM ncim.enumerations where enumGroup = 'ifType';
```

The **Show Connectivity Information** tool displays a table of devices and interfaces connected to a selected device. By default all interface types on the selected device are included in this table. You can specify interface types to include in or exclude from this table.

1. Open the `ITNMHOME/profiles/TIPProfiles/etc/tnm/topoviz.properties` configuration file.
2. Specify interface types to display in the **Show Connectivity Information** tool by either including interface types or excluding interface types.
   a. Include interface types by typing a line similar to the following example anywhere in the `topoviz.properties` file.

      ```
      topoviz.connectivity.includes=2,36
      ```

      In this example, the **Show Connectivity Information** tool displays interface types 2 and 36 only.

   b. Exclude interface types by typing a line similar to the following example anywhere in the `topoviz.properties` file.

      ```
      topoviz.connectivity.excludes=1
      ```

      In this example, the **Show Connectivity Information** tool displays all interface types except for interface type 1.

   Note: You must not use both includes and excludes parameters in the `topoviz.properties` file as this may produce unexpected results in the **Show Connectivity Information** tool.
3. Save and close the `topoviz.properties` file.

Creating tools that open the MIB browser

To provide additional diagnostic information for network operators, create custom tools that open the MIB browser from an AEL or from a topology map, and display information in the MIB browser.

For example, you can create a tool that opens the MIB browser in an AEL, performs an SNMP Walk query on all the interfaces of the affected device, and automatically displays this interface MIB data in the MIB browser.

MIB browser modes

Custom tools can open the MIB browser in one of two modes, *full mode* or *results-only mode*.

Full mode
: The complete MIB browser page is displayed, with the MIB tree, MIB Variable Information panel, and the SNMP Query Results panels

Results-only mode
: The results of the MIB browser query are displayed in the SNMP Query Results panel, as a single page.

Creating a custom tool

To provide additional information for network operators from an AEL or topology map, create a custom tool that displays information in the MIB browser.

1. Decide which data you want the MIB browser to display, and how you want the MIB browser to display the data.
2. Determine the URL that opens the MIB browser with the required content and format. The URL must have the following format:

   ```
   https://host:port/ibm/console/ncp_mibbrowser/Launch.do
   ```

   Where:

   - *host* is the IP address of the host on which the Tivoli Integrated Portal is running.
   - *port* is the port to access on the host. The default value is 16316.

   A URL in this format starts the MIB browser with the `Domain` option set to the first value in the list, and with no **Host** or **Value** options set in the **SNMP Query** toolbar.
3. Write a CGI script that constructs the URL in response to a right-click in an AEL or in a topology map.
4. To define and store the tool for use in Topoviz, register the tool in the Tivoli Netcool/OMNIbus Web GUI. The Tivoli Netcool/OMNIbus Web GUI was known as Netcool/Webtop in versions 2.2 and below.
5. To define and store the tool for use in the Web GUI, create the tool in the Web GUI.
6. To make the tool available as a right-click option in a context menu, create a menu entry in the Web GUI.

Optional parameters for MIB browser URLs

When you define a URL that starts the MIB browser, you can supply a number of additional optional parameters.

domain
The name of the IBM Tivoli Netcool® Manager IP Edition domain to use to obtain the MIB and SNMP data. The value of this parameter is used to set the **Domain** option menu in the **Configuration Toolbar**.

Tip: To write a tool that opens the MIB browser from an AEL, you can specify the name of the ObjectServer instead of the IBM Tivoli Netcool Manager IP Edition. To do this, specify the parameter $selected_rows.*ServerName* where *ServerName* is the field in the AEL event that specifies the name of the ObjectServer.

host The IP address of the target device to be queried for SNMP data. This value is used to populate the **Host** field in the **SNMP Query Toolbar**.

variable
The MIB object to query. This value can be the OID of the MIB object, for example 1.3.6.1.2.1.1.3 or it can be the name of the MIB object, for example sysUpTime. This value is used to populate the **OID** field in the **SNMP Query Toolbar**.

resultsOnly
Specifies whether the MIB browser is started in full mode or results-only mode. Specify one of the following options:

- `true`: The MIB browser opens in results-only mode.
- `false`: The MIB browser is opened in full mode.

