

Tivoli Management Framework



User's Guide

Version 4.3.1

Tivoli Management Framework



User's Guide

Version 4.3.1

Note

Before using this information and the product it supports, read the information in "Notices," on page 167.

Contents

Preface	vii
Who Should Read This Guide	vii
Prerequisite and related documents	vii
What this guide contains	viii
Accessing publications online	viii
Ordering publications	ix
Accessibility	ix
Contacting software support	ix
Conventions used in this guide	x

Chapter 1. Getting started with the Tivoli environment 1

Setting Tivoli environment variables	1
Setting environment variables for UNIX servers	1
Setting environment variables for Windows servers	2
Starting the Tivoli desktop	2
UNIX systems	2
Windows systems	2
Locating resources using the desktop navigator	3
Creating and populating collections	4
Using regular expressions in searches	4
Working with desktop icons	5

Chapter 2. Managing Tivoli clients 9

Working with Managed Node icons	9
Working with Endpoint icons	10
Moving a Client	11
Desktop, drag and drop	11
Command line	11
Modifying client properties	12
Working with managed node properties	12
Viewing managed node properties	12
Adding an IP interface to a managed node	13
Editing an IP interface of a managed node	14
Removing an IP interface from a managed node	15
Working with endpoint properties	15
Viewing endpoint properties from the endpoint manager	16
Viewing and modifying endpoint properties from a Web browser	17
Modifying Endpoint Properties from the Command Line	21
Viewing gateway properties from a Web browser	21
Starting and stopping endpoints	22
NetWare endpoints	22
Windows endpoints, except Windows 98	22
Windows 98 endpoints	23
UNIX endpoints	23
OS/2 endpoints	23
OS/400 Endpoints	23
Opening a remote terminal session	26
Desktop	26
Command line	26

Toggling a Managed Node icon	27
--	----

Chapter 3. Tivoli administrators 29

Working with Administrator icons	29
Understanding administrator logins	30
Managing multiple logins	31
Accounts and user login maps	32
Accounts created during installation	33
The tmersrvd user account	33
The Tivoli_Admin_Privileges group account	34
Considerations for domain controllers	34
Authentication to the primary domain controller	34
Accounts created on the domain controllers	35
Creating a Tivoli administrator	35
Desktop	35
Command line	40
Managing resources for administrators	40
Desktop	41
Command line	41
Managing administrators	42
Changing administrator properties	42
Changing region roles	43
Desktop	43
Command line	44
Changing resource roles	45
Desktop	45
Command line	46
Changing user account logins	46
Desktop	47
Command line	47
Changing notice group subscriptions	48
Desktop	48
Command line	49
Viewing administrators	49
Desktop	49
Command line	49
Removing an Administrator icon	50
Desktop	50
Command line	50
Viewing removed administrators	51
Restoring a removed administrator	51
Deleting an administrator	51
Desktop	51
Command Line	51

Chapter 4. Tivoli regions and interregion connections 53

Secure Sockets Layer data encryption	53
Enabling SSL communications	53
Setting network security level	54
Setting ciphers for data transfer	55
Replacing certificates and keys	56
Making a secure region connection	56
Desktop	57

Command line	58
Making a remote region connection	59
Desktop	59
Command line	61
Determining the status of region connections	61
Desktop	61
Command line	62
Administrators and remote region resources	62
Desktop	63
Exchanging or updating resource information	63
Desktop, from multiple regions.	64
Desktop, from connection status	65
Command line	65
Forcing an update to override time stamps.	66
Updating all resources.	66
Disconnecting regions	66
Desktop	66
Command line	67

Chapter 5. Policies and policy regions 69

Working with Policy Region icons	69
Creating a top-level policy region	70
Desktop	70
Command line	71
Creating a policy subregion	71
Desktop	71
Command line	71
Changing the name of a policy region	72
Modifying managed resource types in policy regions 72	
Desktop	72
Command line	73
Assigning policies to resources types	73
Desktop	74
Command line	75
Validating resources in policy regions.	75
Desktop	75
Command line	77

Chapter 6. Profiles and profile managers 79

Working with Profile Manager icons	79
Creating a profile manager	79
Desktop	80
Command line	80
Modifying subscribers	80
Adding a subscriber using drag and drop	81
Desktop	81
Command line	83
Editing a profile manager.	83
Desktop	83
Command line	84
Deleting a profile manager	84
Desktop	84
Command line	84
Creating profiles.	84
Desktop	84
Command line	85
Distributing profiles	85
Distributing profiles using drag and drop	85
Desktop	85

Command line	86
Synchronizing profiles with a target	86
Desktop	86
Copying profiles from a profile manager	87
Copying profiles using drag and drop	87
Cloning profiles from a profile manager	87
Desktop	88
Moving profiles between profile managers	88
Deleting profiles from a profile manager.	89
Desktop	89
Command line	90

Chapter 7. Queries and query libraries 91

Working with Query Library icons	91
Working with Query icons	91
Creating a query library	92
Desktop	92
Command line	92
Creating a query.	93
Desktop	93
Command line	96
Editing a query	96
Desktop	96
Command line	97
Running a query	97
Desktop	97
Command line	98

Chapter 8. Notices and notice groups 99

Reading notices	99
Desktop	99
Command line	101
Saving notices	101
Desktop	101
Command line	102
Forwarding notices	102
Desktop	102
Command line	102
Marking notices as read and unread.	103
Sorting notices	103
Filtering notices	104
Combining notices.	105
Displaying old notices	106
Setting notice expiration.	107

Chapter 9. Jobs, tasks, and task libraries 109

Task libraries	109
Working with Task Library icons	110
Creating a task library	110
Using the desktop to create task libraries	110
Using commands to create task libraries	111
Listing contents of a task library	111
Importing and exporting task definitions	111
Controlling task-binary distributions.	111
Tasks	112
Working with Task icons	113
Creating a task	113
Using the desktop to create tasks	113
Using commands to create tasks	115

Running a task	115
Using drag and drop to run tasks	116
Using the desktop to run tasks	116
Using commands to run tasks	118
Saving task output to file	118
Editing a task	118
Using the desktop to edit tasks	119
Using commands to edit tasks	119
Deleting a task	119
Using the desktop to delete tasks	119
Using commands to delete tasks	119
Disabling notices for tasks	119
Jobs	120
Working with Job icons	120
Creating a job	120
Using the desktop to create jobs	120
Using commands to create jobs	122
Running a job	123
Using drag and drop to run jobs	123
Using the desktop to run jobs	123
Using commands to run jobs	123
Saving job output to file.	123
Editing a job	124
Using the desktop to edit jobs	124
Using commands to edit jobs	124
Deleting a job	124
Using the desktop to delete jobs	125
Using commands to delete jobs	125
Task library policies	125
Default policies for task libraries	125
Validation policies for task libraries	126
Task libraries on OS/400 systems.	126
Chapter 10. Scheduling jobs	129
Scheduling a job	129
Using drag and drop to schedule jobs	129
Using the desktop to schedule jobs	130
Using commands to schedule jobs	132
Viewing scheduled jobs	132
Using the desktop to view jobs	132
Using commands to view jobs.	133
Controlling the display of job attributes	133
Sorting jobs	134
Finding jobs.	135
Disabling or enabling scheduled jobs	135

Using the desktop to enable and disable jobs	136
Using commands to enable and disable jobs	136
Editing scheduled jobs	136
Using the desktop to edit jobs.	136
Using commands to edit jobs	136
Deleting scheduled jobs	136
Using the desktop to delete jobs	137
Using commands to delete jobs	137
Using the Scheduler across region boundaries	137
Jobs across region boundaries	137
Specifying job start times among regions	138

Chapter 11. Distribution management 139

Before using a distribution service	139
Creating a repeater	140
Configuring repeaters for MDist	141
Configuring repeaters for MDist 2	143
Setting the depot directory	145
Setting permanent storage	145
Configuring repeaters for multicast	146
Configuring endpoints for multicast.	148
Configuring endpoints to install from file servers	148
Using the Distribution Status console	148
Starting the Distribution Status console.	149
Desktop	150
Command line	151
Viewing distribution status.	152
Desktop	152
Command line	152
Viewing details of a distribution	153
Status Chart view	153
Time Spent Chart view	154
Node Table view	155
Distribution Topology view.	156
Mobile Computing console	158
Configuring the Mobile Computing console	160
Starting the Mobile Computing console.	165

Appendix. Notices 167

Trademarks	168
----------------------	-----

Glossary 171

Index 175

Preface

Tivoli® Management Framework is the base component for Tivoli products. Using Tivoli Management Framework and a combination of Tivoli software, you can manage large distributed networks with multiple operating systems, various network services, diverse system operations, and constantly changing nodes and users.

Tivoli Management Framework provides a set of common services or features that are used by the Tivoli software products installed on Tivoli Management Framework. These services include, but are not limited to, the following set:

- A task library through which you can create tasks and execute the task on multiple Tivoli resources
- A scheduler that enables you to schedule all Tivoli operations including the execution of tasks created in the Tivoli task library
- An RDBMS Interface Module (RIM) that enables some Tivoli products to write application-specific information to relational databases
- A query facility that enables you to search and retrieve information from a relational database

All Tivoli applications installed on Tivoli Management Framework are enabled to use the services provided by Tivoli Management Framework.

This guide describes the concepts and procedures for using Tivoli Management Framework services. It provides instructions for performing operations from the Tivoli desktop and from the command line.

Who Should Read This Guide

This guide is intended for use by system administrators who use Tivoli Management Framework to perform daily system management operations. Users of this guide should have a working knowledge of the following:

- The UNIX® or Microsoft® Windows® operating system
- Shell programming
- The Motif or Windows environment

Prerequisite and related documents

Tivoli provides the following related documentation:

- *Tivoli Management Framework Planning for Deployment Guide*
Explains how to plan for deploying your Tivoli environment. It also describes Tivoli Management Framework and its services.
- *Tivoli Enterprise Installation Guide*
Explains how to install and upgrade Tivoli Enterprise software within your Tivoli region using the available installation mechanisms provided by Tivoli Software Installation Service and Tivoli Management Framework. Tivoli Enterprise software includes the Tivoli server, managed nodes, gateways, endpoints, and RDBMS Interface Module (RIM) objects. This guide also provides information about troubleshooting installation problems.
- *Tivoli Management Framework Reference Manual*

Provides in-depth information about Tivoli Management Framework commands. This manual is helpful when writing scripts that are later run as Tivoli tasks. This manual also documents default and validation policy scripts used by Tivoli Management Framework.

- *Tivoli Management Framework Maintenance and Troubleshooting Guide*

Explains how to maintain a Tivoli environment and troubleshoot problems that can arise during normal operations.

References to the interpreter type for a particular client are located throughout this guide. *Interpreter type* is an internal classification used by Tivoli Management Framework to delineate operating systems, platform, or machine type. Interpreter types for each machine type are located in the *Tivoli Management Framework Release Notes*

What this guide contains

The *Tivoli Management Framework User's Guide* contains the following sections:

- Chapter 1, "Getting started with the Tivoli environment," on page 1
Explains the graphical user interface (GUI), including the window controls and icons when using Tivoli Management Framework
- Chapter 2, "Managing Tivoli clients," on page 9
Discusses Tivoli clients and how to view their properties
- Chapter 3, "Tivoli administrators," on page 29
Discusses Tivoli administrators and delegation of Tivoli authority
- Chapter 4, "Tivoli regions and interregion connections," on page 53
Discusses Tivoli management regions, the connection of regions, and exchanging information between connected regions
- Chapter 5, "Policies and policy regions," on page 69
Discusses policy, policy resources, and policy regions
- Chapter 6, "Profiles and profile managers," on page 79
Discusses Tivoli profiles, profile managers, and profile manager operations
- Chapter 7, "Queries and query libraries," on page 91
Discusses query libraries and queries
- Chapter 8, "Notices and notice groups," on page 99
Discusses Tivoli notices and notice groups
- Chapter 9, "Jobs, tasks, and task libraries," on page 109
Discusses jobs and tasks
- Chapter 10, "Scheduling jobs," on page 129
Discusses scheduling jobs
- Chapter 11, "Distribution management," on page 139
Discusses how to create and configure repeaters. It also explains how to use the consoles, available only to Tivoli products using the MDist 2 service.

Accessing publications online

The documentation CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli software information center

Web site. Access the Tivoli software information center by first going to the Tivoli software library at the following Web address:

<http://publib.boulder.ibm.com/tividd/td/tdprodlist.html>

Note: If you print PDF documents on other than letter-sized paper, set the option in the **File → Print** window that allows Adobe Reader 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.ibm.link.ibm.com>

From this Web page, select **Publications** and follow the instructions.

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, see the following Web site for a list of telephone numbers:

<http://www.ibm.com/software/tivoli/order-lit>

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Contacting software support

If you have a problem with any Tivoli product, refer to the following IBM Software Support Web site:

<http://www.ibm.com/software/sysmgmt/products/support/>

If you want to contact software support, see the *IBM Software Support Guide* at the following Web site:

<http://techsupport.services.ibm.com/guides/handbook.html>

The guide provides information about how to contact IBM Software Support, depending on the severity of your problem, and the following information:

- Registration and eligibility
- Telephone numbers, depending on the country in which you are located
- Information you must have before contacting IBM Software Support

Conventions used in this guide

This guide uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text
- Interface controls
- Keywords and parameters in text

Italic

- Words defined in text
- Emphasis of words (words as words)
- New terms in text (except in a definition list)
- Variables and values you must provide

Monospace

- Examples and code examples
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

This guide uses the UNIX convention for specifying environment variables and for directory notation:

- When using the Windows command line, replace *\$variable* with *%variable%* for environment variables and replace each forward slash (/) with a backslash (\) in directory paths.
- When using the bash shell on Windows operating systems, use the UNIX conventions.

Chapter 1. Getting started with the Tivoli environment

The Tivoli desktop is a user interface that provides point-and-click access to Tivoli Management Framework features and components. The Tivoli desktop provides a central control point for you to organize, manage, and delegate system management operations.

Tivoli Management Framework also provides a command line interface (CLI) that enables you to enter commands from the keyboard. You can use these commands in shell scripts and with system utilities such as the UNIX cron utility. Tivoli Management Framework commands perform functions similar to the Tivoli desktop operations. For more information about using commands, refer to the *Tivoli Management Framework Reference Manual*.

Setting Tivoli environment variables

Before you can use the Tivoli desktop or commands, you must set up the Tivoli environment variables. You can manually run one of the scripts provided by Tivoli Management Framework or modify your initialization environment (UNIX operating systems only).

Setting environment variables for UNIX servers

For UNIX operating systems, the installation process creates the following setup scripts:

`/etc/Tivoli/setup_env.csh`

`/etc/Tivoli/setup_env.sh`

To set the Tivoli variables on a UNIX operating system, perform the following steps:

1. Log in to a UNIX Tivoli server or managed node either locally or using telnet.
2. For the Bourne (sh) or Korn (ksh) shells, enter the following command:

`. /etc/Tivoli/setup_env.sh`

For the C (csh) shell, enter the following command:

`source /etc/Tivoli/setup_env.csh`

Optionally, you can change your login initialization procedure to use the appropriate setup file so that the necessary environment variables and search paths are automatically set when you log in to the Tivoli server or managed node.

For example, you can add the following to your initialization procedure:

For sh or ksh shells:

```
if [ -f /etc/Tivoli/setup_env.sh ]; then
. /etc/Tivoli/setup_env.sh
fi
```

For the csh shell:

```
if ( -f /etc/Tivoli/setup_env.csh ) then
source /etc/Tivoli/setup_env.csh
endif
```

Setting environment variables for Windows servers

For Windows operating systems, the installation process creates the following setup scripts:

- %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.cmd
- %SystemRoot%\system32\drivers\etc\Tivoli\setup_env.sh

To set the Tivoli variables on a Windows operating system, perform the following steps:

1. Log in to a Windows Tivoli server or managed node.
2. From a DOS command prompt, enter:

```
%SystemRoot%\system32\drivers\etc\Tivoli\setup_env  
bash
```

The **bash** command starts the bash shell, which is a variation of the Bourne shell.

Starting the Tivoli desktop

Before starting the Tivoli desktop, ensure that the system that you want to connect to accepts remote connections. To determine whether a system accepts remote connections, follow the procedure for enabling and disabling remote connections in the *Tivoli Enterprise Installation Guide*.

UNIX systems

To launch the Tivoli desktop on UNIX systems, perform the following steps:

1. Set your DISPLAY environment variable.
2. Initialize the Tivoli environment variables as described in “Setting Tivoli environment variables” on page 1.
3. Run the **tivoli** command.

For additional information about the **tivoli** command, refer to the *Tivoli Management Framework Reference Manual*

Windows systems

Use the following procedure to start the Tivoli desktop:

1. For Windows operating systems—From the **Start** menu, select **Programs → Tivoli → Tivoli**.

For OS/2[®] operating systems—After adding the icons to your OS/2 desktop, click the **Tivoli (Windows)** icon.

The Tivoli Management Environment window is displayed.

2. In this window, perform the following steps:
 - a. In the **Host Machine** field, type the fully qualified host name of the managed node or type the host name of the Tivoli server. Do not type the IP address.
 - b. In the **Log In As** field, type your domain-qualified user name (Windows) or the account name (UNIX) for the managed node. This field is case sensitive.
 - c. In the **Password** field, type the password for the specified user or account. This field is case sensitive.

Note: Ensure that there are no extra spaces in this field.

- d. Click **OK**.

For more information about logging in to the Tivoli desktop on Windows operating systems, see the chapter about the Tivoli Desktop for Windows in the *Tivoli Enterprise Installation Guide*.

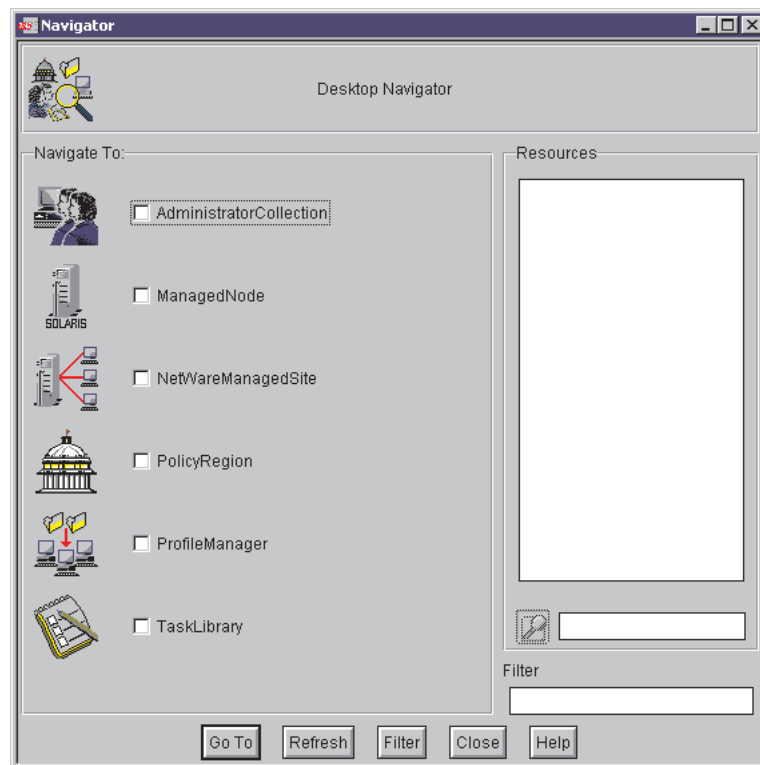
Locating resources using the desktop navigator

The Desktop Navigator window provides an easy way to move through the hierarchical structure of Tivoli Management Framework. Using the navigator from the Tivoli desktop, you can go directly to a selected resource or to the resource containing the selected resource without going through intermediate resources. You can access the navigator from any collection window, such as the Tivoli desktop, a policy region window, or a task library window.

For example, if you want to look at a particular task library without the navigator, you must open the correct policy region window and then open the correct task library window. Using the navigator, you can choose from a list of all the task libraries in the name registry of the local Tivoli region. When you double-click the task library name, the correct task library window opens.

To open the navigator to work with resource, perform the following steps:

1. From the Tivoli desktop, select **Navigator** from the **Desktop** menu. The Desktop Navigator window is displayed:



2. Select a resource type in the **Navigate To** list to show all resource of that type in the **Resource** list. The contents of the **Navigate To** list vary depending on the resources created and applications installed in the Tivoli environment. When you select a resource type from the **Navigate To** list, the **Resource** scrolling list is refreshed with the names of each instance of the resource type you selected.