If you supply the `domain`, `host`, and `variable` parameters, the MIB browser is started, automatically performs the SNMP query specified by these parameters and displays the results in the **SNMP Query Results** area. The type of SNMP query varies depending on the value of the variable parameter

XML elements and attributes for defining tools

Use these XML elements and attributes to define URL tools and tools that open reports.

The following table describes the XML elements and attributes used to define URL tools and tools that open reports.

Table 12. Elements and Attributes used to define URL tools and tools that open reports

Element or attribute	Type	Description
`ncp_tool`	Element	Introduces the definition of a tool.
`id`	Attribute	Contains an alphanumeric identifier for this tool.
`label`	Attribute	Contains the actual text of the menu option for this tool that appears in the context menu.
`type`	Attribute	The following types of tool are supported: • `url`: use this option to define a URL tool. • `local`: use this option to define a local tool.
`runforeach`	Attribute	If set to the value `true`, then this tool is run once for each selected node.

Table 12. Elements and Attributes used to define URL tools and tools that open reports (continued)

Element or attribute	Type	Description
runonlist	Attribute	If set to the value true, then this tool is run once only. The selected nodes are passed to the tool as a comma-separated list.
key	Attribute	Used as a lookup into the ITNMHOME/profiles/TIPProfile/ etc/tnm/locale/ ncp_tools(_xx_XX).properties file. This allows you to specify translations of the tool label for users with different locale settings.
url	Element	Specifies the URL to open when a user selects this tool.
value	Attribute	Specifies the URL for the url element.
target	Attribute	This is standard HTML syntax and specifies the name of the window to open the tool into. Possible values include: • _blank: Opens the tool in a new window • _self: Opens the tool in the current window You can also specify a window name.
parameter	Element	Specifies parameters to pass to the URL. You can configure multiple parameters using the following parameter types. Each of these parameter types is formulated using a different valueType attribute: • Value of an NCIM topology database field. The data retrieved must be associated with an entity. • Name of the Network Manager IP Edition domain containing the device or devices against which the tool is executing. • Name of the Tivoli Netcool/OMNIbus Web GUI data source mapped to the Network Manager IP Edition domain containing the device or devices against which the tool is executing. • Value of a Web browser cookie. • Plain text. Use this parameter type to specify tool-specific parameters, such as the number of hops to pass to the tool that launches the Hop View, or the number of retries.
name	Attribute	Specify a name to be used for the parameter. Use the following keywords to specify the different parameter types: • domain: name of the Network Manager IP Edition domain containing the device or devices against which the tool is executing. • webtopds: name of the Tivoli Netcool/OMNIbus Web GUI data source mapped to the Network Manager IP Edition domain containing the device or devices against which the tool is executing. • host: value of an NCIM topology database field. The data retrieved must be associated with an entity. Use the appropriate name to specify a Web browser cookie or plain text parameter. For example, if a Web browser cookie is called userId, then use userId as the value of the name attribute.

Table 12. Elements and Attributes used to define URL tools and tools that open reports (continued)

Element or attribute	Type	Description
valueType	Attribute	Indicates how the Network Manager IP Edition Web application from which the tool is called obtains the value of the parameter. This attribute can take the following values: • domainName: obtains the name of the Network Manager IP Edition domain containing the device or devices against which the tool is executing. • webtopDataSource: obtains the name of the Tivoli Netcool/OMNIbus Web GUI data source mapped to the Network Manager IP Edition domain containing the device or devices against which the tool is executing. • ncim: retrieves the value of a field in the NCIM topology database. Use the table and column parameters to specify the topology database field. Set the runOnMainNode attribute to true in order to use the entityId field associated with the main node containing a selected interface. • cookie: obtains the value of the cookie specified using the cookieName attribute. • text: specified text attribute is added as a parameter value.
context	Attribute	Specifies the context filters for the tool.
security	Attribute	Specified the security filters for the tool.

Defining context filters for tools and menus

You can specify the views in which a menu or tool is available, and which devices it can be run on, using context filters.

To define a context filter for a menu or tool, complete the following steps.

1. Edit the XML file in the `ITNMHOME/profiles/TIPProfile/etc/tnm/menus` directory that defines the menu or tool to which you want to apply the filter.
2. Edit the `<context>` element to define the filter. Use the reference information about the XML elements and attributes available for context filters and the example provided to help you define the context filter.

Related concepts:

"About filters" on page 83
Filters are pieces of XML code that form part of an XML menu definition or an XML tool definition. There are two types of filter: *context filters* and *security filters*.

XML attributes for defining context filters

Understand the different XML elements and attributes that define context filters.

Sample context filter

The following example shows the format of a context filter:

```
<context>
        <attribute id="class">
                <matches regexp=".*Cisco*"/>
        </attribute>
        <attribute id="clientType">
                <equals value="ncp_hopview"/>
        </attribute>
        <attribute id="managed">
        </attribute>
        <attribute id="entityType">
                <equals value="1"/>
        </attribute>
</context>
```

If the menu is to be displayed, the context must match at least one of the items in each of the id attributes. In this example, the tool or menu is displayed if the following expression is true:

```
class = ".*Cisco*" AND clientType = "ncp_hopview" AND managed = true AND
entityType = "1"
```

This means that this tool is available only in the Hop View, and can be run only against managed, main node devices.

XML attributes of a context filter

The following table describes the XML elements, attributes, and operators available for the definition of a context filter.

Table 13. Elements, attributes, and operators in the context filter XML definition section

Element or Attribute	Type	Description
class	Value	Corresponds to the ClassName of the device on which the right-click is performed
clientType	Value	Web application from which the tool may be run. Possible values are: • ncp_hopview • ncp_networkview • ncp_structurebrowser
managed	Value	Indicates whether the tool can only be run against devices that are in the managed state. Possible values are: • true • false
entityType	Value	The type of device (entityType) that the tool can be run against.
equals	Operator	Performs a simple = comparison between attributes
matches	Operator	Performs a regular expression comparison between attributes
notequals	Operator	Performs a simple not= comparison between attributes

Defining user access for tools and menus

You can specify the users, roles, and groups authorized to display a tool or menu using security filters.

To define a security filter for a tool or menu, complete the following steps.

1. Edit the XML file in the `ITNMHOME/profiles/TIPProfile/etc/tnm/menus` directory that defines the menu or tool to which you want to apply the filter.
2. Edit the `<security>` element to define the filter. Use the reference information about the XML elements and attributes available for security filters and the example provided to help you define the security filter.

Related concepts:

"About filters" on page 83
Filters are pieces of XML code that form part of an XML menu definition or an XML tool definition. There are two types of filter: *context filters* and *security filters*.

XML attributes for defining security filters

Understand the different XML attributes of the `<security>` element that define security filters.

Example

The following example shows a security filter:

```
<security>
        <user name="bob"/>
        <user name="mary"/>
        <group name="Network Manager IP Desktop"/>
        <role name="ncp_networkview"/>
</security>
```

If the menu or tool is to be displayed, the context must match at least one of the following attribute assignments:

- User `bob`
- User `mary`
- Any user with the role `ncp_networkview`
- Any user in the group `Network Manager IP Desktop`

Elements and attributes of a security filter

The following table describes the XML elements, attributes, and operators available for the definition of a security filter.

Table 14. Elements, attributes, and operators in the security filter XML definition section

Element or attribute	Type	Description
`user`	Attribute	Assigns the tool or menu to a specific user
`group`	Attribute	Assigns the tool or menu to a specific group
`role`	Attribute	Assigns the tool or menu to a specific role

Chapter 4. Editing network topology

Edit the discovered network topology to manually add and remove devices and connections.

About topology editing

You can edit the discovered network topology by performing the following actions: adding network devices, adding connections between network devices, removing and deleting devices from the domain, and removing connections between network devices. The topology can only be edited in the Network Hop View.

For information on how to configure the Network Hop View to differentiate between manually added network devices and discovered network devices, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

Topology editing and the discovery process

Following a discovery, the Topology manager, ncp_model, inspects relevant tables in the NCIM topology database to determine which manual topology changes were made, and then makes sure not to overwrite those manual changes.

All manual changes to the topology are recorded in the NCIM topology database entityActions and connectActions tables.

For information on how to examine the audit log for manually added devices and connections, see the description of the `entityActions` and `connectActions` tables in the *IBM Tivoli Network Manager IP Edition Topology Database Reference*.

Audit trail of manual changes to the topology

All manual changes to the topology will be recorded in the NCIM topology database entityActions and connectActions tables. These tables facilitate an audit trail for manual topology changes as well as allow for the undo or reversal of a manual action.