3. To limit the contents of the **Resource** list, use the **Filter** text box. To filter the contents of the list, enter a regular expression in the **Filter** text box and click **Filter**. Refer to “Using regular expressions in searches” for more information.
4. After selecting a resource from the **Resource** list, click **Go To** to open the resource-specific window.

Creating and populating collections

As you become familiar with the Tivoli desktop, you might want to define shortcuts to frequently accessed resources. For example, for authorization or policy reasons, there might be several resources in different policy regions that you would prefer to access through a single window. This can be either on the Tivoli desktop, or if you have several icons, you can organize them with a collection.

A *collection* is a container that you create and place on the Tivoli desktop. You populate a collection through drag-and-drop operations. You can then open the collection to view the resources it contains. The contents of a collection are referred to as its *members*. The icons in a collection are a *link* to the original resource, not a duplicate of the resource. You can create collections from the Tivoli desktop only.

To create a collection, perform the following steps:

1. From the Tivoli desktop, select **Collection** from the **Create** menu to display the Create Collection window.



2. In the **Collection Name** text box, type a name that describes the collection. For example, if you are going to keep a number of icons representing server machines in the collection, you might name the collection **Servers**.
3. Click **Create & Close** to create the new collection and close the window.

To populate the collection, open one or more windows and use drag-and-drop operations to copy the icons representing the resources into the collection. Any action you perform on a resource contained in the collection updates the actual resource.

Using regular expressions in searches

A regular expression is a search string used for pattern matching in the Tivoli object database. A regular expression uses alphanumeric and special characters to specify a pattern.

The following table lists the special characters you can use to construct regular expressions.

Character	Operation
^	Matches lines that begin with the expression
\$	Matches lines that end with the expression

Character	Operation
.	Matches a single character
*	Matches zero or more characters
[Rr]	Matches any one character in brackets
[c-z]	Matches any character in the sequence
[^c-z]	Matches characters not in the sequence
\	Matches any character by disabling special meaning

For example, NoonTide Enterprises has the following systems in its corporate network:



balder	blue	frey
gate-1	green	loki
odin	orange	rainbow
red	thor	violet
yellow		











The following table shows the results of several regular expression searches of the NoonTide host file.







Regular expression	Search results
^b	Returns system names that begin with the letter “b”: balder and blue
e\$	Returns system names that end with the letter “e”: blue and orange
.n	Return systems name that contain the letter “n”: green, odin, orange, and rainbow
[dk]	Returns system names containing the letter “d” or “k”: balder, loki, odin, and red
[o-s]	Returns system names containing the letters “o” through “s”: balder, frey, green, loki, odin, orange, rainbow, red, thor, violet, and yellow
[^o-s]	Returns system names containing any letter <i>except</i> the letters “o” through “s”: blue and gate-1

Working with desktop icons

Following are icons that can appear on a Tivoli desktop.

	The Administrator icon. One icon is displayed for each administrator in the policy region. Right-click this icon to open its pop-up menu.
	The Administrators icon. The Administrators icon represents a collection that contains icons for all administrators defined in the Tivoli environment. Double-click the icon to open the Administrators window, or right-click this icon to open its pop-up menu.

	The Bulletin Board icon with no messages. This icon indicates no messages are waiting to be read. Double-click the icon to open the Read Resources window, or right-click this icon to open its pop-up menu.
	The Bulletin Board icon with messages. Double-click the icon to open the Read Resources window, or right-click this icon to open its pop-up menu.
	The Collection icon. Double-click this icon to open collection window where you can view the members of the collection, or right-click this icon to open its pop-up menu.
	The Database Profile Manager icon. One icon is displayed for each database profile manager in the policy region. A database profile manager can distribute to any profile manager (database or dataless) and all managed nodes—but not to endpoints. Double-click this icon to open the Profile Manager window where you can view the profiles contained in the profile manager, or right-click the icon to view its pop-up menu.
	The Dataless Profile Manager icon. One icon is displayed for each dataless profile manager in the policy region. A dataless profile manager can distribute to any managed nodes and endpoints—but not to profile managers. Double-click this icon to open the Profile Manager window where you can view the profiles contained in the profile manager, or right-click this icon to open its pop-up menu.
	The Endpoint icon. One icon is displayed for each endpoint.
	The Endpoint Manager icon. Double-click this icon to open the Gateway List window where you can view a list of gateways in the Tivoli region, or right-click this icon to open its pop-up menu.
	The Job icon. One icon is displayed for each job in a task library. Double-click this icon to run the job, or right click this icon to view its pop-up menu. You can also drag and drop this icon onto the Scheduler icon to schedule the job to run later.
	The Managed Node icon. One icon is displayed for each computer system on which Tivoli Management Framework is installed. Double-click this icon to open the manage node window, or right-click this icon to open its pop-up menu.
	The Policy Region icon. One icon is displayed for each policy region you create. Double-click the icon to open the Policy Region window, or right-click this icon to open its pop-up menu.

	The Query icon. Double-click this icon to edit a defined query, or right-click this icon to run the query.
	The Query Library icon. Double-click this icon to create new queries.
	The Scheduler icon. Double-click this icon to schedule a job, or right-click this icon to open its pop-up menu. You can also drag and drop a job icon onto the Scheduler icon.
	The Task icon. One icon is displayed for each task in a task library. Double-click the icon to specify the run options and then run the task, or right-click this icon to open its pop-up menu.
	The Task Library icon. One icon is displayed for each task library in the policy region. Double-click this icon to open the Task Library window where you can view the jobs and tasks contained in a task library, or right-click this icon to open its pop-up menu.
	The Unknown icon. This icon appears in a window anytime the resource that it represents is an unknown type or cannot be contacted. This most commonly occurs when the connection between two Tivoli regions is down or unavailable.

Chapter 2. Managing Tivoli clients

A Tivoli environment can include the following types of clients:

- Managed nodes
- Endpoints

A *managed node* runs the full Tivoli Management Framework software and can perform the same security and communication functions performed by the Tivoli server. The Tivoli server is the machine from which system administrators manage other systems in the network. A managed node maintains a client database, which is significantly smaller than the object database on the Tivoli server. A managed node can also be a proxy system for a gateway.

An *endpoint* is the most common type of machine in most Tivoli Management Framework installations. This machine is not used to perform day-to-day management operations. Instead, it is one of the many machines a system administrator must manage, usually from a managed node. An endpoint runs a very small amount of Tivoli software and does not maintain a database.

The Tivoli desktop is not installed with the endpoint software. If you choose to run the Tivoli desktop on an endpoint, you must install Tivoli Desktop for Windows. The Tivoli desktop provides access to the managed node or Tivoli server that manages the endpoint, which enables you to gather information about the endpoint.

Each client is a managed resource and represents a single machine in the Tivoli region. One icon is displayed in a Policy Region window for each managed node in the Tivoli region. By default, Endpoint icons are not added to a policy region or displayed on the Tivoli desktop. You can move them to a policy region by adding them as a valid resource in the region and using the **wmv** command to move the endpoint to the region, or use an **after_install_policy** script to perform these operations.

As with other managed resources, you can move a client from one policy region to another by moving the client icon from one Policy Region window to another. However, you cannot copy a client to other policy regions. Any changes made to a client updates the local system only; the changes cannot be applied to other managed nodes.

Working with Managed Node icons

Managed Node icons represent machines running a supported version of UNIX or Windows operating systems.

The following is the icon for a managed node:



Managed Node icons have two representations, server or client. You can toggle the icon depending on the role the managed node serves in your organization. The icons have identical functionality, and changing the representation of the icon has no affect on Tivoli Management Framework operations.

Figure 1 shows examples of the Managed Node icon when represented as servers:



Figure 1. Managed Node icon when represented as servers

Figure 2 shows examples of the Managed Node icon when represented as clients:



Figure 2. Managed Node icons when represented as clients

The pop-up menu of the Managed Node icon includes the following options:

Open Opens the Managed Node window and shows any relevant contents (such as profiles that have been distributed to the managed node).

Properties

Displays physical information about the machine configuration and allows you to change the IP interfaces for the managed node.

Run xterm

Opens an Xterminal (xterm) session on the machine. This option is not valid on Windows managed node. If you select this option on a Windows managed node, an error message is displayed.

Toggle Icon

Toggles the managed node icon between the client representation and server representation. See “Toggling a Managed Node icon” on page 27 for more information about toggling icon representations.

Synchronize

Allows you to synchronize the information stored in one or more profiles with the corresponding data in system files. See Chapter 6, “Profiles and profile managers,” on page 79 for more information about synchronizing profiles.

Working with Endpoint icons

An endpoint is a Tivoli resource that can be created on UNIX or PC operating systems, including NetWare and OS/2. Endpoints communicate with gateways.

The following icon represents an endpoint client:



One of these icons is created each time you install an endpoint. The Endpoint icons are not displayed in the Policy Region window unless you add them to the policy region using the **wmv** command or use an **after_install_policy** script. Endpoint icons always display in the subscriber section of the Profile Manager window.

The Endpoint icon does not have a pop-up menu. To view the properties of an endpoint, use the Endpoint Manager icon. Refer to “Working with endpoint properties” on page 15 for instructions.

Moving a Client

As with other resources in a policy region, you can move clients from one policy region to another, either to reflect changes in your organization or to redistribute resource management responsibilities among administrators. When you move clients, the default and validation policies for the client change to that of the new policy region. However, any subscriptions that the client has remain intact and uses the default and validation policies of their respective policy regions. Refer to Chapter 6, “Profiles and profile managers,” on page 79 for more information about subscriptions.

The move operation deletes the client from one policy region and creates it in another. For example, if you have permission to delete clients from the original policy region but do not have permission to create clients in the target policy region, the client remains in the original policy region.

The following table provides the contexts and authorization roles required for these operations:

Activity	Context	Required Role
Delete a client from a policy region	Policy region	senior
Create a client in a policy region	Policy region	senior
Note: You also need the senior Tivoli region role to complete this operation.		

You can move a client from one policy region to another using either the Tivoli desktop or the command line.

Desktop, drag and drop

To move a client from one policy region to another, perform the following steps:

1. Select the icon of the client that you want to move.
2. Press and hold the Shift key.
3. Click the left mouse button, and drag the icon into a policy region or over a Policy Region icon.
4. Release the mouse button and the Shift key. The client is cut from the original policy region and pasted in the destination region.

Command line

For information about using the command line to move any resource, including managed nodes and endpoints, from one policy region to another, refer to the **wmv** command in the *Tivoli Management Framework Reference Manual*.

Modifying client properties

Each client has a set of associated properties, which you can view from a window. The information varies by machine type and client type. Generally, this information includes machine name, operating system, and IP addresses.

Working with managed node properties

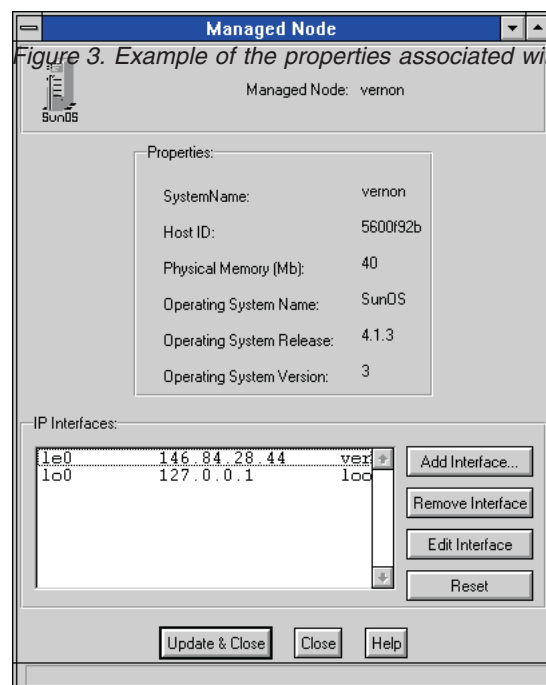
You can view and manage the properties associated with a managed node.

Viewing managed node properties

You can view the properties on a managed node from the Tivoli desktop or using the command line.

Desktop: To view the properties of managed node, right-click the Managed Node icon and select **Properties** to open the Managed Node window.

Figure 3 shows an example of the Managed Node window for managed node vernon:



The **Properties** list displays information about the managed node, including the system name and host ID, memory size, and operating system name, release, and version. You cannot edit these fields.

The **IP Interfaces** scrolling list displays all interfaces on the managed node. In the preceding example, there are two IP interface entries for managed node vernon:

- vernon.ibm.com
- localhost

In this example, the system name and primary (or loopback) IP interface name are the same, vernon. On your system, the names might be different.

From this window, you can add, edit, or remove entries. However, you cannot edit or remove the primary IP or loop (loopback or local host) addresses with this window. If you attempt to edit or remove the primary IP interface, you receive an error message.

Note: You can edit the primary IP address for the local system with the **wifconfig** command only. For more information about this command, see the *Tivoli Management Framework Reference Manual*.

Command Line: To view managed node properties from the command line, use the **whostid**, **wmannode**, **wmemsize**, and **wuname** commands. For information about these command, see the *Tivoli Management Framework Reference Manual*.

Adding an IP interface to a managed node

If the managed node can be contacted by multiple IP addresses, you might need to add IP interfaces for a managed node. You can add IP addresses from either the Tivoli desktop or command line.

The following table provides the context and authorization role required for this operation:

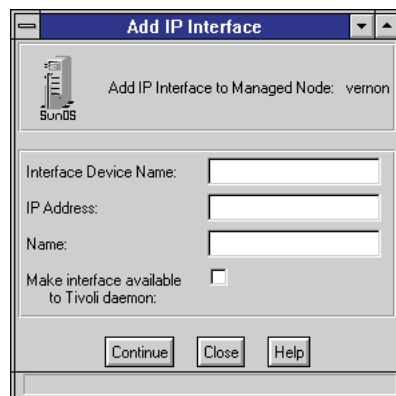
Activity	Context	Required Role
Adding an IP interface	Managed node	admin

Note: If the machine has already had the IP interface added through some means external to Tivoli Management Framework, see the *Tivoli Management Framework Maintenance and Troubleshooting Guide* for information about how to inform the Tivoli software of this change.

You can add an IP interface for a managed node from either the Tivoli desktop or the command line.

Desktop: To add an IP interface for a managed node, perform these steps:

1. In the Tivoli desktop, right-click the Managed Node icon and select **Properties** to display the Managed Node window.
2. Click **Add Interface** to display the Add IP Interface window:



3. In the **Interface Device Name** text box, type the device name. The device name is how the operating system knows this interface device.
4. In the **IP Address** text box, type the IP interface. The address must be in four-part dotted notation. For example, 146.84.28.44 is a valid IP address.

5. In the **Name** text box, type the name of the IP interface. The name is how you would like to expose the device; for example, a fully-qualified host name.
6. Select **Make interface available to Tivoli daemon** if you want to notify the Tivoli software of the new IP address as a communication channel.
7. Click **Continue** to add the IP interface and return to the Managed Node window.
8. Click **Update & Close** to save the changes and close the window.

Command Line: For information about using the **wifconfig** command to add an IP interface for a managed node, see the *Tivoli Management Framework Reference Manual*.

Editing an IP interface of a managed node

When you edit an IP interface, you can change the IP address or interface name but not the interface device name. You cannot edit the primary IP interface or loop (loopback or local host) IP interface from the Tivoli desktop. You can edit these IP interfaces from the command line only. If you attempt to edit one of these IP interfaces from the Tivoli desktop, you will receive an error message.

The following table provides the context and authorization role required for this operation:

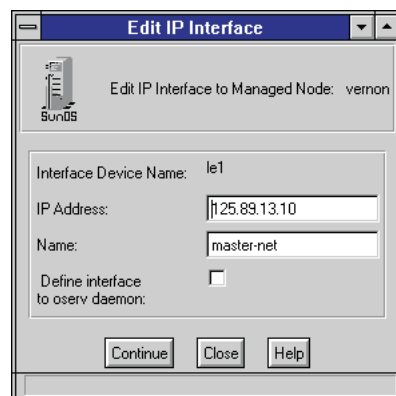
Activity	Context	Required Role
Editing an IP address or interface name	Managed node	admin

Note: If the machine has already had the IP interface changed through some means external to Tivoli Management Framework, refer to the *Tivoli Management Framework Maintenance and Troubleshooting Guide* for information about how to inform the Tivoli software of this change.

You can edit an IP interface for a managed node from either the Tivoli desktop or the command line.

Desktop: To edit an IP interface of a managed node, perform the following steps:

1. In the Tivoli desktop, right-click the Managed Node icon and select **Properties** to display the Managed Node window.
2. Select an entry in the **IP Interfaces** scrolling list and click **Edit Interface**. The Edit IP Interface window is displayed:



3. To change the IP address, type the new IP address in the **IP Address** text box. The address must be in four-part dotted notation. For example, 125.89.13.10 is a valid IP address.
4. To change the IP interface name, type the new name in the **Name** text box.
5. Select **Define interface to oserv daemon** if you want to notify the Tivoli software of the existence of the new IP address as a communication channel.
6. Click **Continue** to update the IP interface and return to the Managed Node window.
7. Click **Update & Close** to save the changes and close the window.

Command Line: For information about using the **wifconfig** command to edit an IP interface on a managed node, refer to the *Tivoli Management Framework Reference Manual*.

Removing an IP interface from a managed node

You can remove an IP interface for a managed node when the IP interface is no longer needed by the managed node. However, you cannot remove the primary IP address or loop interface. If you attempt to remove one of these IP interfaces, you will receive an error.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required Role
Removing an IP interface	Managed node	admin

Note: If the machine has already had the IP interface removed through some means external to Tivoli Management Framework, refer to the *Tivoli Management Framework Maintenance and Troubleshooting Guide* for information about how to inform Tivoli Management Framework of this change.

You can remove an IP interface for a managed node from either the Tivoli desktop or command line.

Desktop: To remove entries from the IP interface list of a managed node, perform the following steps:

1. In the Tivoli desktop, right-click the Managed Node icon and select **Properties** to display the Managed Node window.
2. From the list of interfaces in the **IP Interfaces** scrolling list, choose one or more entries.
3. Click **Remove Interface** to remove the selected IP interfaces.
4. Click **Update & Close** to save the changes and close the window.

Command Line: For information removing an IP address from a managed node from the command line, refer to the **wifconfig** command in the *Tivoli Management Framework Reference Manual*.

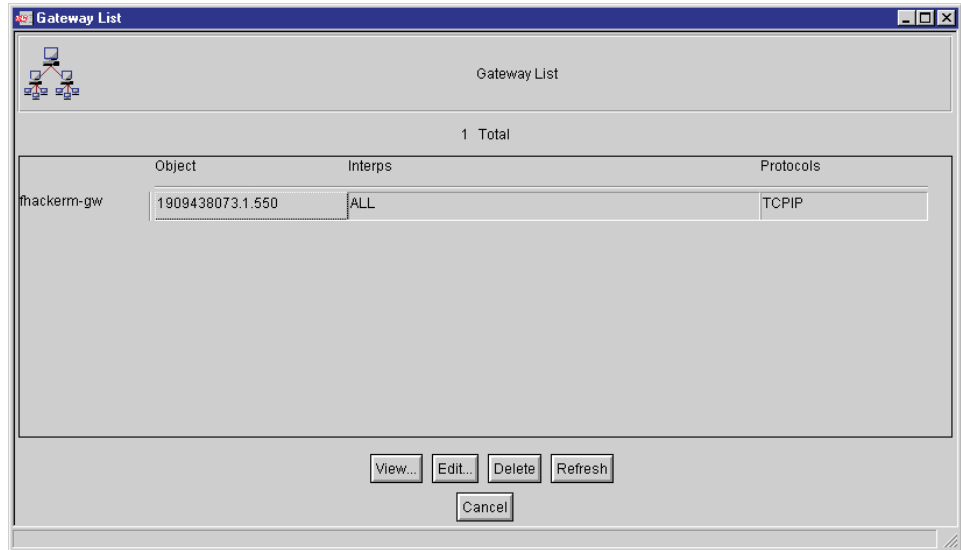
Working with endpoint properties

You can view endpoint properties from either the Tivoli desktop or a Web browser, but you cannot change endpoint properties from the Tivoli desktop. To change endpoint properties, you must use the appropriate **lcf** command from the command line or through the **Additional configuration options** link on the Endpoint Web page.

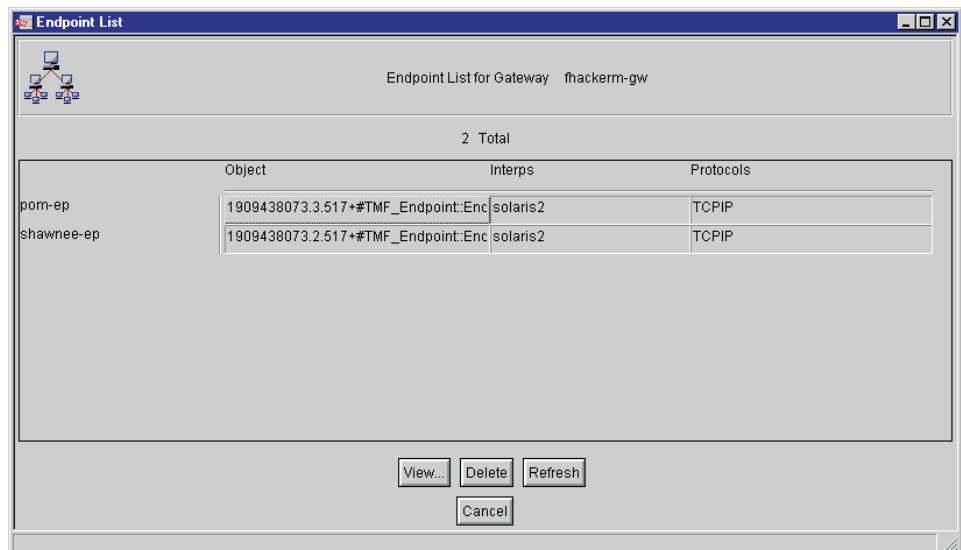
Viewing endpoint properties from the endpoint manager

To view endpoint properties from the Endpoint Manager icon, perform the following steps:

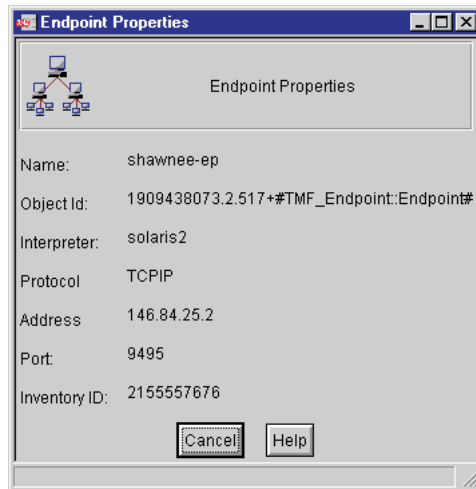
1. In the Tivoli desktop, double-click the Endpoint Manager icon to open the Gateway List window:



2. Double-click the gateway to which the endpoint is assigned or select a gateway from the list and click **View** to open the Endpoint List window:



3. Double-click the appropriate endpoint or select the endpoint from the list and click **View** to open the Endpoint Properties window:



4. Click **Cancel** to close the window.

Viewing and modifying endpoint properties from a Web browser

You can view endpoint properties from a Web browser, and you can view a wide variety of endpoint information from the browser, including message files and configuration information. To view endpoint information from a Web browser, enter the following URL:

`http://host_name:port_number`

where:

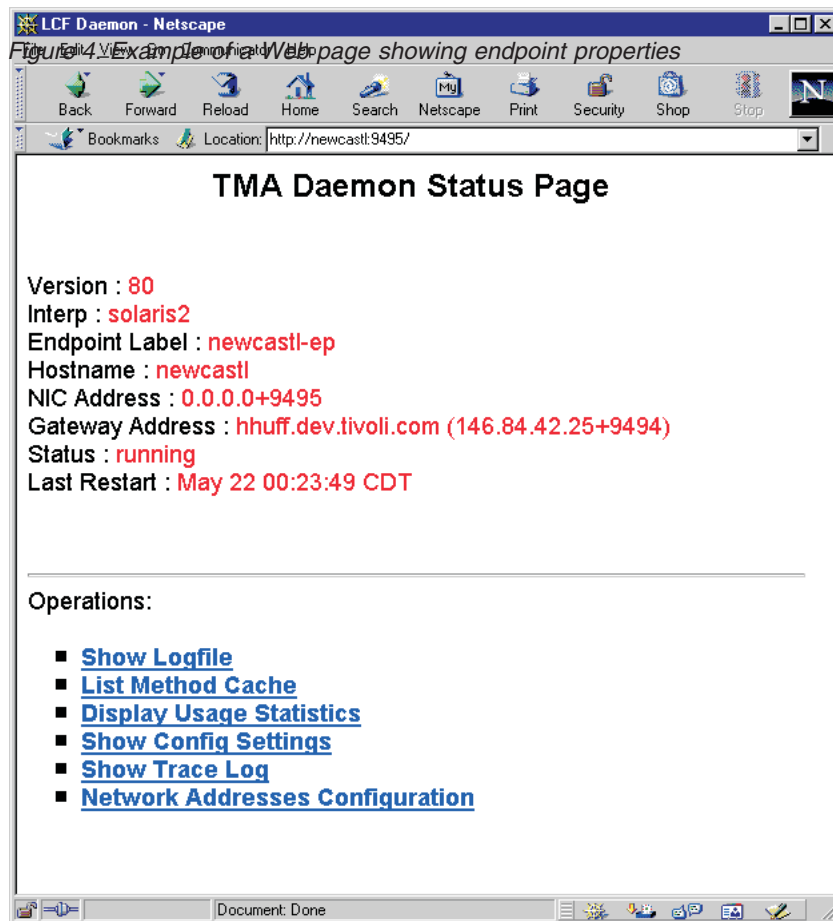
host_name

Specifies the name of the endpoint

port_number

Specifies the port number that the endpoint is using

Figure 4 shows an example Web page for an endpoint:



The top half of the page displays basic endpoint information and status:

Version

Shows the endpoint software version number.

Interp Shows the internal representation of the operating system, or interpreter type.

Endpoint Label

Shows the label for the endpoint

Hostname

Shows the host name of the computer system hosting the endpoint.

NIC Address

Shows the IP address and listening port of the endpoint.

Gateway Address

Shows the IP address and port number of the assigned gateway.

Status Shows the current login status of the endpoint. The possible status of an endpoint are as follows:

initializing

The endpoint is starting.

logging in

The endpoint is logging in to its assigned gateway.

login failed

The endpoint login process failed. Look for errors in the `lcfld.log` file. When you have corrected the problem, restart the endpoint.

running

The endpoint is running.

broadcasting

The endpoint is attempting to log in by broadcasting a login packet.

For more information about endpoint login processes, see the *Tivoli Management Framework Planning for Deployment Guide*.

Last Restart

Provides the date and time that the endpoint was last started.

The bottom half of the Web page includes the following links. With the exception of the **Network Addresses Configuration** link, you cannot edit any of this information displayed through the Web browser.

Show Logfile

Displays the contents of the `lcfld.log` file.

List Method Cache

Displays a list of the methods or dependencies contained in the method cache.

Display Usage Statistics

Displays the following information:

Cache Size

Current size of the method cache.

Cache Hits

Number of times the method cache was checked and the method was found.

Cache Misses

Number of times the cache did not contain the requested method.

Downcall Hits

Number of times an endpoint method was successfully launched.

Downcall Misses

Number of times an endpoint method was not successfully launched.

http Requests

Number of times endpoint files were viewed through the Web.

Up Time

How long the endpoint has been running since the last restart.

Show Config Settings

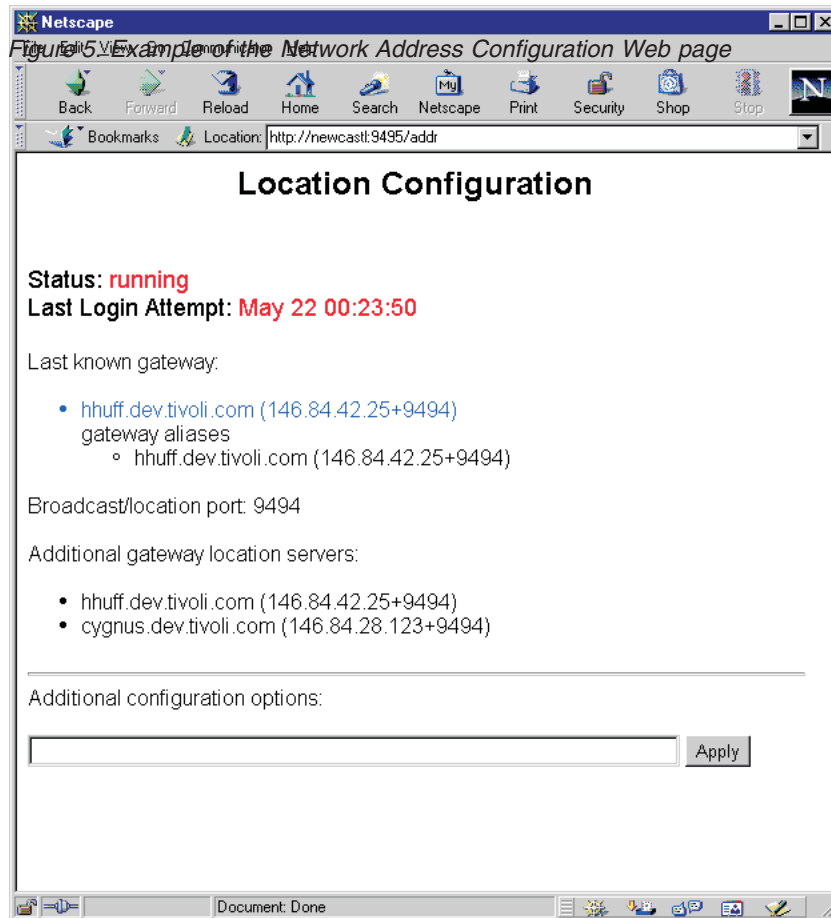
Displays the configuration information contained in the `lcfld.cfg` file.

Show Trace Log

Displays the method trace messages. The trace log is for debugging purposes only.

Network Addresses Configuration

Displays configuration information for the assigned gateway for the endpoint. Figure 5 shown is an example of the Location Configuration Web page:

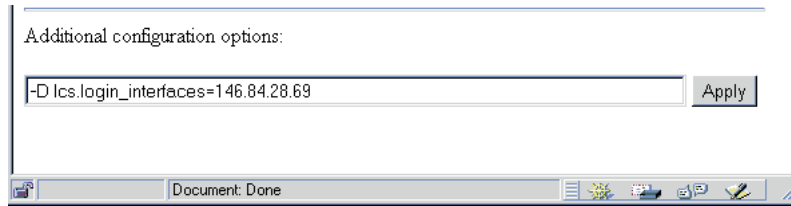


At the bottom of the Location Configuration Web page is the **Additional configuration options** text box. Using this text box, you can specify **lcmd** command options to change the endpoint startup files.

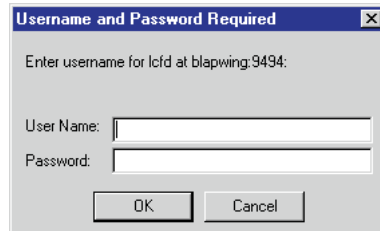
Although many **lcmd** command options require a manual restart of the endpoint daemon, you can reset the amount and type of debug messages written to the **lcmd.log** file (using the **-d** option of the **lcmd** command) without restarting the endpoint daemon.

Another use of the Web browser is for reassigning isolated endpoints. An endpoint is considered isolated when it attempts to communicate with its assigned gateway, but finds the gateway unreachable. To request an endpoint to contact a different gateway, perform the following steps:

1. In the **Additional configuration options** text box, type the IP address or IP address and port number of the gateway that the endpoint should contact.



2. Click **Apply** to access the Username and Password Required window.



3. Type the user name and password assigned to the endpoint.

Note: Each endpoint has a unique user name and password. The name and password are required only to change the endpoint configuration. When an endpoint is installed, the default user name is *tivoli* and the password is *boss*. When the endpoint successfully logs in to its assigned gateway, a new password is randomly generated. Use the **wep** command to retrieve the user name and password for an endpoint. For information about the **wep** command, see the *Tivoli Management Framework Reference Manual*.

4. Click **OK** to implement the configuration changes you made. In this example, the specified interface is added to the list used by the endpoint to search for a gateway.

Modifying Endpoint Properties from the Command Line

If an endpoint is connected to a gateway that supports IPX, you can stop and restart the endpoint to allow it to communicate to the same gateway in a different protocol.

If your endpoint uses TCP/IP to connect to the gateway, to restart the endpoint in IPX you need to stop it and then restart it with the following command:

```
lcfid -x IPX -g IPX_address+port
```

where *IPX_address* is the IPX address for the gateway of your previous connection.

If your endpoint uses IPX to connect to the gateway, to restart the endpoint in TCP/IP you need to stop it and then restart it with the following command:

```
lcfid -x TCP/IP -g IP_address+port
```

where *IP_address* is the TCP/IP address for the gateway of your previous connection.

Viewing gateway properties from a Web browser

To view this gateway information, enter the following URL in the **Location** text box:

```
http://host_name:port_number
```

where:

host_name

Specifies the name of the gateway

port_number

Specifies the port number that the gateway is using

From this Web page, you can accomplish a variety of operations that include the following:

- Viewing endpoints assigned to the gateway
- Viewing endpoint status
- Rescuing endpoints
- Finding endpoints by name
- Choosing the communication protocol for an endpoint
- Viewing gateways

Note: When a gateway is created, the HTTPd service is disabled by default. To access gateway information from a browser, you need to use the **wgateway** command to define the access account and password and enable the gateway to accept http requests. For information about enabling and disabling http requests and for information about setting the access account, refer to the **wgateway** command in the *Tivoli Management Framework Reference Manual*.

Starting and stopping endpoints

When the endpoint is installed, it automatically logs in to a gateway. Occasionally, you might need to manually stop or restart an endpoint. The manual procedure depends on the operating system on which the endpoint is running.

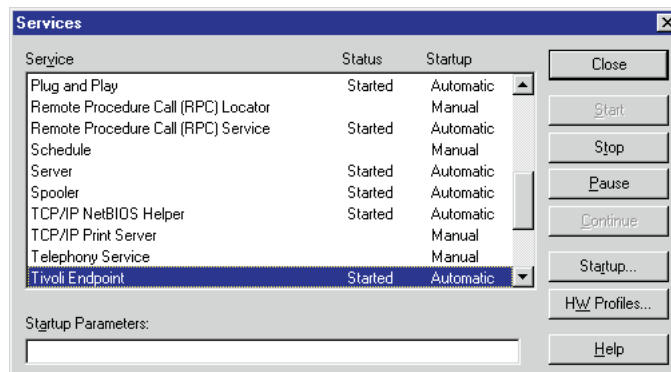
NetWare endpoints

Start and stop a NetWare endpoint from the NetWare Console. To start an endpoint, enter the **lcf** command. To stop an endpoint, enter the **lcfstop** command.

Windows endpoints, except Windows 98

You can start and stop an endpoint from the Services window (available through the Control Panel) or from a command prompt.

From the Services panel, select the Tivoli Endpoint from the Service list and click **Start** or **Stop**.



From a command prompt , use the **net start lcf** or **net stop lcf** command.

Windows 98 endpoints

If installed, double-click the Endpoint icon in the Tivoli program group to start an endpoint.



Use the `-r` option of the `lcfid` command to stop the endpoint.

UNIX endpoints

Use the `lcfid.sh start` or `lcfid.sh stop` commands to start or stop UNIX endpoints.

OS/2 endpoints

Use the `lcfid start` command to start OS/2 endpoints or the `lcfid stop` command to stop OS/2 endpoints.

OS/400 Endpoints

Use the `STRTMEEPT` and `ENDTMEEPT` command to start and stop OS/400 endpoints.

Starting OS/400 Endpoints: The `STRTMEEPT` command starts the endpoint daemon process for an endpoint. This endpoint daemon communicates with the endpoint gateway to receive and launch endpoint methods. The endpoint daemon job is always submitted to the QSYS/QSYSNOMAX job queue.

Note: `STRTMEEPT` is equivalent to the `lcfid.sh` command, which is available for other platforms.

The `STRTMEEPT` command starts the QLCD job on the OS/400 with the appropriate configuration information. To enter endpoint configuration parameters from a prompt screen, press the F4 key.

The default value for all parameters is `*NONE`. If `*NONE` is used, the value of the parameter is set from the `last.cfg` file. If these parameters are not available in the `last.cfg` file or the `last.cfg` file is not available, the parameter values are assigned from internal default values. The following table lists and describes parameters that are available for the `STRTMEEPT` command:

Keyword and description	Parameter	Value
LGNINTRFC Specifies the IP address, or host name and port number, of one or more gateways to which the endpoint will send its login packet. This option is required for the endpoint to log in to a gateway on a different subnet or to log in to a specific gateway when two or more gateways exist on a subnet.	Login interface	<code>*NONE</code>
	Name	<i>host_name</i>
	Port	<i>port_number</i>

Keyword and description	Parameter	Value
GATEWAY Specifies the name of the gateway to be used after the endpoint successfully logs in. If the endpoint has not previously logged in, use the LGNINTRFC (or lcs.login_interfaces option in the configuration file) to provide one or more gateways through which the endpoint can login.	Gateway	*NONE
	Name	<i>host_name</i>
	Port	<i>port_number</i>
BCASTDSBL Disables the UDP broadcast. If you set this option to yes, you must use the lcs.login_interfaces option.	Broadcast disable	*NONE *YES or 1 to disable *NO or 0 to enable
EPTNAME Specifies the name of this endpoint. This name is displayed when the wep ls command is executed in the gateway.	Endpoint name	*NONE *HOSTNAME Use the host name as the name for this endpoint. <i>endpoint_name</i> Use a valid OS/400 endpoint name
PORT Specifies the port on which the endpoint daemon (lcf) monitors gateway communications. The default value is 9494.	Local TCP/IP port	*NONE <i>port_number</i>
MACHINEID Identifies the endpoint.	Machine unique ID	<i>machine_unique_id</i> Use a string that contains a unique identifier
THRESHOLD Defines the level of debug messages written to the lcf.log file. Note: Level 3 and greater logging generates a large number of messages. For troubleshooting endpoints, Level 2 is recommended.	Log threshold	0 No message logging 1 Minimal logging (default) 2 Tracing and moderate output 3 Data buffers and tight loops 4 Data
LOGSIZE Specifies the maximum size in bytes of the log file.	Log size	*NONE <i>size</i> Use a value between 10240 and 10240000.
LOGQSIZE Specifies the maximum size in bytes of the log queue.	Log queue size	*NONE <i>size</i> Use a value between 10240 and 10240000.

Keyword and description	Parameter	Value
LOGFILE Specifies the name of the log file to be used for logging messages.	Log name	* NONE <i>path_name</i> Use the name of the integrated file system (IFS) file used for the log.
CACHESIZE Specifies the maximum size of the method cache. Note: When the maximum size is reached, the least recently used methods are deleted from the cache.	Cache size	* NONE <i>size and integer</i>
UPINTRVL Specifies the number of seconds between endpoint broadcast calls.	UDP interval	* NONE <i>seconds</i>
UDPATTMPT Specifies the number of times an endpoint will transmit a broadcast call.	UDP attempts	* NONE <i>number_of_times</i> as an integer value
STRTIMEOUT Specifies the amount of time in seconds before a communications timeout occurs during login.	Start timeout	* NONE <i>seconds</i>
RUNTIMEOUT Specifies the amount of time in seconds before a communications timeout occurs following a successful login.	Run timeout	* NONE <i>seconds</i>
CFGFILE Specifies the name of the configuration file to be used to start the endpoint.	Configuration file name	* NONE <i>config_file_name</i>
RUNDIR Specifies the name of the directory from which the endpoint code will run on the OS/400.	Running directory	* NONE <i>directory_name</i>

Stopping OS/400 endpoints: The **ENDTMEEPT** command stops the endpoint daemon process for an endpoint. The job can be on a job queue, it can be active within a system, or it could have already completed running. Spooled files for an endpoint process that has been stopped remain in the output queue. Note, however, that the **ENDTMEEPT** command does not end any application jobs that have been started by the endpoint daemon—these jobs continue to run.