For information on how to examine the audit log for manually added devices and connections, see the description of the `entityActions` and `connectActions` tables in the *IBM Tivoli Network Manager IP Edition Topology Database Reference*.

Adding devices to the topology

You can manually add main node device entities to the discovered network topology. You might want to do this because there is no access to a specific network device, or because device support (discovery agents) is not available for certain device types.

You use the Add Device Wizard to manually add a device to the topology. This wizard updates the NCIM topology database entityData, chassis, and ipEndPoint tables. For more information on these NCIM topology database tables, see the *IBM Tivoli Network Manager IP Edition Topology Database Reference*.

Note: Devices that are added manually can be displayed in the Network Views. Go to **Network Availability** > **Network Views** and select **Manually Added Devices** from the Network View tree.

To launch the wizard, complete these steps.

1. Click **Network Availability** > **Network Hop View** to go to the Network Hop View, and display a topology map. The topology map displayed must contain at least one of the devices to which you want to add a connection. For information on how to display a topology map in the Network Hop View, see the *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*.
2. In the Network Hop View, right-click a device or the background area of the topology map, and click **Topology Management** > **Add Device**. The Add Device Wizard Entity Details window opens.
3. Complete the Entity Details window as follows. The fields in this window populate the NCIM entityData table for the device that you are adding.

   domain
   The domain to which the device is being added. This value is retrieved from the domain of the Hop View from which the Add Device Wizard was launched.

   entityName
   IP address or DNS name for this device. For example, an IP address such as 172.20.1.7, or a DNS name, such as company-abc.net.

   Note: This value must be unique for all entities within the current domain.

   - If a manually added device with the same entity name already exists in this domain, then the wizard requires you to specify a different name.
   - If a discovered devices with the same entity name already exists in this domain, then the wizard allows you to add the device to the database, but not to the current domain.

   entityType
   Type of entity. This value is set to chassis. This means that you can only add a chassis, or main node device.

   displayLabel
   Label to display for this device in a network view or network hop view.

   description
   Textual description of this device

   reason Reason for adding this device to the topology.
4. Click **Next**. The Add Device Wizard checks the entity details entered.
   - If the entity name specified is unique within the domain, then the Chassis Details window opens.
   - If a discovered device with the same entity name specified already exists in the current domain, then a warning message is displayed at the bottom of the window together with an adjacent check box. Choose one of the following actions:
     - Select the check box to add this device to the NCIM topology database but not to the current domain. You will be able to view the entity in the Manually Added Devices network view only. You cannot add the device to the domain until the discovered device with the same name is

removed. For more information on the Manually Added Devices network view, see the *IBM Tivoli Network Manager IP Edition Administration Guide*.

– Leave the check box unchecked and click **Cancel** to exit without adding this device.

5. Complete the Chassis Details window as follows. The fields in this window populate the NCIM chassis table for the device that you are adding.

Classify By

Specify whether to classify this device by class name or by the sysObjectId field, the vendor's authoritative identification of the network management subsystem contained in the device itself.

className

The name of a class of devices. The master className field is in the entityClass table.If you specified **className** then this field lists the classes available in the NCIM database entityClass table. Select a class from this list to classify the device.

sysObjectId

The vendor's authoritative identification of the network management subsystem contained in the entity. If you specified **sysObjectId** then type a valid sysObjectId value for this device.

sysName

An administratively-assigned name for this managed node. By convention, this is the fully-qualified domain name of the node. If the name is unknown, the value is the zero-length string.

sysDescr

A textual description of the entity. This value must include the full name and version identification of the system hardware type, software operating-system, and networking software.

sysLocation

The physical location of this node, for example “telephone closet, 3rd floor.” If the location is unknown, the value is the zero-length string.

sysContact

The textual identification of the contact person for this managed node, and information on how to contact this person. If no contact information is known, the value is the zero-length string.

ipForwarding

Indication of whether this entity is acting as an IP gateway in respect to the forwarding of datagrams received by this entity but not addressed to this entity. IP gateways forward datagrams, whereas IP hosts do not (unless the source is routed through the host).

serialNumber

The serial number of the entity.

modelName

The model name of the entity.