Use the **DELAY** option with the **ENDTMEEPT** command to specify if the endpoint is to end in a controlled manner with a time delay. The following syntax specifies valid parameters for the **ENDTMEEPT** command:

```
ENDTMEEPT [OPTION(*CTRLD|*IMMED) [DELAY(30|1-9999999)]]
```

where:

***CTRLD**

Specifies the default option that enables the endpoint daemon to finish any pending requests within the amount of time specified by the **DELAY** option (in seconds). The default delay is 30 seconds.

***IMMED**

Specifies to stop the endpoint immediately. Use this option only when a ***CTRLD** end fails to end the job and a delay time is not used.

DELAY

Specifies the timed delay in seconds after which the endpoint daemon is stopped.

Opening a remote terminal session

From a UNIX managed nodes, you can open an Xterminal (xterm) session to run Tivoli commands from a PC computer system. This terminal session operates in the same manner as a terminal emulator opened from the command line. The terminal is displayed on the same system as your Tivoli desktop, and you are logged in as the user associated with your Tivoli administrator name.

Note: To open an xterm session, you must have a user account on the managed node from which you want to open the session. If you are running Tivoli Desktop for Windows, you must be running X Window System software to display the xterm session.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required Role
Opening a remote xterm session	Managed node	user

You can open an xterm session from either the Tivoli desktop or the command line.

Desktop

To open an xterm session from a UNIX managed node, perform the following steps:

1. In the Tivoli desktop, right-click the Managed Node icon and select **Run xterm** to open an xterm session with your login name as the user.

Note: If you do not have an account on the selected managed node, you cannot open an xterm session.

2. To view emulator options, perform any of the following actions:
 - Press Ctrl and click the left mouse button to view a list of xterm options.
 - Press Ctrl and click the middle mouse button (or both left and right mouse button simultaneously) to view a list of virtual terminal options.
 - Press Ctrl and click the right mouse button to view a list of virtual terminal fonts.

Command line

For information about opening an xterm session from the command line, refer to the **wxterm** command in the *Tivoli Management Framework Reference Manual*.

Toggling a Managed Node icon

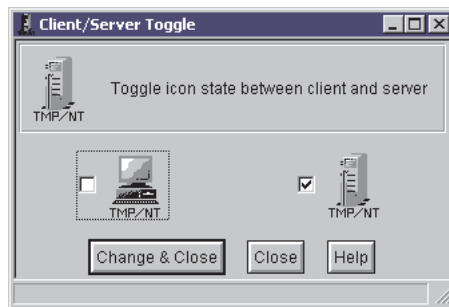
You can toggle the icon associated with a managed node between a client representation and a server representation depending on its role in your environment.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required Role
Toggling the icon for a managed node	Policy region	admin

To toggle the icon associated with a managed node, perform the following steps:

1. In a policy region, right-click the Managed Node icon and select **Toggle Icon** to display the Client/Server Toggle window:



2. Select the appropriate check box to indicate the icon you want to represent the managed node.
3. Click **Set & Close** to change the icon and return to the Tivoli desktop. The icon in the Policy Region window is updated.

Chapter 3. Tivoli administrators

A *Tivoli administrator* is the person or group of people each with user account and access to a machine where Tivoli Enterprise products are installed. A Tivoli administrator can perform system management operations against resources and manages one or more policy regions in the Tivoli environment. When the Tivoli server is installed, an initial administrator, or *root administrator*, is created. A root administrator has root authority on UNIX operating systems and Administrator privileges on Windows operating systems.

A single Tivoli administrator can represent multiple system administrators. Each system administrator associated with a Tivoli administrator shares assigned management operations. When one of these system administrator logs into the Tivoli environment and opens the Tivoli desktop, the Tivoli desktop displayed is common to all system administrators defined to this Tivoli administrator.

Working with Administrator icons

The Administrators icon is displayed on the Tivoli desktop of the root administrator and can be displayed on the Tivoli desktop of other Tivoli administrators. This icon represents a collection of defined administrators, but potentially not all administrators.

Note: A root administrator can remove an administrator from the Administrators collection without deleting the administrator from the Tivoli object database. Until the administrator is deleted from the object database, the removed administrator can be relinked to the Administrators collection.

The pop-up menu of the Administrators icon includes the following options:

Open Opens the Administrators window and displays icons for the defined administrators

Create Administrator

Displays the window where you can create a Tivoli administrator

The pop-up menu of an Administrator icon includes the following options:

Open Displays the Tivoli desktop for the administrator

Edit Properties

Displays the window where you can change the name, user login name, or group name associated with the administrator

Edit TMR Roles

Displays the window where you can change the region authorization roles for the administrator

Edit Resource Roles

Displays the window where you can change the resource authorization roles for the administrator

Edit Logins

Displays the window where you can change the user account names for the administrator

Edit Notice Group Subscriptions

Displays the window where you can modify the notice groups available to the administrator

Understanding administrator logins

Each system to be managed by Tivoli Enterprise applications might already have user accounts defined for system administrators. At many customer sites, these administrative accounts might use many different names. Additionally, these names can differ from the ones used by Tivoli administrators. When you create a Tivoli administrator, you define the following entities:

- The label used to identify the administrator within the Tivoli environment
- The mechanism that identifies which Tivoli administrator to use, based on the login name
- The ability to perform a management operation using another system-specific account name

The combination of these entities allows someone to log into a system and perform a Tivoli operation. For example, the definition of a Tivoli administrator determines that a user who logged in as `mdove` become the Tivoli administrator `InstallAdmin`. When she performs an operation on a Windows XP endpoint, that operation is performed as the user Administrator.

Therefore to perform management operations on different operating systems and managed resources, the record for a Tivoli administrator defines a relationship between the user account name that a system administrator logs in with to the Tivoli administrator name and to the user and group names.

The following terms are used to clarify the different names that can be associated with a Tivoli administrator:

administrator name

Refers to the name used within a Tivoli environment to uniquely identify a Tivoli administrator

Note: The administrator name cannot be same as a user account name.

user login name and group name

Refer to the account used to initiate requests on systems of different operating systems. These names must be defined on all computer systems used by the Tivoli administrator, but they do not have to match the user account name.

Notes:

- UNIX numeric user and group IDs are not supported.
- These names can be specified by user login maps. For additional details, refer to “Managing multiple logins” on page 31.

The user login name must be in one of the following formats:

- *username*
- *domain\username*

user account name

Refers to the user name with which a system administrator logs into the system.

Note: The same user account name cannot be defined to more than one Tivoli administrator. Because user accounts can be qualified or unqualified, the user account mario is not the same as mario@loki.

The user account name must be in one of the following formats:

- *username*
- *username@ManagedNode*
- *domain\username*
- *domain\username@ManagedNode*

Note: Possible values for *ManagedNode* are listed under the Hostname(s) column in the output of the **odadmin odlist** command.

Operations that require a user login name will not be started if the administrator does not have a user account on that managed system. The following are examples of management activities that require a user login name:

- Writing to a log file
- Running a Tivoli task where the user or group name is specified by an asterisk (*)
- Opening an xterm session from a managed node
- Performing a backup of the Tivoli object database

If you specify an *unqualified* login name (that is, *username* or *domain\username*), the administrator can start the Tivoli desktop and run Tivoli commands from any machine in the local Tivoli region. If you specify a *qualified* login name (that is, *username@host_name* or *domain\username@host_name*), the administrator can bring up the Tivoli desktop only from the specified managed node.

For example, Mario cannot start the Tivoli desktop on managed node thor unless the login mario or mario@thor is defined. If he has only the login mario@loki defined, he can start the Tivoli desktop and run Tivoli commands only on managed node loki.

Managing multiple logins

In a heterogeneous environment, an administrator can have different user accounts on different operating systems. To allow administrators to log in to Tivoli Management Framework or perform some Tivoli operations with a single login name, Tivoli Management Framework provides user login maps. A *user login map* enables Tivoli Management Framework to associate a single user login name to a user account on a specified operating system.

For example, Chris Sanders has user account chriss on a Solaris system and chris_sanders in a Windows domain. Because Chris has different user account names, you can create the user login map chris for him. To create this user login map, enter the following commands:

```
widmap add_map chris
widmap add_entry chris default chris
widmap add_entry chris w32-ix86 chris_sanders
widmap add_entry chris solaris2 chriss
```

To determine whether the user login map chris was created, enter the following command and verify its output:

```
# widmap list_entries chris
default chris
w32-ix86 chris_sanders
solaris2 chriss
```

You need to create user login maps before using them. When you create a Tivoli administrator, you can specify a user login map the user login name or group name. When you specify a user login map in the text area, use *\$map_name*. For example, if you want to use user login map chris in the **User Login Name** text box of the Create Administrator window, type \$chris in this text box.

You can also specify user login maps when you create a task. When the task is run on different operating systems, Tivoli Management Framework resolves the user to the appropriate user account for that operating system. For example, if you want the task to run under Chris Sanders' user account, type \$chris in the Execution Privileges text box. When the task is run on Windows operating systems, the task is run as chris_sanders; when the task is run on UNIX operating systems, the task runs as chriss.

For information about the **widmap** command, refer to the *Tivoli Management Framework Reference Manual*.

Accounts and user login maps

Because Tivoli Enterprise software spans a heterogeneous environment, you can map a special ID, referred to as a *user login map*, to an operating system-specific user account. On Windows operating systems, the user login map can contain a reference to w32-ix86, which is the identification within Tivoli Enterprise software for Windows operating systems.

The user login map root_user is a preconfigured user login map that resolves on Windows operating systems to BuiltinNTAdministrator. This map is used for various Windows processes. When a Tivoli service needs to resolve a method that is to run as root_user, it runs the method as the user assigned to root_user. Therefore, the root_user user login map must map correctly to a local or domain user account.

Notes:

1. \$root_user must be a member of the Administrators group and the Tivoli_Admin_Privileges group.
2. Some Tivoli methods run as root rather than \$root_user. On UNIX and Linux systems, these methods default to the root user. On Windows systems, these methods default to the built-in administrator account. If the built-in administrator account has a restriction such as an expired password, the method will fail.

To create or modify user login maps, use the **widmap** command. For example, if you have a user named fhackerm and want to add him to the **root_user** user login map, enter the following command:

```
widmap add_entry root_user fhackerm w32-ix86
```

If you have Windows systems with different administrator accounts, you can use the **widmap** command to map these accounts to the built-in administrator account instead of an account specified by name. You do this by mapping root_user to BuiltinNTAdministrator as shown in the following example:

```
widmap rm_entry root_user w32-ix86
widmap add_entry root_user w32-ix86 BuiltinNTAdministrator
```

Note: The BuiltinNTAdministrator account is not an actual Windows account name.

You can also use a domain account in one of the following ways:

- If the *machine*\Administrator account is not renamed, do not modify the root_user user login map unless you want to run the Tivoli Enterprise privileged programs as another local or domain account.
- If the *machine*\Administrator account is renamed or the design of the Tivoli region dictates using a domain account for privileged accounts, ensure that *machine*\Administrator renaming is consistent on all managed nodes and endpoints or a local Administrator account is created on each managed node or endpoint. You can name the account with a name other than Administrator, but it must be consistent on all managed nodes and endpoints. The root_user user login map must be updated to reflect the new name.

Note: The \$root_group map or another group ID must exist for an administrator. This user login map is not used when a process starts. However, it is important that \$root_group map has a group listed for w32-ix86. This map does not need to be a privileged group.

For information about the **widmap** command, refer to the *Tivoli Management Framework Reference Manual*.

Accounts created during installation

When you install Tivoli Management Framework, the tmersrvd user account and the Tivoli_Admin_Privileges group account are created. These accounts are created locally in the Security Accounts Manager (SAM) database on the Windows system and are configured the same for managed nodes and endpoints.

The tmersrvd user account

The tmersrvd account is an unprivileged account. A password is randomly generated at installation. The account can be disabled without affecting Tivoli Management Framework. Many Tivoli methods run in the context of tmersrvd. You can change the password.

You can refer to the tmersrvd account configuration for minimum requirements when creating a custom account. Refer to the Local Security Policy object in Administrative Tools window of the Windows Control panel for additional information about defining security policies for custom accounts.

The tmersrvd account needs the following user rights:

Bypass Traverse Checking

The tmersrvd account does not get assigned this user right directly. When a Windows system is installed, this right is assigned to the special group Everyone. This right allows a user to traverse a directory tree even if the user has no other rights to access this directory. If security policies in your enterprise disallow Bypass Traverse Checking, add this right to the tmersrvd account.

Note: For non-U.S. versions of a Windows system, the Everyone group account is referred to by its local language equivalent.

Log on Locally

This right is assigned to the tmersrvd account during installation of Tivoli Management Framework.

The Tivoli_Admin_Privileges group account

The Tivoli_Admin_Privileges group account is assigned by default to the built-in administrator or \$root_user map unless the Tivoli server is on a Windows system. In this case, the account used to install the Tivoli server is assigned to this group.

The Tivoli_Admin_Privileges account needs the following advanced user rights:

- Act as Part of the Operating System
- Increase Quotas
- Replace a process level token

The Act as Part of the Operating System right is required when running the **wsettap** and **wlcftap** commands without options. These commands communicate with the LSA to retrieve the current configuration of Tivoli Authentication Package. Other operations of the **wsettap** and **wlcftap** commands communicate with the registry and not the LSA, so they do not require special rights, except they can only be run by a member of the Administrators group.

The Increase Quotas and Replace a process level token rights are required to start a process as a different user. Examples of these processes are the **run_task** and **sentry_engine** methods.

Note: If you change the value of \$root_user, you need to ensure that this account is a member of the Tivoli_Admin_Privileges group. If the account is not part of this group, you will receive the following error:

```
tap_call_init failed, error 38
```

Considerations for domain controllers

This section discusses issues particular to primary and backup domain controllers.

Authentication to the primary domain controller

When using Tivoli Authentication Package, it requests domain user authentication from the Primary Domain Controller (PDC) and bypasses any local backup domain controllers (BDCs). This can flood the primary domain controller with authentication requests if the domain account is used for the \$root_user user login map or for applications, such as Tivoli Distributed Monitoring, that can run a large number of processes in a short span of time.

Many Windows environments use several domains to manage the environment. Commonly, a master domain with resource domains that are two-way trusted with the master domain are used. If requirements demand that you use a domain account for your Tivoli environment and the Windows domains, you could create an account in each domain with the same names. For example, you could create the tivuser account in multiple domains:

- MASTER\tivuser
- US\tivuser
- GERMANY\tivuser
- JAPAN\tivuser

The \$root_user map would map w32-ix86 to tivuser. When a managed node or endpoint runs a privileged process, Tivoli Authentication Package ensures that the map references tivuser. It first looks in the SAM database. If Tivoli Authentication Package does not find the account there, it queries the primary domain controller

for the system. Therefore, a system in the JAPAN domain will only be authenticated to the JAPAN domain controller rather than the MASTER domain controller.

Using the same model in the JAPAN domain, assume a given task must run as MASTER\tivuser. You would specify MASTER\tivuser in the user ID (UID) field of the task or create a user login map that resolves to this account. If MASTER is not part of the specified account, the same system in the JAPAN domain gets the system ID (SID) for the JAPAN\tivuser account rather than the MASTER\tivuser account.

Accounts created on the domain controllers

If using both primary and backup domain controllers within a Tivoli environment, it is recommended that you install the managed node or endpoint on the primary domain controller first and then synchronize the backup domain controllers to allow the newly created accounts to propagate. If an installation is attempted first on a backup domain controller, the installation fails because the accounts have not been updated from the primary domain controller. Wait 15 minutes for the domain servers to resynchronize and attempt the installation again.

For account management, primary and backup domain controller accounts are considered a domain account. When Tivoli Management Framework runs on either a primary domain controller or backup domain controller, the authentication will still take place on the local SAM database with no impact to the network or other domain controllers. Additionally, Tivoli Enterprise software does not force partial or full synchronization with a domain.

Creating a Tivoli administrator

Each system administrator that uses Tivoli Enterprise applications to manage resources must be associated with a Tivoli administrator.

The following table provides the context and authorization role required for this operation:

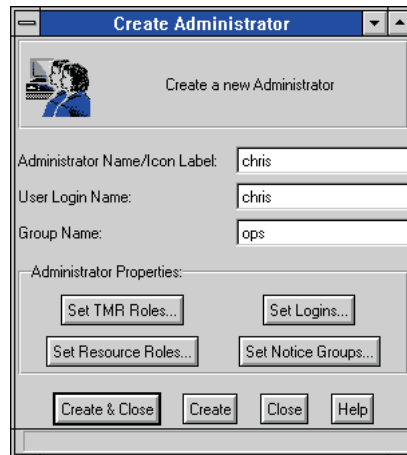
Activity	Context	Required role
Creating a Tivoli administrator	Tivoli region	senior

You can create a Tivoli administrator from either the Tivoli desktop or the command line.

Desktop

To create a new Tivoli administrator, perform the following steps:

1. In the Tivoli desktop, right-click the Administrators icon and select **Create Administrator** to display the Create Administrator window.



Note: Clicking **Create & Close** before specifying the administrator properties (administrator name, user login name, group name), authorization roles (region or resource), and logins (user account names) will fail. You must specify all these values before you can successfully create a Tivoli administrator.

2. Specify the label and accounts for the administrator.
 - a. In the **Administrator Name/Icon Label** text box, type the name of the administrator.

Note: The name of a Tivoli resource can include alphanumeric characters, underscores (_), hyphens (-), periods (.), and spaces. If you use a resource name that contains spaces on the command line, you must enclose the resource name in double quotation marks (" ").

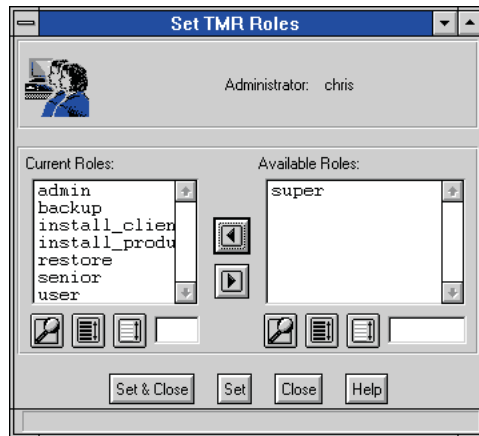
- b. In the **User Login Name** text box, type the user login name (not a numeric user ID). The user login name must be either a valid login name on all machines managed by this administrator or a user login map in the form *\$map_name*.

Note: The value specified here is important. It is used to determine the system account under which many operations are performed. For example, various windows contain options to save output to a file on a particular machine. Such operations are performed with an account calculated from the user login name specified. An operation that runs on a managed node, such as **Run Xterm**, fails if the user login name cannot be resolved to a system account on that machine.

- c. In the **Group Name** text box, type the group name (not a numeric group ID). The group name can be a user login map in the form *\$map_name*. This text box is used for operations performed on UNIX managed nodes.

Note: The value specified here is important. It is used to determine the group account under which many operations are performed. For example, various windows contain options to save output to a file. Such operations are performed with a group account calculated from the group name specified.

3. Click **Set TMR Roles** to display the Set TMR Roles window where you can set the Tivoli region roles for the administrator:



a. Add or remove Tivoli region roles.

- To add roles, select one or more roles from the **Available Roles** list and click the left-arrow button. The selected roles are moved from the **Available Roles** list to the **Current Roles** list.

Notes:

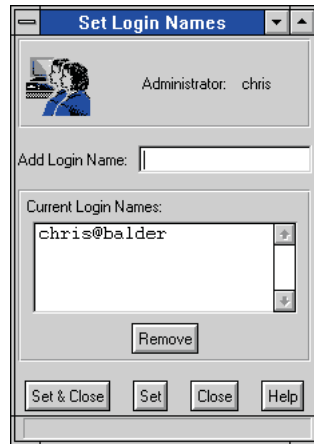
- You must have the **super** role in the local region to assign an administrator the **super** role.
- In general, do not assign an administrator a region role. Instead, assign only resource roles. Region roles are required only for specific region-wide operations, such as connecting and disconnecting regions.
- To remove roles, select one or more roles in the **Current Roles** list and click the right-arrow button. The selected roles are moved from the **Current Roles** list to the **Available Roles** list.

Note: Do not remove the **super** or **senior** region roles for the root administrator without ensuring that another administrator with these roles also has root authority. Root authority is granted with the **wauthadmin** command.

You can also double-click an entry to move it from one list to the other list.

Note: Depending on the Tivoli Enterprise applications installed, the region roles can differ. As authorization roles are added to your Tivoli environment, you must modify previously defined administrators if they are to perform management operations requiring these new roles.

- Click **Set & Close** to save your changes and return to the Create Administrator window.
- Click **Set Logins** to display the Set Login Names window where you can set the login names under which the administrator will run Tivoli operations from either the Tivoli desktop or the command line.



a. Add or remove user account names.

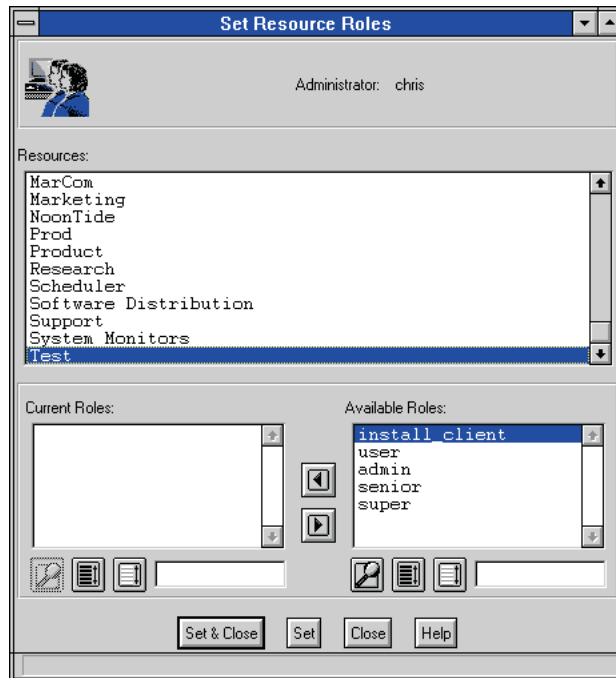
- To add a user account name, type the login name for the system administrator in the **Add Login Name** text box and press **Enter**. The user account name must be in one of the following formats:
 - *username*
 - *username@ManagedNode*
 - *domain\username*
 - *domain\username@ManagedNode*

Note: Possible values for *ManagedNode* are listed under the Hostname(s) column in the output of the **odadmin odlist** command.

The new user account name is added to the **Current Login Names** list. To add another user account name, repeat this step for each name that you want to add.

Note: It is recommended that all user account names be qualified for the security and integrity of your distributed system.

- To remove a user account name from the list, select the names to be removed from the **Current Login Names** list and click **Remove**.
- b. Click **Set & Close** to save your changes and return to the Create Administrator window.
5. Click **Set Resource Roles** to display the Set Resource Roles window where you can set the resource roles for the administrator.



- a. From the **Resources** list, select a resource type for which the administrator requires access. An administrator can have different roles for different resource types.
- b. Add or remove roles for the selected resource.
 - To add roles, select one or more roles from the **Available Roles** list and click the left-arrow button. The selected roles are moved from the **Available Roles** list to the **Current Roles** list.
 - To remove roles, select one or more roles from the **Current Roles** list and click the right-arrow button. The selected roles are moved from the **Current Roles** list to the **Available Roles** list.

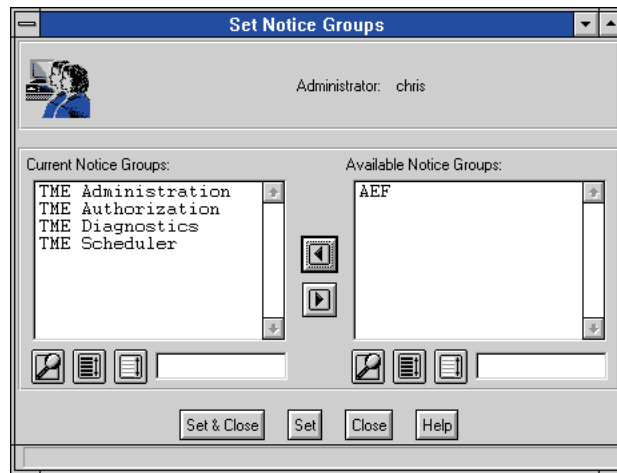
You can also double-click an entry to move it from one list to the other list.

Notes:

- For an administrator to create other Tivoli administrators or schedule tasks, the administrator must have one or more resource roles specific to the Administrators collection or Scheduler resource. In addition, you must drop the Administrators or Scheduler icon onto the Tivoli desktop of that administrator. Refer to “Managing resources for administrators” on page 40 for details.
 - Depending on the Tivoli Enterprise applications installed, the resources and roles can differ. As resources or roles are added to your Tivoli environment, you must modify the administrators if they are to perform management operations against these new resources.
- c. If you are adding or removing roles for more than one resource, click **Set** and select the next resource and set its roles. If you are finished assigning resource roles, click **Set & Close** to return to the Create Administrator window.

Note: You must click **Set** after each resource to which you assign roles. Roles are not added or removed until you click **Set** or **Set & Close**.

6. Click **Set Notice Groups** to display the Set Notice Groups window where you can set the notice groups for the administrator.



- a. Add or remove notice group subscriptions.
 - To subscribe an administrator to one or more notice groups, select the notice groups to be added from the **Available Notice Groups** list and click the left-arrow button. The selected groups are moved from the **Available Notice Groups** list to the **Current Notice Groups** list.
 - To unsubscribe an administrator from one or more notice groups, select the groups to be removed from the **Current Notice Groups** list and click the right-arrow button. The selected groups are moved from the **Current Notice Groups** list to the **Available Notice Groups** list.
- You can also double-click an entry to move it from one list to the other list.

Note: Depending on the Tivoli Enterprise applications installed, the notice groups can differ. As notice groups are added to your Tivoli environment, you must modify the administrators if they are to monitor management operations against these new resources.

- b. Click **Set & Close** to save your changes and return to the Create Administrator window.
7. Click **Create & Close** to create the new administrator and return to the Administrators window. An icon for the new administrator is displayed in the Administrators window.

Command line

For information about creating administrators from the command line, refer to the **wcrtadmin** command in the *Tivoli Management Framework Reference Manual*.

Managing resources for administrators

After you create administrators, you need to allow these administrator to access those resources from their Tivoli desktops. In Tivoli Management Framework, providing access to resources from the Tivoli desktop is accomplished through drag and drop.

You can copy icons representing most managed resources from the Tivoli desktop of one administrator to another. To keep the Tivoli desktop ordered, you can create a collection and drop it.

The following table provides the context and authorization role required for this operation:

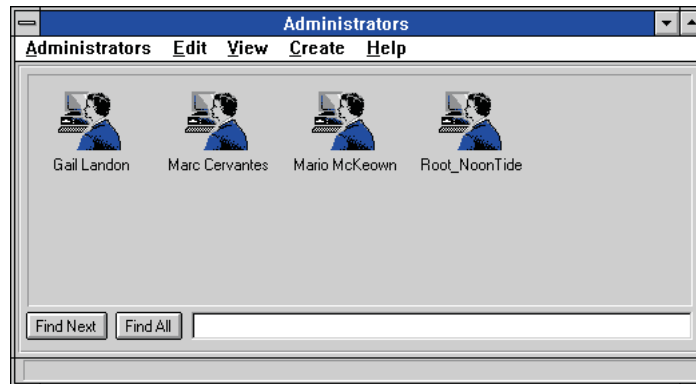
Activity	Context	Required role
Adding and removing resources associated with an administrator	Tivoli region	admin

You can add or remove resources from either the Tivoli desktop or the command line.

Desktop

To add a resource to an administrator Tivoli desktop, perform the following steps:

1. Double-click the Administrators icon to display the Administrators window that contains the icons representing defined Tivoli administrators.



2. Select one or more resource icons from the Tivoli desktop and drag and drop them on an Administrator icon. That Tivoli desktop now contains the references to these resources.

Note: The Tivoli administrator on whose Tivoli desktop you dropped the icons must have the appropriate roles for those resource for that administrator to perform management operations against those resources. If you have not set these roles, refer to "Changing resource roles" on page 45 for details.

To remove resources from a Tivoli desktop, perform the following steps:

1. In the Tivoli desktop, double-click the Administrators icon to open the Administrators window.
2. Double-click the icon representing an administrator to open that Tivoli desktop.
3. Select the resource icon to be removed.
4. From the **Edit** menu, select **Remove**. The resource icon is removed from that Tivoli desktop.

Note: After removing a resource, you can modify the resource roles as appropriate. Refer to "Changing resource roles" on page 45 for details.

Command line

For information about changing resources associated with administrators using the command line, refer the **wgetadmin** and **wsetadmin** commands in the *Tivoli Management Framework Reference Manual*.

Managing administrators

Because a single Tivoli administrator can represent multiple system administrators, it might be necessary to modify a Tivoli administrator when system administrators are added or removed from assignments. The following sections detail the procedures for modifying the properties, authorization roles, user logins, and subscriptions.

When managing administrators, do not change the user login name or group name. Changing these values can cause specific resources to behave unexpectedly. These resources include gateways and tasks. These affected resources are directly associated with the user login name or group name of the administrator who created them.

Changing administrator properties

The properties associated with an administrator (name, user login name, and group name) can be changed to adjust to new and changing requirements.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Changing administrators properties	Administrators collection	senior

You can change properties associated with an administrator from the Tivoli desktop only.

To set the properties of an administrator, perform the following steps:

1. Double-click the Administrators icon to open the Administrators collection.
2. From the pop-up menu of an administrators, select **Edit Properties** to display the Administrator Properties window.



3. In the **Administrator Name/Icon Label** text box, type the name of the administrator.

Note: The name of a Tivoli resource can include alphanumeric characters, underscores (_), hyphens (-), periods (.), and spaces. If you use a resource name that contains spaces on the command line, you must enclose the resource name in double quotation marks (" ").

4. In the **User Login Name** text box, type the user login name (not a numeric user ID). The user login name must be either a valid login name on all machines managed by this administrator or a user login map in the form `$map_name`.

Note: The value specified here is important. It is used to determine the system account under which many operations are performed. For example, various windows contain options to save output to a file on a particular machine. Such operations are performed with an account calculated from the user login name specified. An operation that runs on a managed node, such as **Run Xterm**, fails if the user login name cannot be resolved to a system account on that machine.

5. In the **Group Name** text box, type the group name (not a numeric group ID). The group name can be a user login map in the form `$map_name`. This text box is used for operations performed on UNIX managed nodes.

Note: The value specified here is important. It is used to determine the group account under which many operations are performed. For example, various windows contain options to save output to a file. Such operations are performed with a group account calculated from the group name specified.

6. Click **Change & Close** to change the properties of the administrator as specified. An informational window is displayed. Changes to the user login name and group name for an administrator do not take effect immediately if the administrator's desktop is currently active.
7. Click **Dismiss** to return to the Administrators window.

Changing region roles

After an administrator is defined, it might be necessary to change the region roles for an administrator because of changes in your environment or the responsibilities of the administrator.

If you assign an administrator a role other than **super**, **install_product**, or **install_client**, the roles for the administrator are mapped across two-way connected regions and on the managing side of any one-way connected regions. If you assign an administrator a role of **super**, **install_product**, or **install_client** in a region, these roles map across connected regions as **user**. The default mapping for roles can be changed by using the **odadmin** command with the region option. Refer to the *Tivoli Management Framework Reference Manual* for more information.

Administrators with these roles can perform tasks that require these roles only within the Tivoli region where the administrator was created. To assign an administrator one of these roles in more than one region, you must create separate administrators in each Tivoli region. However, creating separate administrators still does not allow tasks requiring these roles to complete across Tivoli regions.

The following table provides the context and authorization role required for this operation:

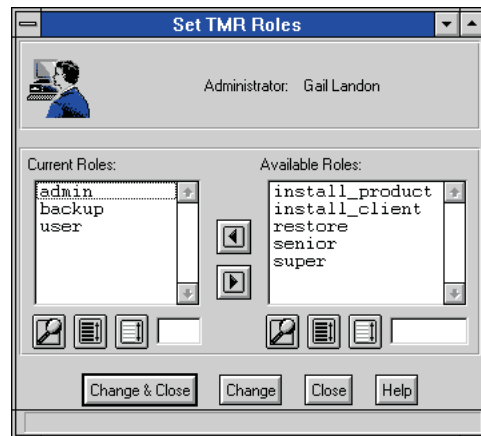
Activity	Context	Required role
Changing region roles for an administrator	Tivoli region	senior

You can edit Tivoli region roles for an administrator from either the Tivoli desktop or the command line.

Desktop

To change an Tivoli region roles for an administrator, perform the following steps:

1. In the Tivoli desktop, double-click the Administrators icon to open the Administrators window.
2. Right-click an Administrator icon and select **Edit TMR Roles** to display the Set TMR Roles window:



3. Add or remove Tivoli region roles.
 - To add roles, select one or more roles from the **Available Roles** list and click the left-arrow button. The selected roles are moved from the **Available Roles** list to the **Current Roles** list.

Notes:

- You must have the **super** role in the local region to assign an administrator the **super** role.
- In general, do not assign an administrator a region role. Instead, assign only resource roles. Region roles are required only for specific region-wide operations, such as connecting and disconnecting regions.
- To remove roles, select one or more roles in the **Current Roles** list and click the right-arrow button. The selected roles are moved from the **Current Roles** list to the **Available Roles** list.

Note: Do not remove the **super** or **senior** region roles for the root administrator without ensuring that another administrator with these roles also has root authority. Root authority is granted with the **wauthadmin** command.

You can also double-click an entry to move it from one list to the other list.

Note: Depending on the Tivoli Enterprise applications installed, the region roles can differ. As authorization roles are added to your Tivoli environment, you must modify previously defined administrators if they are to perform management operations requiring these new roles.

4. Click **Change & Close** to add or remove the selected Tivoli region roles for the administrator, as specified, and return to the Administrators window.

Command line

For information about using the command line to set or change Tivoli region roles for an administrator, refer to the **wgetadmin** and **wsetadmin** commands in the *Tivoli Management Framework Reference Manual*.

Changing resource roles

After an administrator is defined, it might be necessary to change the resource roles for an administrator because of changes in your environment or the responsibilities of the administrator.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Changing resource roles for an administrator	Administrators collection	senior

You can set a resource role for an administrator from either the Tivoli desktop or the command line.

Desktop

To set or change resource authorization roles for an administrator, perform the following steps:

1. In the Tivoli desktop, double-click the Administrators icon to open the Administrators window.
2. Right-click an Administrator and select **Edit Resource Roles** to display the Set Resource Roles window:



3. From the **Resources** list, select a resource type for which the administrator requires access. An administrator can have different roles for different resource types.
4. Add or remove roles for the selected resource.
 - To add roles, select one or more roles from the **Available Roles** list and click the left-arrow button. The selected roles are moved from the **Available Roles** list to the **Current Roles** list.

- To remove roles, select one or more roles from the **Current Roles** list and click the right-arrow button. The selected roles are moved from the **Current Roles** list to the **Available Roles** list.

You can also double-click an entry to move it from one list to the other list.

Notes:

- For an administrator to create other Tivoli administrators or schedule tasks, the administrator must have one or more resource roles specific to the Administrators collection or Scheduler resource. In addition, you must drop the Administrators or Scheduler icon onto the Tivoli desktop of that administrator. Refer to “Managing resources for administrators” on page 40 for details.
 - Depending on the Tivoli Enterprise applications installed, the resources and roles can differ. As resources or roles are added to your Tivoli environment, you must modify the administrators if they are to perform management operations against these new resources.
5. If you need to add or remove roles from another resource type, click **Change** and select another resource type to which to assign roles. If you are finished assigning roles, click **Change & Close** to return to the Administrators window.

Note: You must click **Change** after each resource type to which you assign roles. Resource roles are not added or removed until you click **Change** or **Change & Close**.

Command line

For information about changing the resource authorization roles for an administrator using the command line, refer to the **wgetadmin** and **wsetadmin** commands in the *Tivoli Management Framework Reference Manual*.

Changing user account logins

Tivoli Management Framework sets the logins and managed nodes that are valid for an administrator. Administrators can have different logins for different managed nodes. For example, Juan might have logins such as `juan@snowdon`, `juan@orodruin`, and `juan@ayers-rock`.

To define an administrator as valid from a specific managed node (for example, to enable an administrator to start the Tivoli desktop or invoke Tivoli commands from a specific machine), the administrator must have a login name on that managed node. For example, Juan cannot run as administrator `juan` on managed node `cook` unless the login `juan` or `juan@cook` is defined. For security reasons, it is recommended that all administrators be defined as valid from one or more specific managed nodes. For example, if administrator `juan` is to run only on managed nodes `cook` and `wichita`, it is preferable to assign the logins `juan@cook` and `juan@wichita`, rather than assigning the login `juan`, which would allow administrator `juan` to run on any managed node.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Changing logins for an administrator	Administrators collection	senior

You can change logins for an administrator from either the Tivoli desktop or the command line.

Desktop

To change logins for an administrator, perform the following steps:

1. In the Tivoli desktop, double-click the Administrators icon to open the Administrators window.
2. Right-click an Administrator icon and select **Edit Logins** to display the Set Login Names window:



3. Add or remove user account names.

- To add a user account name, type the login name for the system administrator in the **Add Login Name** text box and press **Enter**.

The user account name must be in one of the following formats:

- *username*
- *username@ManagedNode*
- *domain\username*
- *domain\username@ManagedNode*

Note: Possible values for *ManagedNode* are listed under the Hostname(s) column in the output of the **odadmin odlist** command.

The new user account name is added to the **Current Login Names** list. To add another user account name, repeat this step for each name that you want to add.

Note: It is recommended that all user account names be qualified for the security and integrity of your distributed system.

- To remove a user account name from the list, select the names to be removed from the **Current Login Names** list and click **Remove**.

4. Click **Change & Close** to add or remove logins for the administrator as specified and return to the Administrators window.

Command line

For information about setting on changing the login for an administrator using the command line, refer to the **wgetadmin** and **wsetadmin** commands in the *Tivoli Management Framework Reference Manual*.

Changing notice group subscriptions

An administrator can be subscribed to one or more notice groups to receive information about management operations performed by other Tivoli administrators.

The following table provides the context and authorization role required for this operation:

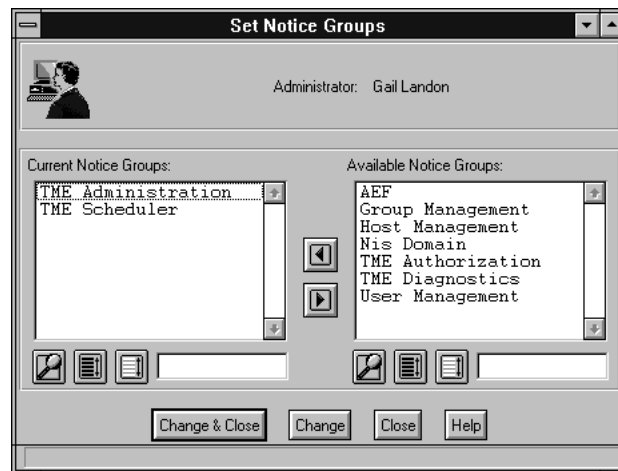
Activity	Context	Required role
Changing a notice group subscription	Administrators collection	senior

You can subscribe an administrator to notice groups from either the Tivoli desktop or the command line.

Desktop

To set the notice group subscriptions for an administrator, perform the following steps:

1. In the Tivoli desktop, double-click the Administrators icon to open the Administrators window.
2. Right-click and Administrator icon and select **Edit Notice Group Subscriptions** to display the Set Notice Groups window:



3. Add or remove notice group subscriptions.
 - To subscribe an administrator to one or more notice groups, select the notice groups to be added from the **Available Notice Groups** list and click the left-arrow button. The selected groups are moved from the **Available Notice Groups** list to the **Current Notice Groups** list.
 - To unsubscribe an administrator from one or more notice groups, select the groups to be removed from the **Current Notice Groups** list and click the right-arrow button. The selected groups are moved from the **Current Notice Groups** list to the **Available Notice Groups** list.

You can also double-click an entry to move it from one list to the other list.

Note: Depending on the Tivoli Enterprise applications installed, the notice groups can differ. As notice groups are added to your Tivoli environment, you must modify the administrators if they are to monitor management operations against these new resources.

4. Click **Change & Close** to add or remove notice group subscriptions for the administrator and return to the Administrators window.