accessIPAddress

The IP address through which this entity was discovered and will be monitored. If you specify a value for **accessIPAddress** then you must also specify a value for **accessProtocol**. The value specified for **accessIPAddress** must be valid within the Internet protocol specified for **accessProtocol**. For example, if you set **accessProtocol** to IPv4, then you must specify an IPv4 address.

accessProtocol
The Internet protocol used by the chassis. If you specify a value for **accessProtocol** then you must also specify a value for **accessIPAddress**.

DNSName
DNS name for the IP address associated with this IP end point. The value specified in this field is used to populate the NCIM ipEndPoint table for the device that you are adding.

Note: The DNSName field in the NCIM ipEndPoint table is only updated if you have specified a value for both the **accessProtocol** and **accessIPAddress** fields in this window.

6. Click **Next**. The Add Device Wizard checks the chassis details entered.
   - If no errors are returned, then the Confirm Details window opens.
   - If there are any errors, then you are prompted to correct them before proceeding.
7. In the Confirm Details window, review the information that you specified and click **Finish**. The Add Device Wizard checks the entity details entered.
   - If the operation was successful then a window opens indicating that the device was successfully added to the domain. Click **Add Like** option to add more devices with identical data except for the **entityName** and **displayName** fields.
   - If the value you entered in the **entityName** field was not unique in the current domain and a discovered device already exists with the same entity name, then the wizard displays a message indicating that the device was added to the NCIM topology database but not to the domain.

   The topology map in the Network Hop View is updated to display the newly added device.

   Note: If the Network Hop View is refreshed before a connection is added to the manually added device, then the manually added device will disappear from the network hop view as it has no connections.

Adding connections between devices

You can manually add connections between devices in the discovered network topology. You can add these connections between manually added devices or between discovered devices or between a mix of the two. This enables you to add connections that the Discovery engine was unable to discover.

You use the Add Connection Wizard to manually add a connections between devices. All connections added are stored in the NCIM topology database as bidirectional.

To launch the wizard, complete these steps.

1. Click **Network Availability** > **Network Hop View** to go to the Network Hop View, and display a topology map. The topology map displayed must contain at least one of the devices to which you want to add a connection. For

information on how to display a topology map in the Network Hop View, see the *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*.

2. In the Network Hop View, select one device or two devices. Then right-click to display the context menu and click **Topology Management** > **Add Connection.** from the context menu. Based on your device selections, you can perform one of the following actions:

   You selected one device

   You can connect this device to a device that is not displayed in the current hop view.

   You selected two devices

   You can connect these two devices to each other.

   Note: If you select more than two devices then the **Topology Management** > **Add Connection.** option is not available in the context menu.
   The Add Connection Wizard Device Selection window opens.

3. Complete the Device Selection window as follows. The fields in this window populate the NCIM connects table for the connection that you are adding.

   From Device

   IP address of the device that is the notional start of the connection.

   To Device

   IP address of the device that is the notional end of the connection. If you selected one device only then this field contains the text **<Click Next to select device>**.

   Swap Devices

   Allows you to switch the notional start and notional end of the connection.

4. Click **Next**. The next window displayed depends upon whether you initially selected one or two devices in the Network Hop View.
   - If you selected one device, then the Entity Search window opens. Use the Entity Search window to locate the **To Device**, the device at the notional end of the connection.
   - If you selected two devices then the Connection Details window opens. Go to Step 6 on page 106

5. Complete the Entity Search window as follows.
   - Use the Basic tab to search by IP address or device name.

     Domain

     Select the domain in which you want to search.

     IP Address

     Specify the IP address of the device. You can specify all of the address, or only the first part of the address. You can also use the percent character (%) or the asterisk (*) as wildcards.

     Device Name

     Specify the name of the device. You can specify all of the name, or only the first part of the name. You can also use the percent character (%) or the asterisk (*) as wildcards. Device names are not case-sensitive. If you specify both an IP address and a device name, the IP address takes precedence.
   - Use the Advanced tab to search by device attributes.

Domain
Select the domain in which you want to search.

Table Select the database table that you want to search. The mainNodeDetails table lists network devices.

Field Select the field whose value you want to search. The selection available for this field is automatically populated based on the chosen database.

Comparator
Select a comparator.

Value Required. Type the value that you want to search for. You can use the percent character (%) or the asterisk (*) as wildcards.