Command line

For information about using the command line to set or change notice group subscriptions for an administrator, refer to the **wgetadmin** and **wsetadmin** commands in the *Tivoli Management Framework Reference Manual*.

Viewing administrators

You can view all defined administrators in a Tivoli region.

The Tivoli desktop shows only a subset of non-deleted administrators. The command line output lists all defined administrators, including those that were removed from being displayed in the Administrators window.

The following table provides the context and authorization role required for this operation:

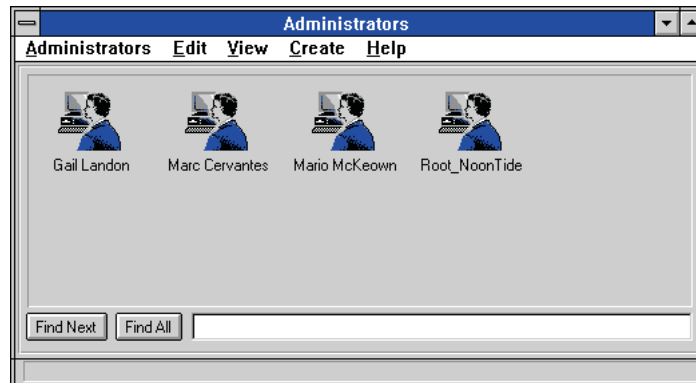
Activity	Context	Required role
Viewing administrators	Tivoli region	user

You can view Tivoli administrators from either the Tivoli desktop or the command line.

Desktop

To view administrators, perform the following steps:

1. In the Tivoli desktop, double-click the Administrators icon to display the Administrators window:



Each icon represents an administrator. The icon label is the administrator name. Depending on the size of your organization, you can have only a few or many Tivoli administrators.

2. To view the contents of the Tivoli desktop of a particular administrator, double-click that icon.

Command line

You can use one of the following commands to view administrators from the command line:

```
wls /Administrators
wlookup -ar Administrator
```

The **wls** command shows the administrator names as seen in the Administrators collection. The **wlookup** command shows the Administrator resources, including administrator name and user login names.

To display information about a specific administrator, enter the following command:

```
wgetadmin admin_name
```

where *admin_name* is the name of the administrator.

Refer to the **wls**, **wlookup**, and **wgetadmin** commands in the *Tivoli Management Framework Reference Manual* for complete details.

Removing an Administrator icon

Tivoli Management Framework creates a database object and a desktop object for each defined Tivoli administrator. Removing an administrator removes the icon from the Tivoli desktop. However, the database object for the account remains in the Tivoli object database. Refer to “Deleting an administrator” on page 51 for information about deleting the database object.

The ability to remove the icon without deleting the account gives administrators flexibility when maintaining a Tivoli desktop that other administrators share. For example, an administrator in a position of authority can create administrator accounts—which become objects in the database—and then remove them from the Tivoli desktop. This tactic prevents administrators with less authority or experience from mismanaging the accounts.

Removing an administrator is useful in managing collections. For example, suppose you create administrators in the Administrators collection, and then copy the icons to a new collection, **Support Admins**. Because you no longer need the original icons in the Administrators collection, you can remove them.

You can remove an Administrator icon using either the Tivoli desktop or the command line.

Desktop

To remove a Tivoli administrator from the Tivoli desktop using the Tivoli desktop, perform the following steps:

1. Double-click the Administrators icon to open the Administrators collection.
2. Select the administrator to be removed.
3. From the **Edit** menu, select **Remove**.

The administrator is removed from the Tivoli desktop, but its database object remains in the Tivoli object database.

Command line

To remove an administrator from the Tivoli desktop using the command line, enter the following command:

```
wrm /administrators/admin_name
```

where *admin_name* is the name of the administrator.

For additional details, refer to the **wrm** command in the *Tivoli Management Framework Reference Manual*.

Viewing removed administrators

Removed administrators no longer appear on the Tivoli desktop, but their database objects remain in the database. To view a list of all administrators, including those removed, enter the following command:

```
wls /Library/Administrator
```

Restoring a removed administrator

Removing an administrator removes its icon from the Tivoli desktop. To restore the icon, perform the following steps:

1. From the command line, enter:

```
wln /Library/Administrator/admin_name /Administrators
```

where *admin_name* is the name of the administrator. This command restores the icon to the Administrators collection, but the icon is not visible in the Administrators window until you complete the next step.

2. From the **View** menu, select **Refresh**. The icon is displayed on the Tivoli desktop.

Deleting an administrator

Deleting an administrator removes the icon from the Tivoli desktop and deletes the database object from the Tivoli object database. You cannot restore deleted administrators.

Tivoli Management Framework prevents you from deleting the root administrator and prevents you from deleting the last administrator with the **admin** role. These fail-safe features ensure that you retain necessary accounts.

Note: If the administrator to be deleted created any gateways or tasks, then these objects will behave unexpectedly after the administrator is deleted. Do not delete these administrators.

You can delete an administrator from either the Tivoli desktop or the command line.

Desktop

The Tivoli desktop for each Tivoli administrator can contain resources specific to that account. Before deleting an administrator, delete any collections in that Tivoli desktop. To delete a Tivoli administrator, perform the following steps:

1. Delete any collections in the Tivoli desktop for that administrator.
2. From the **Edit** menu, select **Delete**. A confirmation window is displayed.
3. Click **Yes** to delete the database object.

Command Line

To delete an administrator from the command line, enter the following command:

```
wdel /Library/Administrator/admin_name
```

where *admin_name* is the name of the administrator.

Chapter 4. Tivoli regions and interregion connections

A *Tivoli region* consists of a Tivoli server and the set of clients (managed nodes, gateways, and endpoints) that it serves. Depending on the size and operational requirements of your organization, you might have more than one Tivoli region.

In most situations, standalone Tivoli regions do not meet the needs of an organization. One of the regions might contain resources that another region needs, or an administrator might want all Tivoli regions to be managed in a consistent fashion. In either case, the regions need to be connected.

After you connect Tivoli regions, schedule periodic exchanges of resource information between them. When Tivoli regions are first connected, the administrator is asked if resources should be updated immediately on connection.

Note: Always update resources *after* the connection to the other Tivoli region is complete.

You can use the scheduler service to schedule an information exchange for a later time or to update information on a regular basis. Two-way interconnected regions should update information at different times. Refer to Chapter 10, "Scheduling jobs," on page 129 for more information.

Secure Sockets Layer data encryption

Although Tivoli Management Framework provides data encryption, you should use one of the provided Secure Sockets Layer (SSL) packages for increased security.

SSL provides for secure communication by using public-key cryptography and digital signatures. SSL provides authentication, data integrity, and encryption to protect the privacy of network traffic in a Tivoli environment. Tivoli Management Framework supports SSL encryption.

For additional information about SSL within a Tivoli environment, refer to *Tivoli Management Framework Planning for Deployment Guide*.

Enabling SSL communications

Support for SSL security on non-Linux managed nodes is provided by the Tivoli Management Framework SSL-A run-time package, an implementation of the Secure Sockets Layer Protocol, Version 3.0. You must install this package on each managed node on which you want to enable SSL connections. For Linux managed nodes, SSL is enabled by default. Installing the SSL-B package provides access to the keystore management utilities.

You can install the SSL-A package before or after creating a managed node. However, you must install SSL-A before setting the network security level. If SSL-A is not installed on a managed node, it can only accept non-SSL connections. Because SSL is enabled on a per-node basis, it is possible to have a mix of SSL and non-SSL operating systems within a Tivoli region or across region boundaries.

To enable SSL communications, perform the following steps:

1. Install the SSL-A run-time package to make a managed node capable of handling SSL connections.

Note: The Tivoli server must be SSL-capable before any managed node can use SSL.

2. Set the network security level on each managed node on which you want to enable SSL communications. This setting determines how the managed node logs in to the server.
3. Specify the cipher list on each managed node to dictate the strength of the encryption used by SSL.

Note: After making a network security or cipher change, restart the managed node for the changes to take effect.

Setting network security level

After installing SSL-A to make managed nodes capable of accepting SSL connections, you must set the network security level for each node on a per-node basis. For two managed nodes to use SSL, both managed nodes must be set to support it. To set the network security level, use the **odadmin set_network_security** command.

Notes:

1. This setting does not replace protection provided by the encryption level of the managed node (**odadmin set_crypt_level**). The encryption level (**none**, **simple**, or **DES**) is still used for method authorization and authentication and continues to operate whether SSL is enabled.
2. The creation of an inter-region connection is not supported when the network security setting on a remote Tivoli server is set to **FORCE_SSL**. Therefore, you must temporarily set the network security setting on the remote Tivoli server to **SSL** using the **odadmin set_network_security** command until the inter-region connection is successful. After you complete the inter-region connection, you can reset the network security setting on the remote Tivoli server to **FORCE_SSL**.

Network security levels are as follows. You can set these levels for specific managed nodes, all clients, or all managed nodes in a Tivoli region.

none Specifies that the managed node does not use SSL to communicate. This is the default setting. If the managed node is set to **none** and is SSL-capable, the managed node does not use SSL except when communicating with a managed node set to **FORCE_SSL**.

SSL Specifies that the managed node uses SSL when communicating with other SSL-enabled managed nodes. SSL is not used when communicating with a managed node set to **none**.

FORCE_SSL

Specifies that the managed node only communicates using SSL. Any non-SSL connections are dropped by the managed node.

The network security setting for a managed node dictates how it logs in to the Tivoli server, regardless of the setting for the server. Therefore, a managed node with a setting of **SSL** establishes an SSL session to the Tivoli server even if the server has a setting of **none**. This occurs because the managed node is unaware of the setting of the server until after it logs in. For this reason, the Tivoli server must be SSL-capable (has the SSL package installed) before any managed nodes can use

SSL connections. Also, if a managed node mistakenly logs in to the Tivoli server with no security (a setting of **none**) and finds that it should use SSL, the Tivoli server immediately secures the connection with SSL.

Note: If the Tivoli server is set to **FORCE_SSL** and a managed node is set to **none**, running the **odadmin reexec all** command stops the managed node but does not restart it. This is due to the fact that the managed node cannot get the security state of the Tivoli server.

In emergency situations, such as if the SSL package was inadvertently removed from a SSL-enabled managed node, you can use the **oserv -n** command to set the network security level.

Note: Restart the managed node for the changes to take effect. For more information about the **odadmin** and **oserv** commands, refer to the *Tivoli Management Framework Reference Manual*.

Setting ciphers for data transfer

Ciphers dictate the strength of the encryption used by SSL. During SSL negotiation, both the initiator and the receiver of the SSL connection share their cipher list. The SSL session is established through a handshake sequence between the managed nodes. Typically, the managed node assigned the role of SSL server determines the cipher to use. The SSL server does this by checking its cipher list and selecting the first cipher that is also supported by the client. The server then uses the session keys and begins encrypted communications.

The following table lists the ciphers supported by the SSL packages. Each cipher is represented by a two-character code.

Cipher code	Key exchange (public/private)	Symmetric encryption	Integrity check (hash)
05	RSA	RC4_128	SHA
04	RSA	RC4_128	MD5
0A	RSA	3DES_EDE_CBC	SHA
03	RSA	RC4_40	MD5
06	RSA	RC2_CBC_40	MD5
09	RSA	DES_CBC	SHA
02	RSA	None	SHA
01	RSA	None	MD5
00	None	None	None

Use the **odadmin set_ssl_ciphers** command to set ciphers on managed nodes that protect the channel. The managed node must be SSL-capable before you can change a user-defined cipher list. You can set ciphers for specific managed nodes, all clients, or all managed nodes in a Tivoli region. For example, to specify the cipher list (050A09) for a specific object dispatcher number (*od#*), enter the following command:

```
odadmin set_ssl_ciphers "050A09" [od#]
```

Moreover, the order in which you specify the ciphers indicates the order of preference that the SSL server searches its cipher list. For example, if the SSL server contacts a client, it checks whether the client has cipher 05. If the cipher list for a

does not include 05, the SSL server checks for 0A and so on. You also can specify that a managed node has the **default** setting, which means that the managed node has the default Tivoli cipher list of 05040A030609. Note that any managed node can be set to the default regardless of its SSL capabilities.

In emergency situations, such as if the SSL-A package was inadvertently removed from a SSL-enabled managed node, you can use the **oserv -E** command. This command affects only the initial connection of managed node to the Tivoli server, at which time it defaults back to the cipher value stored on the server. This is an additional check to make sure that a hacker who has gained access to a particular managed node cannot weaken the overall encryption. If you specify **oserv -E** on the Tivoli server itself, the new cipher values become the new settings for the server.

Note: You must restart the managed node for the changes to take effect. For more information about the **odadmin** and **oserv** commands, refer to the *Tivoli Management Framework Reference Manual*.

Replacing certificates and keys

The steps to replace the default Tivoli certificates and keys include the following:

1. Remove the Tivoli certificate, Tivoli global signing key, and any generated Tivoli key from the keystores.
2. Add your own certificates to both files. The trust hierarchy that you use can be any granularity, ranging from a deployment-wide certificate encompassing all Tivoli regions to trusting only certain managed nodes.
3. Add your own private key to Tivoli.kdb, signed by the certificate authority of your choice. The only requirement is that the label for the private key is Framework.

The default password is password for both Tivoli.kdb and TivoliCert.kdb files. You must change the password on the Tivoli.kdb file, and stash the password. Tivoli Management Framework uses the password encrypted in the stash file to access either keystore. The names of the stashed password files are Tivoli.sth and TivoliCert.sth, respectively. The permission of each file must be equivalent to the keystore; that is, root read and write access only for Tivoli.sth; read permission for all users on TivoliCert.sth

Note: Use caution when using a stash file to automate SSL initialization. You must ensure that the key database password in the stash file is protected. The key database password is encrypted in the stash file so that it cannot be recognized by a casual observer. You should not allow unauthorized persons access to either the stash file or the key database file. As with all Web server resources, managing proper file permissions and protections is vital to the security of the system.

Making a secure region connection

You can make a secure Tivoli region connection and specify the connection properties from the Tivoli desktop. To create a secure connection, you must make the connection locally on each of the regions that you are connecting.

The following table provides the context and authorization role required for this operation:

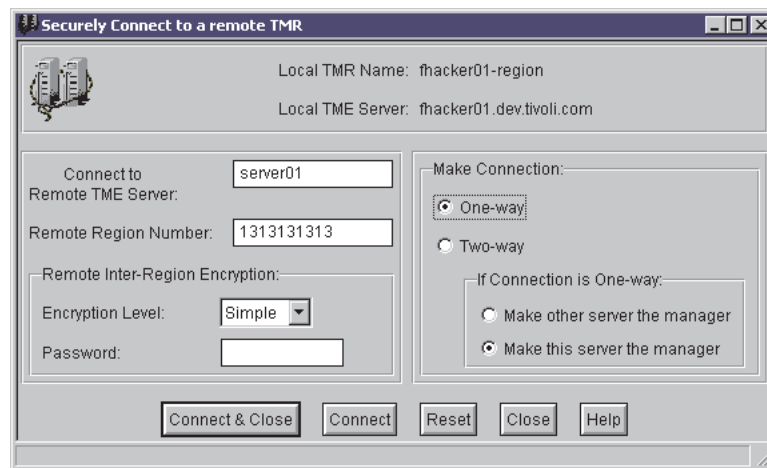
Activity	Context	Required role
Making a secure Tivoli region connection	Tivoli region	super

You can make a secure Tivoli region connection from either the Tivoli desktop or the command line.

Desktop

To make a secure connection, perform the following steps:

1. Select **TMR Connections** → **Secure Connect** from the **Desktop** menu to display the Securely Connect to a remote TMR window:



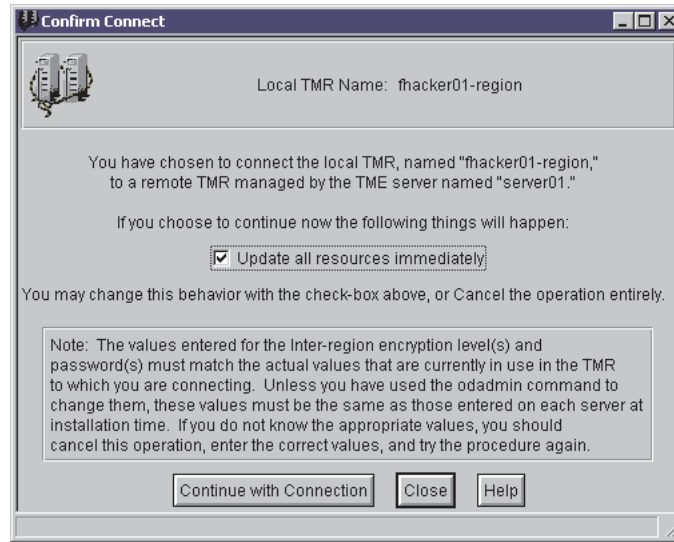
2. Type the name of the server you want to connect to in the **Connect to Remote Tivoli Server** text box.
3. Type the region number of the server that you want to connect to in the **Remote Region Number** text box. To find the region number, use the **odadmin** command. Refer to the *Tivoli Management Framework Reference Manual* for more information about the **odadmin** command.
4. From the **Encryption Level** drop-down list, select the encryption level that was specified when the remote Tivoli server was installed.
5. If you specified an encryption level of **DES** or **Simple** in step 4, type the password in the **Password** text box.

Notes:

- a. If you specified an encryption level of **None** in step 4, no encryption key is necessary and the **Password** text box is not active.
 - b. For an interregion encryption level other than **None**, you must set the region interregion encryption password to connect successfully. To set the interregion encryption password, enter:

```
odadmin region set_region_pw
```
6. Specify the type of connection:
 - Select **One-way** to specify a one-way connection. Then select either **Make this server the manager** to make your local server the managing server, or select **Make other server the manager** to make your local server the managed server.
 - Select **Two-way** to specify a two-way connection.

7. Click **Connect & Close** to initiate the secure connection on the local server, or managing server. (If you are performing the connection on the managed server, skip to step 8.) The Confirm Connect window is displayed.



- a. Select **Update all resources immediately** if you want to exchange the resource information between the Tivoli regions immediately after the connection is made. If you do not select this option, you must exchange the resource information at a later time.
For troubleshooting purposes, it is recommended that you update resources at a later time.
- b. Click **Continue with Connection** to connect the two Tivoli regions.
8. An informational window reminding you that you must complete the secure connection operation on the other server is displayed.
9. Click **Continue** to acknowledge the message, close the window, and return to the Tivoli desktop.

After performing the preceding procedure on the first server being connected, you should repeat the procedure from the Tivoli desktop on the second server being connected.

To exchange resource information between the Tivoli regions, use the Top Level Policy Regions window. To access this windows, select **Local Level Policy Regions** from the **TMR Connection** menu of the Tivoli desktop. The Top Level Policy Regions windows provides access to the icons for the top-level policy regions in the Tivoli region to which you connected. From this window, you can drag and drop remote resources onto the appropriate local or remote administrator desktop. Refer to "Administrators and remote region resources" on page 62 for complete details.

Command line

For information about using the command line to make a secure connection, refer to the **wconnect** command in the *Tivoli Management Framework Reference Manual*.

Making a remote region connection

You can make a remote Tivoli region connection and specify the connection properties from the Tivoli desktop. When using this option, it is only necessary to perform this procedure on one of the Tivoli servers you are connecting. However, you will have to provide either the remote server root password or the password of a user on the server, or make use of the trusted host facility.

If you are making a remote one-way connection, you should perform this procedure on the server that will be the managing server. If you are making a remote two-way connection, it does not matter which server you perform the operation from.

The following table provides the context and authorization role required for this operation:

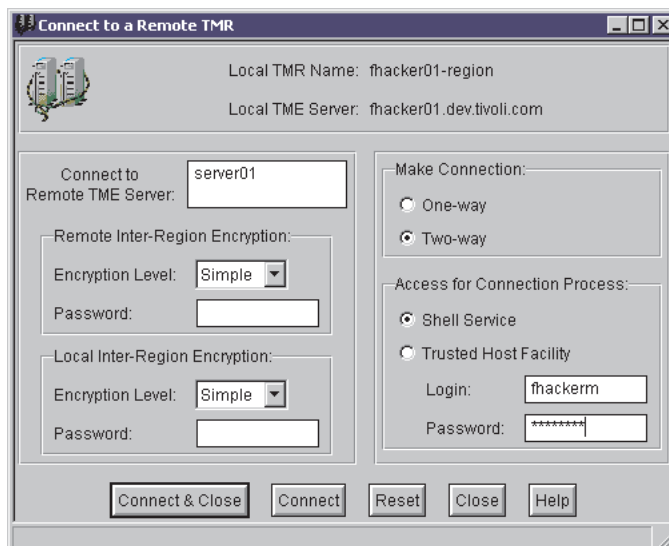
Activity	Context	Required role
Making a remote Tivoli region connection	Tivoli region	super

You can make a remote Tivoli region connection from either the Tivoli desktop or the command line.