6. Complete the Connection Details window as follows.

   From Device
   IP address of the device that is the notional start of the connection.

   From Interface
   If interfaces exist on this device, then these are presented in the **From Interface** list. If an interface list exists, then you can make the connection at the interface or device level for this device.

   To Device
   IP address of the device that is the notional end of the connection. If you selected one device only then this field contains the text **<Click Next to select device>**.

   To Interface
   If interfaces exist on this device, then these are presented in the **To Interface** list. If an interface list exists, then you can make the connection at the interface or device level for this device.

   Connectivity
   Defaults to the connectivity setting in the Network Hop View.

   Note: If the topology map in the Network Hop View is set to IP Subnets then the **Connectivity** setting in this window defaults to Layer 2, the first item in the list.

   Speed The speed for this connection. This must be an integer value.

   Reason
   Reason for adding this connection to the topology.
7. Click **Next**. The Confirm Details window is displayed.
8. Review the information that you specified and click **Finish**. The Add Connection Wizard checks that a connection between the specified interfaces on the two devices does not already exist. If such a connection already exists, then a screen is displayed indicating that the wizard is unable to create this connection.
9. If one of the following conditions holds, then the Success window requires you to recenter the topology map before you can display the new connection. Click **Recenter & Close** to do this.
   - Neither of the devices selected for connection were seed devices in the original network hop view and one of the selected devices was not on the current network hop view.
   - The connectivity specified for the connection is not the same as the connectivity on the original network hop view.

Removing devices from the domain

You can remove both discovered devices and manually added devices from the current domain so that they no longer appear in the topology map. This action does not delete the affected devices from the NCIM topology database.

You use the Remove Device Wizard to manually remove devices from the current domain. This removes the association of the device or devices with the current domain and prevents the device from being visualized in topology maps in the Network Hop View or **Network Views** for the current domain. However, the underlying device data is not removed from the NCIM topology database.

Note: You can also delete a manually added device from the NCIM topology database using the **Topology Management** > **Delete Device** option. This option is not available for discovered devices.

To launch the wizard, complete these steps.

1. Click **Network Availability** > **Network Hop View** to go to the Network Hop View, and display a topology map. The topology map displayed must contain at least one of the devices which you want to remove. For information on how to display a topology map in the Network Hop View, see the *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*.
2. In the Network Hop View, select one or more devices to remove from the domain. Then right-click to display the context menu and click **Topology Management** > **Remove Device from Domain** from the context menu. The Remove DeviceWizard Device Selection window opens.
3. Complete the Device Selection window as follows.

   Please select the devices you would like to remove from the domain *domain_name*

   Lists all device selected in the topology map. You can change the selection here by deselecting devices as required.

   Reason

   Reason for removing these devices from the domain.
4. Click **Next**. The Confirm Details window is displayed.
5. Review the information on the Confirm Details window and click **Finish** The Success window is displayed indicating that the specified devices have been removed from the domain.

Deleting manually added devices

You can delete manually added devices from the topology. This action completely removes all data associated with the deleted devices from the NCIM topology database.

You use the Delete Device Wizard to delete manually added devices from the topology. All data associated with the manually added device is removed from the NCIM topology database.

To launch the wizard, complete these steps.

1. Click **Network Availability** > **Network Hop View** to go to the Network Hop View, and display a topology map. The topology map displayed must contain at least one of the devices which you want to delete. For information on how to

display a topology map in the Network Hop View, see the *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*.

2. In the Network Hop View, select one or more manually added devices to delete. Then right-click to display the context menu and click **Topology Management** > **Delete Device** from the context menu.

   Note: You can distinguish manually added devices from discovered devices by noting which devices have the associated manually added device icon 👤.
   The Delete Device Wizard Device Selection window opens.
3. Complete the Device Selection window as follows.

   Please select the devices you would like to permanently delete
   Lists all manually added device selected in the topology map. If you also selected discovered devices, these are ignored and are not shown in this list. You can change the selection here by deselecting devices as required.
4. Click **Next**. The Confirm Device Deletion window is displayed.
5. Review the information on the Confirm Device Deletion window and click **Finish**. The Success window is displayed indicating that the specified devices have been deleted from the topology.

Removing connections between devices

You can manually remove connections between devices in the network topology.

1. Click **Network Availability** > **Network Hop View** to go to the Network Hop View, and display a topology map. The topology map displayed must contain the connection that you want to delete. For information on how to display a topology map in the Network Hop View, see the *IBM Tivoli Network Manager IP Edition Network Troubleshooting Guide*.
2. In the Network Hop View, select the connection to remove. Then right-click to display the context menu and click **Topology Management** > **Remove Connection** from the context menu. The header at the top of the context menu displays the connection that is selected for removal.

   Note: You can only remove one connection, or one link in a multilink connection, at a time.
   - If the selected connection is made up of multiple links, then you must first click the link you want to remove, and then from the submenu that is displayed, click **Topology Management** > **Remove Connection**.
   - If you selected two or more different connections, then only the first connection that you selected is presented for removal.

   The Confirm Connection Removal window opens.
3. Complete the Device Selection window as follows.

   Connection
   Displays the device and interface details at either end of the connection. If the connection endpoint at either end is the device itself, then no interface data is shown.

   Layer Displays the connection layer for this connection.

   Reason
   Specify a reason for removing these devices from the domain.

4. Click **Confirm**. The Success window is displayed confirming that the connection has been removed.

Appendix. Network Manager glossary

Use this information to understand terminology relevant to the Network Manager product.

The following list provides explanations for Network Manager terminology.

AOC files
Files used by the Active Object Class manager, `ncp_class` to classify network devices following a discovery. Device classification is defined in AOC files by using a set of filters on the object ID and other device MIB parameters.

active object class (AOC)
An element in the predefined hierarchical topology of network devices used by the Active Object Class manager, `ncp_class`, to classify discovered devices following a discovery.

agent See, discovery agent.

class hierarchy
Predefined hierarchical topology of network devices used by the Active Object Class manager, `ncp_class`, to classify discovered devices following a discovery.

configuration files
Each Network Manager process has one or more configuration files used to control process behaviour by setting values in the process databases. Configuration files can also be made domain-specific.

discovery agent
Piece of code that runs during a discovery and retrieves detailed information from discovered devices.

Discovery Configuration GUI
GUI used to configure discovery parameters.

Discovery engine (ncp_disco)
Network Manager process that performs network discovery.

discovery phase
A network discovery is divided into four phases: Interrogating devices, Resolving addresses, Downloading connections, and Correlating connectivity.

discovery seed
One or more devices from which the discovery starts.

discovery scope
The boundaries of a discovery, expressed as one or more subnets and netmasks.

Discovery Status GUI
GUI used to launch and monitor a running discovery.

discovery stitcher
Piece of code used during the discovery process. There are various discovery stitchers, and they can be grouped into two types: data collection stitchers, which transfer data between databases during the data collection

phases of a discovery, and data processing stitchers, which build the network topology during the data processing phase.

domain
See, network domain.

entity A topology database concept. All devices and device components discovered by Network Manager are entities. Also device collections such as VPNs and VLANs, as well as pieces of topology that form a complex connection, are entities.

event enrichment
The process of adding topology information to the event.

Event Gateway (ncp_g_event)
Network Manager process that performs event enrichment.

Event Gateway stitcher
Stitchers that perform topology lookup as part of the event enrichment process.

failover
In your Network Manager environment, a failover architecture can be used to configure your system for high availability, minimizing the impact of computer or network failure.

Failover plug-in
Receives Network Manager health check events from the Event Gateway and passes these events to the Virtual Domain process, which decides whether or not to initiate failover based on the event.

Fault Finding View
Composite GUI view consisting of an **Active Event List (AEL)** portlet above and a Network Hop View portlet below. Use the Fault Finding View to monitor network events.

full discovery
A discovery run with a large scope, intended to discover all of the network devices that you want to manage. Full discoveries are usually just called discoveries, unless they are being contrasted with partial discoveries. See also, partial discovery.

message broker
Component that manages communication between Network Manager processes. The message broker used byNetwork Manager is called Really Small Message Broker. To ensure correct operation of Network Manager, Really Small Message Broker must be running at all times.

NCIM database
Relational database that stores topology data, as well as administrative data such as data associated with poll policies and definitions, and performance data from devices.

ncp_disco
See, Discovery engine.

ncp_g_event
See, Event Gateway.

ncp_model
See, Topology manager.