Desktop

To make a remote connection, perform the following steps:

1. Select **TMR Connections** → **Connect** from the **Desktop** menu to display the Connect to a Remote TMR window:



2. Type the name of the server you want to connect to in the **Connect to Remote TME Server** text box.
3. In the **Remote Inter-region Encryption** group box, select the remote encryption level from the **Encryption Level** drop-down list. This encryption level is the level that was specified when the remote Tivoli server was installed. If you specified an encryption level of **DES** or **Simple**, type the password in the **Password** text box.

Notes:

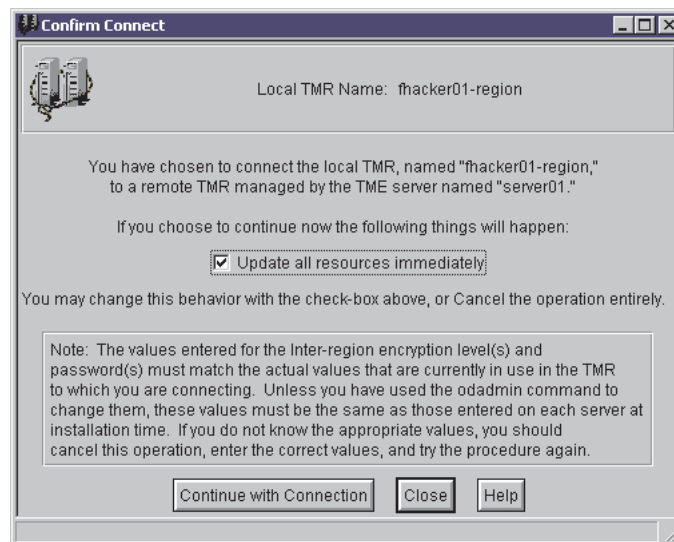
- a. If you specified an encryption level of **None**, no encryption key is necessary and the **Password** text box is not active.
- b. For an interregion encryption level other than **None**, you must set the region interregion encryption password to connect successfully. To set the interregion encryption password, enter:

```
odadmin region set_region_pw
```

4. In the **Local Inter-region Encryption** group box, select the local encryption level from the **Encryption Level** drop-down list. This encryption level is the level that was specified when the local Tivoli server was installed. If you specified an encryption level of **DES** or **Simple**, type the password in the **Password** text box.
5. If you specified a local encryption level of **DES** or **Simple** in step 4, type the local encryption password in the **Password** text box.

Note: If you selected a local encryption level of **None**, no encryption password is necessary and the **Password** text box is not active.

6. Click either **One-way** to specify a one-way connection or **Two-way** to specify a two-way connection. When a remote one-way connection is made, the server making the connection is the managing server.
7. Specify the access connection process:
 - Select **Shell Service** to set the remote access mechanism to be a shell service, and then perform the following steps:
 - a. Type a login name in the **Login** text box. The identified user must have the **super** role in the remote Tivoli region.
 - b. Type the password in the **Password** text box.
 - Select **Trusted Host Facility** to set the remote access mechanism to be a trusted host.
8. Click **Connect & Close** to initiate the remote connection. The Confirm Connect window is displayed.



- a. Select **Update all resources immediately** if you want to exchange the resource information between the Tivoli regions immediately after the connection is made. If you do not select this option, you must exchange the resource information at a later time.

- b. Click **Continue with Connection** to connect the two regions and return to the Tivoli desktop.

Note: If the remote Tivoli server refuses access, a window is displayed informing you of the access failure and the reason for the failure. You should either repeat this procedure with the correct information, correct the problem on the remote server, or make a secure connection on the Tivoli servers you are attempting to connect.

To exchange resource information between the Tivoli regions, use the Top Level Policy Regions window. To access this window, select **Local Level Policy Regions** from the **TMR Connection** menu of the Tivoli desktop. The Top Level Policy Regions window provides access to the icons for the top-level policy regions in the Tivoli region to which you connected. From this window, you can drag and drop remote resources onto the appropriate local or remote administrator desktop. Refer to “Administrators and remote region resources” on page 62 for complete details.

Command line

For information about using the command line to make a remote connection, refer to the **wconnect** command in the *Tivoli Management Framework Reference Manual*.

Determining the status of region connections

You can determine the current status of a Tivoli region connection from the Tivoli desktop. You can also determine which other servers are connected to the local server and whether a particular connection is one-way or two-way.

The following table provides the context and authorization role required for this operation:

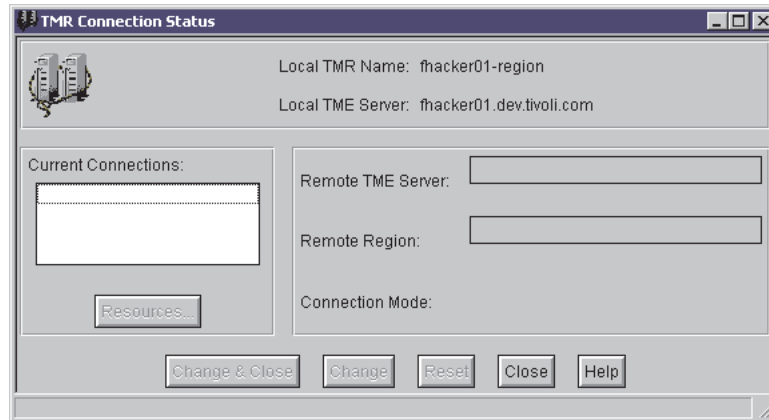
Activity	Context	Required role
Determining the status of Tivoli region connections	Tivoli region	senior

You can determine the status of a Tivoli region connection from either the Tivoli desktop or the command line.

Desktop

To display the current status of a Tivoli region connection, perform the following steps:

1. Select **TMR Connections → List Connections** from the **Desktop** menu to display the TMR Connection Status window. The local server name and local region are displayed at the top of the window.



Note: This window is read only; you cannot edit the information. Tivoli Management Framework does not support changing connection parameters.

2. From the **Current Connections** scrolling list, select an entry for which you want status information. The connection status is displayed to the right.
3. Click **Close** to close this window and return to the Tivoli desktop.

Command line

For information about using the command line to display the current status of a Tivoli region connection, refer to the **wlsconn** command in the *Tivoli Management Framework Reference Manual*.

Administrators and remote region resources

When two or more Tivoli regions are connected, the locally defined Tivoli administrators in either one or both regions are exchanged and placed in the Administrators collection in the other region. As a result, you can drag and drop resources from one Tivoli region to the Tivoli desktop of a remotely defined administrator or from the Tivoli desktop of a remotely defined administrator to another region.

After the authorization roles are updated for an administrator who has had one or more remote resources placed on his or her Tivoli desktop, the administrator can manage the resources as if they were defined locally.

The following table provides the context and authorization roles required for these operations:

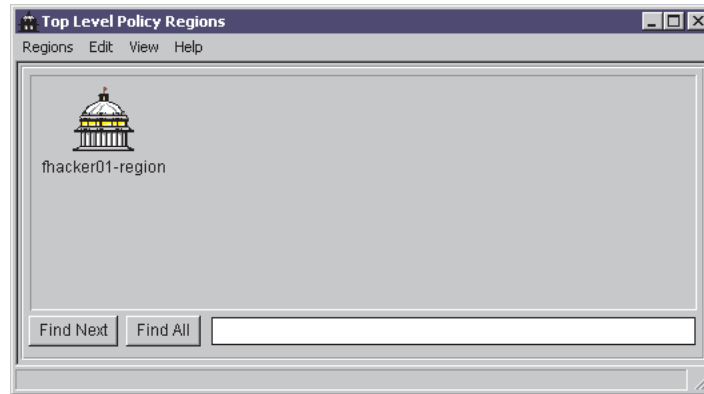
Activity	Context	Required role
Dragging and dropping local resources onto a remote administrator Tivoli desktop	Tivoli region	user
Dragging and dropping remote resources onto a local administrator Tivoli desktop	Tivoli region	user

You can update the resources on either a local or remote administrator desktop from the Tivoli desktop only.

Desktop

To update the resources to which an administrator has access, perform the following steps:

1. Select **TMR Connections → Top Level Policy Regions** from the **Desktop** menu to display the Top Level Policy Regions window.



2. Select the top-level policy regions in the remote Tivoli region to which you want an administrator to have access.
3. Follow the procedure described in “Managing resources for administrators” on page 40 to place the selected top-level policy regions on the Tivoli desktop of the administrator.
4. Ensure that the administrator has been given one or more resource roles for the top-level policy regions added to his desktop. Refer to the procedure described in “Creating a Tivoli administrator” on page 35 for details.

Exchanging or updating resource information

After connecting two or more Tivoli regions, immediately exchange resource information between them. After the initial exchange, this information should be updated on a regular basis. The frequency of these updates depends on the stability of your installation. For example, during the initial phase of deployment, clients and resources might be added frequently, requiring you to update the resource information more than once a day. As the environment stabilizes and enters production, updating resources once a day should be sufficient.

Resource updates are resource-intensive and should not be scheduled too frequently to avoid causing performance problems in your environment. In general, do not update all resources more frequently than once every couple of hours. If you must access a new resource immediately, update only that resource type and not all types. Also, be sure that one update completes before the next begins.

Refer to the appropriate Tivoli application documentation for listings of which resources should be exchanged for each application.

You can update resources from either the Update Resources from Multiple TMRs window or the TMR Connection Status window. However, you can schedule updates from the Update Resources from Multiple TMRs window only.

The following table provides the context and authorization role required for this operation:

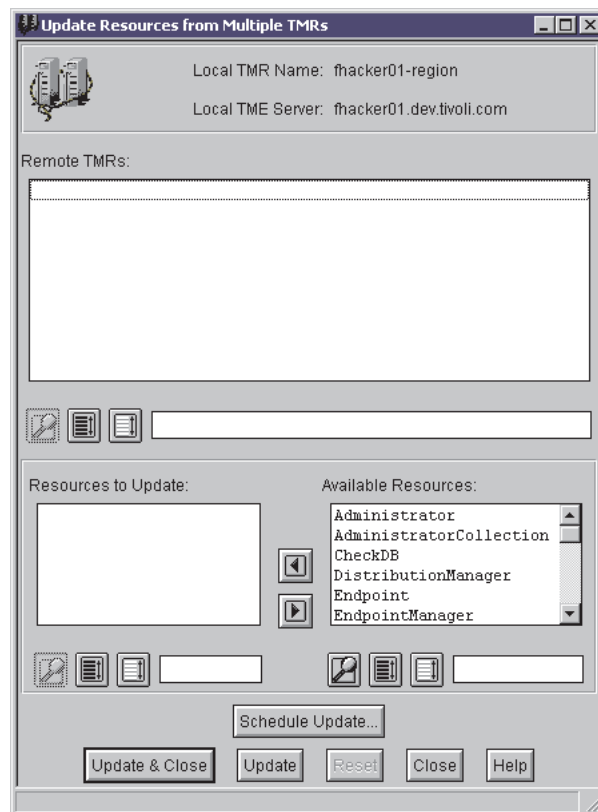
Activity	Context	Required role
Exchanging or updating Tivoli region information	Tivoli region	senior

You can exchange or update resource information across connected Tivoli regions from either the Tivoli desktop or the command line.

Desktop, from multiple regions

To exchange resource information between two Tivoli regions, perform the following steps:

1. Select **TMR Connections** → **Update Resources** from the **Desktop** menu to display the Update Resources from Multiple TMRs window.



2. Select one or more remote Tivoli regions from the **Remote TMRs** scrolling list.
3. Select one or more resource types to be updated from the **Available Resources** scrolling list and click the left-arrow button. The selected resource types are moved to the **Resources to Update** scrolling list.

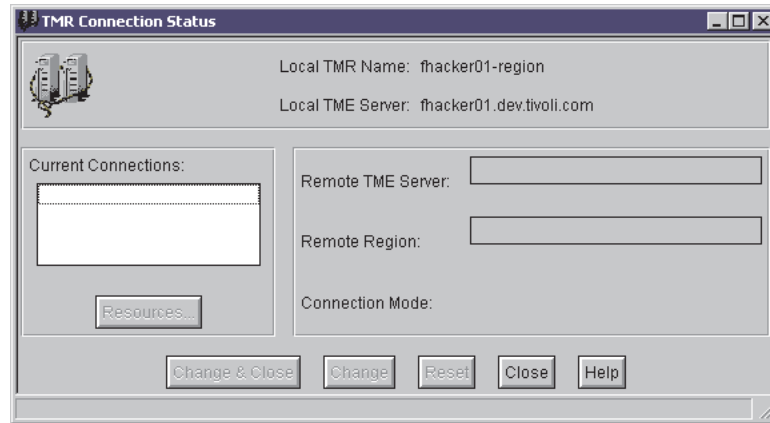
You can also double-click an entry to move it automatically to the **Resources to Update** scrolling list.

4. To schedule the information update on a regular basis or for some time in the future when system activity is lower, click **Schedule Update**. Refer to Chapter 10, "Scheduling jobs," on page 129 for details about scheduling jobs.
5. Click **Update & Close** to immediately update the resource information for the specified resource types in the selected Tivoli regions and return to the Tivoli desktop.

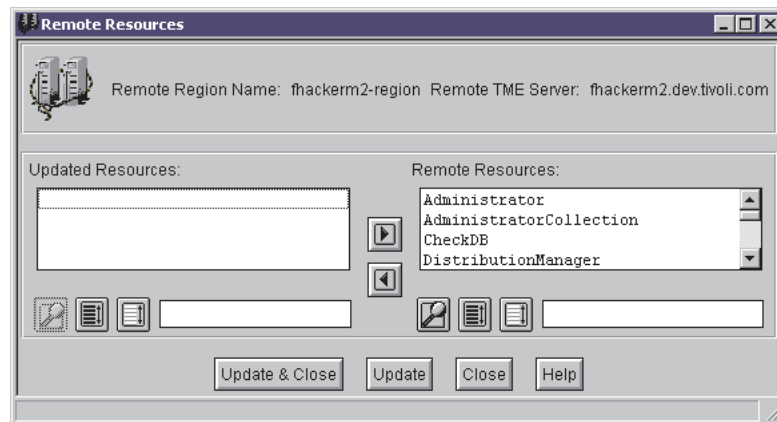
Desktop, from connection status

To exchange resource information between two Tivoli regions by using the **TMR Connection Status** window, perform the following steps:

1. Select **TMR Connections → List Connections** from the **Desktop** menu to display the TMR Connection Status window. The local server name and local region are displayed at the top of the window.



2. Select an entry from the **Current Connections** scrolling list for which you want to exchange resource information. The connection status is displayed to the right.
3. Click **Resources** to display the Remote Resources window.



4. To perform an information exchange, select one or more resources from the **Remote Resources** list and click the left-arrow button. The selected resource types are moved to the **Updated Resources** scrolling list.
You can also double-click an entry to move it automatically to the **Updated Resources** scrolling list.
5. Click **Update & Close** to update the resource information and close the Remote Resources window.

Command line

For information about using the command line to exchange information between two Tivoli regions, refer to the **wupdate** command in the *Tivoli Management Framework Reference Manual*.

Forcing an update to override time stamps

Each resource type in the name registry carries a time stamp. The time stamp is updated every time there is a change to a local instance of that resource type. This includes when a new instance of that resource type is added, an existing instance of that resource type has its information changed, or an instance of that resource type is removed.

In connected Tivoli regions, each interregion resource type object maintains a per-region/per-resource type time stamp as well. This allows each region to know when it last received an update of that specific resource type from that specific remote region. This per-region/per-resource type time stamp is used to determine whether an actual update of a resource type in some remote region is actually necessary.

If you want to force an update of resources, regardless of the time stamp, use the **wupdate -f** command. Refer to the *Tivoli Management Framework Reference Manual* for more information about the **wupdate** command.

Updating all resources

A common operation is to update all resource types from a single remote Tivoli region or to update a single resource type from all connected remote regions. You can update all resources from the command line using the **wupdate** command. Refer to the *Tivoli Management Framework Reference Manual* for usage and examples of the **wupdate** command.

You can update all resource types from the Tivoli desktop by selecting all resources from the **Available Resources** scrolling list. To update from all connected Tivoli regions, select all regions from the **Remote TMRs** scrolling list in the Update Resources from Multiple TMRs window.

Disconnecting regions

You can disconnect two Tivoli regions; however, before doing so, you should consider your system configuration. Also, whenever you disconnect two regions, you should always run the **wchkdb -ux** command in each region to clean up any dangling object references. Refer to the **wchkdb** command in the *Tivoli Management Framework Reference Manual* for more details.

The following table provides the context and authorization role required for this operation:

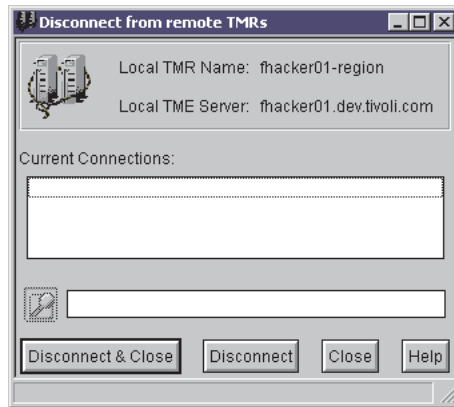
Activity	Context	Required role
Disconnecting Tivoli regions	Tivoli region	super

You can disconnect Tivoli regions from either the Tivoli desktop or the command line.

Desktop

To disconnect two Tivoli regions, perform the following steps:

1. Select **TMR Connections → Disconnect** from the **Desktop** menu to display the Disconnect from Remote TMRs window:



2. Select the current connection you want to disconnect in the **Current Connections** scrolling list.
3. Click **Disconnect & Close**. A confirmation window is displayed.
4. Click **Yes** to continue the disconnection.
5. Run the **wchkdb -ux** command to ensure database consistency and repair any object references across region boundaries.

Command line

For information about using the command line to disconnect two Tivoli regions, refer to the **wdisconn** command in the *Tivoli Management Framework Reference Manual*.

Chapter 5. Policies and policy regions

A *policy* is a written rule that you put into effect for a system and that Tivoli Management Framework enforces as management operations are performed by administrators. Management operations are enforced using default policies and validation policies.

Tivoli Management Framework maintains and enforces policies within policy regions. A *policy region* is a special collection of resources that share one or more common policies.

A *default policy* is a set of default resource property values that are assigned to a resource when the resource is created. You can accept these default values or you can edit them in the resource properties. See Chapter 6, “Profiles and profile managers,” on page 79 for information about profile policies. A *validation policy* ensures that all resources in a policy region comply with the establish policy for the region. A validation policy prevents Tivoli administrators from creating or modifying resources that do not conform to the validation policy of the policy region in which the resources are created. A validation policy also ensures that modification of any resource is done only in a policy-compliant manner.

For information about creating and editing default policies that are not profile-based and for information about creating and editing validation policies, see *Tivoli Management Framework Reference Manual*.

Working with Policy Region icons

The set of managed resources accessible from the local Tivoli region and any connected regions are grouped and displayed within one or more policy regions.

The pop-up menu of a Policy Region icon identifies the policy region and includes the following options:

Open Opens the policy region view and shows any Tivoli resources that are members of the policy region

Region Properties

Displays the window where you can change the name of the policy region

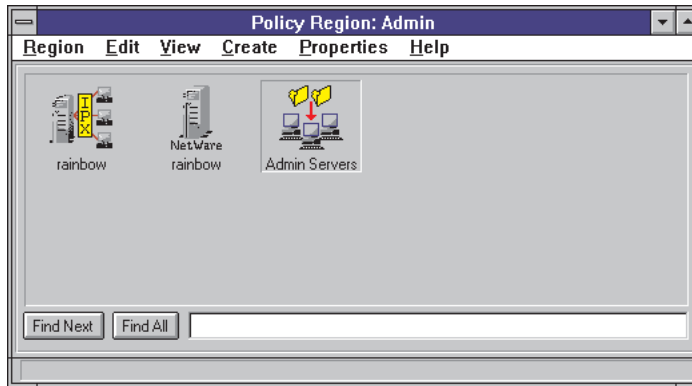
Managed Resources

Displays the window where you can define valid resource types for the policy region

Managed Resource Policies

Displays the window where you can change the policy for one or more managed resource types within the context of the policy region

To view the set of managed resources within a policy region, open the appropriate policy region on the Tivoli desktop. A window similar to the following one, with an icon for each managed resource, is displayed.