ncp_poller
See, Polling engine.

network domain
A collection of network entities to be discovered and managed. A single Network Manager installation can manage multiple network domains.

Network Health View
Composite GUI view consisting of a Network Views portlet above and an **Active Event List (AEL)** portlet below. Use the Network Health View to display events on network devices.

Network Hop View
Network visualization GUI. Use the Network Hop View to search the network for a specific device and display a specified network device. You can also use the Network Hop View as a starting point for network troubleshooting. Formerly known as the Hop View.

Network Polling GUI
Administrator GUI. Enables definition of poll policies and poll definitions.

Network Views
Network visualization GUI that shows hierarchically organized views of a discovered network. Use the Network Views to view the results of a discovery and to troubleshoot network problems.

OQL databases
Network Manager processes store configuration, management and operational information in OQL databases.

OQL language
Version of the Structured Query Language (SQL) that has been designed for use in Network Manager. Network Manager processes create and interact with their databases using OQL.

partial discovery
A subsequent rediscovery of a section of the previously discovered network. The section of the network is usually defined using a discovery scope consisting of either an address range, a single device, or a group of devices. A partial discovery relies on the results of the last full discovery, and can only be run if the Discovery engine, `ncp_disco`, has not been stopped since the last full discovery. See also, full discovery.

Path Views
Network visualization GUI that displays devices and links that make up a network path between two selected devices. Create new path views or change existing path views to help network operators visualize network paths.

performance data
Performance data can be gathered using performance reports. These reports allow you to view any historical performance data that has been collected by the monitoring system for diagnostic purposes.

Polling engine (ncp_poller)
Network Manager process that polls target devices and interfaces. The Polling engine also collects performance data from polled devices.

poll definition
Defines how to poll a network device or interface and further filter the target devices or interfaces.

poll policy
Defines which devices to poll. Also defines other attributes of a poll such as poll frequency.

Probe for Tivoli Netcool/OMNIbus (nco_p_ncpmonitor)
Acquires and processes the events that are generated by Network Manager polls and processes, and forwards these events to the ObjectServer.

RCA plug-in
Based on data in the event and based on the discovered topology, attempts to identify events that are caused by or cause other events using rules coded in RCA stitchers.

RCA stitcher
Stitchers that process a trigger event as it passes through the RCA plug-in.

root-cause analysis (RCA)
The process of determining the root cause of one or more device alerts.

SNMP MIB Browser
GUI that retrieves MIB variable information from network devices to support diagnosis of network problems.

SNMP MIB Grapher
GUI that displays a real-time graph of MIB variables for a device and usse the graph for fault analysis and resolution of network problems.

stitcher
Code used in the following processes: discovery, event enrichment, and root-cause analysis. See also, discovery stitcher, Event Gateway stitcher, and RCA stitcher.

Structure Browser
GUI that enables you to investigate the health of device components in order to isolate faults within a network device.

Topology Manager (ncp_model)
Stores the topology data following a discovery and sends the topology data to the NCIM topology database where it can be queried using SQL.

WebTools
Specialized data retrieval tools that retrieve data from network devices and can be launched from the network visualization GUIs, Network Views and Network Hop View, or by specifying a URL in a web browser.

Notices

This information applies to the PDF documentation set for IBM Tivoli Network Manager IP Edition 3.9.

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

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

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

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

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

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

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
958/NH04
IBM Centre, St Leonards
601 Pacific Hwy
St Leonards, NSW, 2069
Australia
IBM Corporation
896471/H128B
76 Upper Ground
London
SE1 9PZ
United Kingdom
IBM Corporation
JBF1/SOM1 294
Route 100
Somers, NY, 10589-0100
United States of America

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

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

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

COPYRIGHT LICENSE:

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

Trademarks

The terms in Table 15 are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Table 15. IBM trademarks

AIX
ClearQuest
Cognos
Current
DB2
developerWorks
Enterprise Storage Server
IBM
Informix
iSeries
Lotus
Netcool
NetView
Notes
OMEGAMON
PowerVM
PR/SM
pSeries
RDN
SecureWay
solidDB
System z
Tivoli
WebSphere
z/OS
z/VM
zSeries

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

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

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

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Index

Printed in the Republic of Ireland

SC27-2764-04