Creating a top-level policy region

There are two types of policy regions that you can create: top-level policy regions and subregions. Top-level policy regions are useful for organizing the managed resources into broad organizational categories. Top-level policies regions are used to contain managed resources, including policies subregions. In addition, top-level policy regions are visible across Tivoli regions and can be used to allow local administrators to manage remote machines.

The following table provides the context and authorization roles required for this operation:

Activity	Context	Required role
Creating a top-level policy region	Tivoli region	senior
Creating a top-level policy region and adding a resource	Tivoli region	senior and policy

You can create a top-level policy region from either the Tivoli desktop or the command line.

Desktop

To create a top-level policy region, perform the following steps:

1. In the Tivoli desktop, select **Region** from the **Create** menu to display the Create Policy Region window:



2. In the **Name** text box, type the name for the new top-level policy region. The policy region name must be unique within the local Tivoli region.
The name of a policy region can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.

3. Click **Create & Close** to create the new policy region and return to the Tivoli desktop.

Command line

For information about using the command line to create a policy region, see the **wcrtpr** command in *Tivoli Management Framework Reference Manual*.

Creating a policy subregion

After the top-level policy regions are defined, you can create subregions under them to further categorize and define administrative authority and policy within your organization. Each policy region can contain an arbitrary grouping of managed resources. For example, you can create a policy region that contains all the machines in the Engineering group.

The following table provides the context and authorization roles required for this operation:

Activity	Context	Required role
Creating a policy subregion	Tivoli region	senior
Creating policy subregion and adding a resource	Tivoli region	senior and policy

You can create a policy subregion in a policy region from either the Tivoli desktop or the command line.

Desktop

To create a policy subregion in a policy region, perform the following steps:

1. In a Policy Region window, select **Subregion** from the **Create** menu to display the Create Policy Region window:



2. In the **Name** text box, type the name for the new policy subregion. The policy subregion name must be unique within its policy region.
The name of a policy region can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.
3. Click **Create & Close** to create the new policy subregion and return to the Policy Region window.

Command line

For information about using the command line to create a policy subregion, see the **wcrtpr** command in *Tivoli Management Framework Reference Manual*.

Changing the name of a policy region

Each policy region, top-level and subregion, has a name that uniquely identifies it in the local Tivoli region. You can change this name at any time.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Changing the name of a policy region	Policy region	senior

You can change the name of a policy region from the Tivoli desktop only.

To change the name of a policy region, perform the following steps:

1. In the Policy Region window, select **Policy Region** from the **Properties** menu to display the Policy Region Properties window.



2. In the **Name** text box, type a new name for the policy region.
The name of a policy region can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.
3. Click **Set & Close** to change the name of the policy region and close the window.

Modifying managed resource types in policy regions

Each policy region maintains a list of managed resource types that are valid or defined for that specific policy region. You can add or remove managed resource types at any time.

The following table provides the context and authorization roles required for this operation:

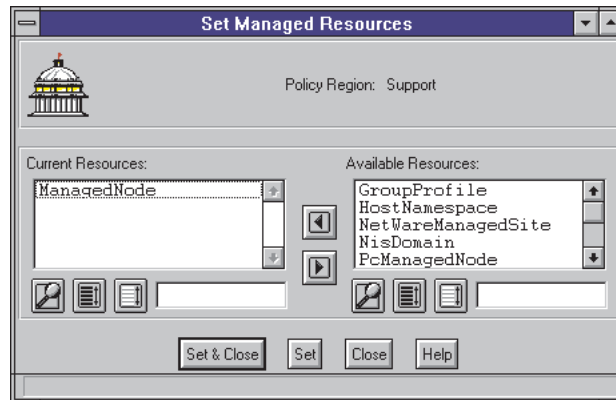
Activity	Context	Required role
Modifying managed resource types in a policy region	Policy region	senior and policy

You can modify the set of managed resource types in a policy region from either the Tivoli desktop or the command line.

Desktop

To modify the set of valid managed resource type in a policy region, perform the following steps:

1. In the Policy Region window, select **Managed Resources** from the **Properties** menu to display the Set Managed Resources window:



The **Current Resources** scrolling list displays the current managed resource types. The **Available Resources** scrolling list displays the available managed resource types.

2. Add or remove managed resource types.

To add managed resource types to the policy region, select one or more managed resource types from the **Available Resources** scrolling list and click the left-arrow button. The selected managed resource types are moved to the **Current Resources** scrolling list.

To remove managed resource types from the policy region, select one or more managed resource types from the **Current Resources** scrolling list and click the right-arrow button. The selected managed resource types are moved to the **Available Resources** scrolling list.

You can also double-click an entry in the either scrolling list to move it to the other scrolling list.

3. Click **Set & Close** to modify the selected managed resource types in the policy region and to return to the Policy Region window.

When you add a managed resource type to a policy region, the managed resource type inherits the basic default policy defined for that resource type. The managed resource type is made available to the policy region **Create** menu so that you can create new instances of the managed resource in the policy region.

Command line

For information about using the command line to examine and change the managed resource types of a policy region, see the **wgetpr** and **wsetpr** commands in *Tivoli Management Framework Reference Manual*.

Assigning policies to resources types

Each managed resource type has a defined default policy that it inherits when added to a policy region. You can then change the default policy of a resource type after it is added. Policies are usually shell scripts that are used to implement policy criteria. These criteria are then applied to policy region resources. You can also create your own policy implementations and assign them to policy region resources.

The following table provides the context and authorization roles required for this operation:

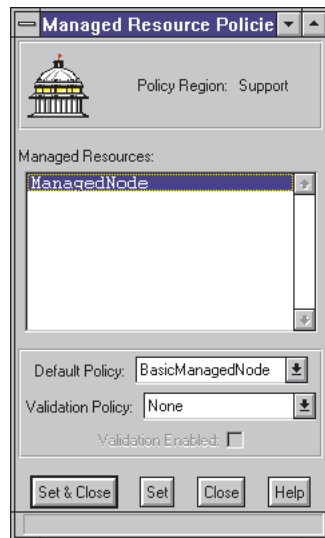
Activity	Context	Required role
Assigning policy for a managed resource type	Policy region	senior and policy

You can assign policies to a resource in a policy region from either the Tivoli desktop or the command line.

Desktop

To assign a new policy to a managed resource type, perform the following steps:

1. In the Policy Region window, select **Managed Resource Policies** from the **Properties** menu to display the Managed Resources Policies window:



The **Managed Resources** scrolling list displays the managed resources defined for the policy region.

2. From the **Managed Resources** scrolling list, select a managed resource type. The current default and validation policies of the selected resource type are displayed.
3. From the **Default Policy** drop-down list, select a default policy for the resource type.

Note: If you change the default policy of a managed resource type to **None**, you can no longer create objects of that type in the policy region. Nor can you move any existing objects of this type into the policy region, although the resource type is defined as a managed resource type.

4. From the **Validation Policy** drop-down list, select a validation policy for the resource type.
5. Select **Validation Enabled** to enable or disable the validation policy for the resource type.
6. Click **Set & Close** to assign the new policy to the selected managed resource type and to close the Policy Region window.

When you change the default policy of a managed resource type, Tivoli Management Framework begins using the new default policy the next time a new instance of the resource type is created.

Similarly, when you change the validation policy of a managed resource type, Tivoli Management Framework begins using the new validation policy the next time an operation is performed. Existing objects are not reevaluated to determine whether they valid against the newly defined criteria.

Command line

For information about using the command line to change the managed resource polices of a policy region, see the **wgetpr** and **wsetpr** commands in *Tivoli Management Framework Reference Manual*.

Validating resources in policy regions

You can identify any policy region resources that do not conform to the polices of the current policy region.

When you move a resource from one policy region to another, the resource retains the properties of the policy region in which the resource was created or last modified. Tivoli Management Framework does not validate resource properties automatically when a resource is moved to a different policy region. Therefore, the properties of a resource that is moved to another policy region might not conform to the policies of the new policy region.

Also, if the validation policies of a policy region is changed after a resource was created or last modified, the resource might not conform to the current policies of the policy region.

The following table provides the context and authorization role required for this operation:

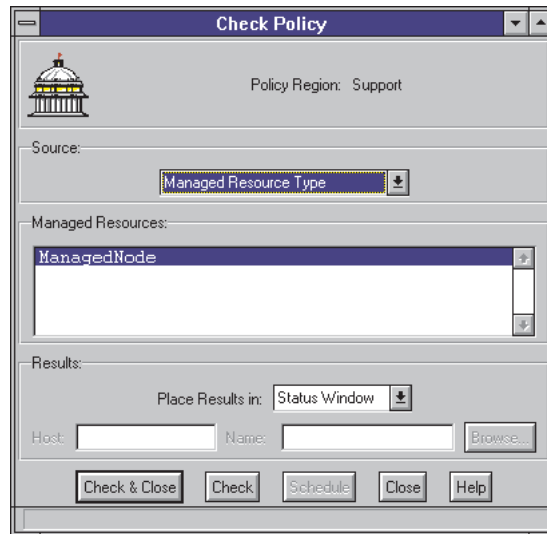
Activity	Context	Required role
Validating changed policy in a policy region	Policy region	admin

You can check the policy of resources within the policy region from either the Tivoli desktop or the command line.

Desktop

To determine which policy region resources do not conform to the current policies, perform the following steps:

1. In the Policy Region, select **Check Policy** from the **Region** menu to display the Check Policy window:



2. Check the validation policy.
 - To check the validation policy against a specific resource type, ensure that **Managed Resource Type** is selected from the **Source** drop-down list and select a resource type from the **Managed Resources** scrolling list.
 - To check the validation policies against all resource types, select **All Members of the Policy Region** from the **Source** drop-down list.
3. Select where the results are placed by selecting one of the following options from the **Place Results in** drop-down list:

Status Window

Displays results in a window.

Collection

Places the icon of any resource that fails the policy validation in a collection on the Tivoli desktop.

When you select **Collection**, the **Name** text box is made available. Type the name of the collection where the icons should be placed. If the collection does not already exist, a new one is created.

Text File

Writes the name of any resource that fails the policy validation to a file on a managed node.

When you select **Text File**, the **Host** and **Name** text boxes and the **Browse** button become available. In the **Host** text box, type the name of the managed node where the file is to be written. In the **Name** text box, type the full path name for the file. You can also click the **Browse** button to use the file browser to specify the machine and file name in which the results are to be written.

4. If you want to schedule policy checking on a regular basis or for some time in the future when system activity is lower, click **Schedule**. See Chapter 10, "Scheduling jobs," on page 129 for details on scheduling jobs.
5. Click **Check & Close** to validate the specified resources and return to the Policy Region window.

Command line

For information about using the command line to determine which policy region resources do not conform to the current policies of a policy region, see the **wchkpol** command in *Tivoli Management Framework Reference Manual*.

Chapter 6. Profiles and profile managers

In large distributed networks, machines are frequently grouped according to the type of work for which they are used. For example, machines in an engineering group might be used to produce Computer Aided Design (CAD) drawings, while those in an accounting group might be used to produce tax documents. With Tivoli Management Framework, you can place common configuration information for machines used for similar purposes in a centralized area. Doing so makes it easier to access, manage, and duplicate resources. Profiles and profile managers allow you to do this.

A *profile* is a collection of information associated with a specific Tivoli application. Each item in a profile contains system configuration information. The information in a profile is specific to the particular profile type. Profile records are stored in a platform-independent format that allows the same profile records to be distributed across an environment that contains multiple operating system types.

A *profile manager* is a container for individual profiles. It provides a place to create and organize groups of profiles and to link targets (*subscribers*) to them. A profile manager can contain multiple profiles of the same type, or it can contain profiles of more than one type. Profile managers control the distribution of profiles to subscribers.

Working with Profile Manager icons

The Profile Manager icons are displayed in any Policy Region window in the Tivoli desktop. There are two Profile Manager icons, one for database profile managers and another for dataless profile managers. The pop-up menu of either Profile Manager icon includes the following options:

Open Opens the Profile Manager window and displays icons for the defined profiles and subscribers

Distribute

Distributes the defined profiles to the defined subscribers

Get New Copy

Displays the window where you can get new copies of profiles already defined for the profile manager

Subscribers

Displays the window where you can add subscribers to the profile manager.

Subscriptions

Displays the windows where you can view the profiles defined to the profile manager.

Creating a profile manager

You can create a profile manager within a policy region.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Creating a profile manager	Policy region	senior

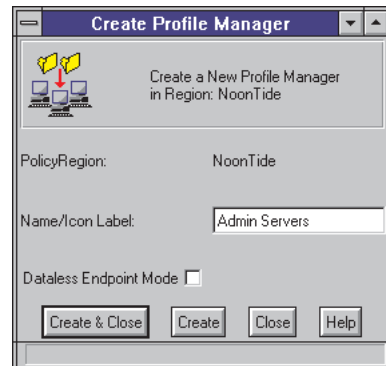
You can create a profile manager from either the Tivoli desktop or the command line.

Desktop

To create a profile manager, perform the following steps:

1. In a Policy Region window, select **Profile Manager** from the **Create** menu to display the Create Profile Manager window.

If there is no entry on the **Create** menu for creating a profile manager, you must first add **Profile Manager** as a managed resource type for the policy region. See “Modifying managed resource types in policy regions” on page 72 for more information about adding or removing managed resources from a policy region.



2. In the **Name/Icon Label** text box, type the name for the profile manager.
The name of a Tivoli resource, such as a profile manager, can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.
3. Select **Dataless Endpoint Mode** if this profile manager needs to distribute profiles to endpoints. If **Dataless Endpoint Mode** is selected, the profile manager can distribute to endpoints and managed nodes, but *not* to other profile managers. If this mode is not selected, the profile manager can distribute to profile managers and managed nodes, but *not* to endpoints.
4. Click **Create & Close** to create the profile manager and return to the policy region window. The new Profile Manager icon is displayed in the Policy Region window.

Command line

For information about using the command line to create a profile manager, see the **wcrtprfmgr** command in *Tivoli Management Framework Reference Manual*.

Modifying subscribers

Subscribing targets to a profile manager determines which resources will receive a profile when it is distributed.

Distributing profiles to subscribers enables you to maintain control of some system management operations, while delegating other operations to lower management levels. Depending on the restrictions you place on the profile, other administrators can modify selected profile attributes before further distributing the profile to endpoints in their management areas.

Note: To subscribe to a profile manager, both the profile manager being subscribed to and the subscribing target must conform to the necessary subscription validation policies.

When a subscriber is removed from a profile manager, that subscriber will no longer receive profile distributions from the profile manager. To remove a subscriber from a profile manager, both the profile manager subscribed to and the subscribing target must conform to the necessary subscription removal validation policies.

When you remove a subscriber, you can choose to keep all copies of the profiles from that point on down the subscription hierarchy, or you can delete all copies of profiles. If you choose to keep the copies, they will become original profiles.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Modifying subscribers of a profile manager	Policy region of the profile manager and the policy region of the subscriber	admin

You can add subscribers to a profile manager using drag and drop, from the Tivoli desktop, or from the command line. You can remove a subscriber from either the Tivoli desktop or the command line.

Adding a subscriber using drag and drop

To subscribe a target to a profile manager using drag and drop, perform the following steps:

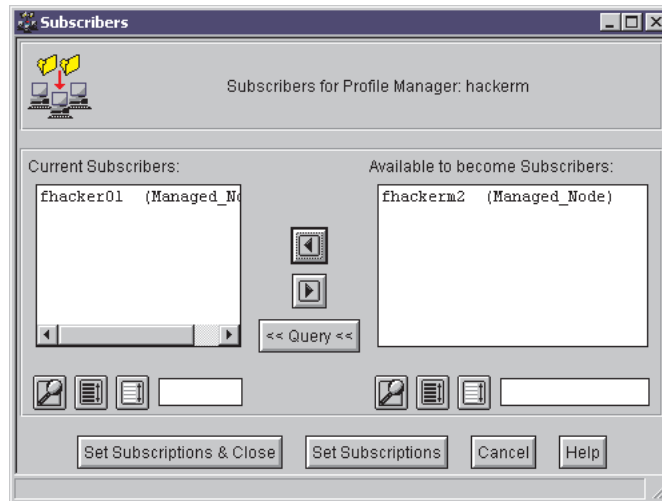
1. Select the icon of the target that you want to subscribe to a profile manager. These icons can be found on the Tivoli desktop.
2. Drag the selected icon and drop it on the Profile Manager icon, or drag the selected icon and drop it in the subscriber area of the Profile Manager window.

The selected target is subscribed to the profile manager.

Desktop

To remove a subscriber to a profile manager, perform the following steps:

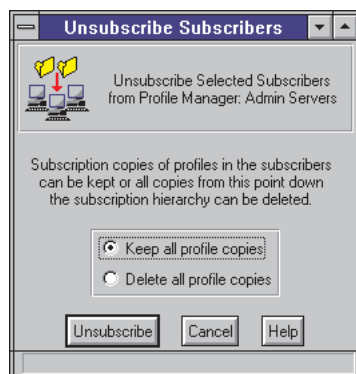
1. In a Policy Region window, right-click a Profile Manager icon and select **Subscribers** to display the Subscribers window:



The **Current Subscribers** scrolling list displays a list of all targets that are subscribed to the current profile manager.

You can modify the resource types that can be subscribers by modifying the **pm_def_subscribers** default policy. See *Tivoli Management Framework Reference Manual* for instructions.

2. Modify the subscribers:
 - To add subscribers, select one or more targets in the **Current Subscribers** scrolling list, and click the right-arrow button. The selected targets are moved to the **Available to become Subscribers** scrolling list.
 - To remove subscribers, select one or more targets in the **Available to become Subscribers** scrolling list, and click the left-arrow button. The selected targets are moved to the **Current Subscribers** scrolling list.
 - Double-click an entry in one list to move it to the other list.
3. Click **Set Subscriptions & Close** to update the subscribers.
4. If removing a subscriber and it is associated with a profile type that uses local profile copies, the Unsubscribe Subscribers window is displayed:



5. Keep or delete the local copies of the profiles.

Select **Keep all profile copies** to keep the local copy of each profile at each subscriber. These copies will become the equivalent of the original profiles.

Select **Delete all profile copies** to remove all traces of the local copy of each profile at each subscriber. The local copy of each profile is removed from subscribers at all subscription levels down to the final target.

6. Click **Unsubscribe** to remove the subscribers and return to the Policy Region window.

Command line

To adding subscribers to a profile manager, use the **wsusb** command. To remove subscribers from a profile manager, use the **wunsub** command. For information about these commands, see *Tivoli Management Framework Reference Manual*.

Editing a profile manager

You can change the name of a profile manager or change the mode in which the profile manager operates.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Editing a profile manager	Policy region	senior

You can edit the name of a profile manager from the Tivoli desktop only. You can, however, change the operating mode using either the Tivoli desktop or the command line.

Desktop

To edit a profile manager, perform the following steps:

1. In a Policy Region window, double-click a Profile Manager icon to open the Profile Manager window.
2. From the **Edit** menu, select **Profile Manager** to display the Edit Profile Manager window:



3. In the **Name/Icon Label** text box, edit the name for the profile manager.
The name of a Tivoli resource, such as a profile manager, can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.
4. Edit the mode in which the profile manager will operate. If **Dataless Endpoint Mode** is selected, the profile manager can distribute to endpoints and managed nodes, but not to other profile managers. If this mode is not selected, the profile manager can distribute to other profile managers and managed nodes, but not to endpoints.
5. Click **Change & Close** to update the profile manager name and return to the Profile Manager window.

Command line

For information about using the command line to change the operating mode of a profile manager, see the **wsetpm** command in *Tivoli Management Framework Reference Manual*.

Deleting a profile manager

Before you can delete a profile manager, you must remove all subscribers from the profile manager. (See “Modifying subscribers” on page 80 for instructions.) You must also delete any original profiles from the profile manager. An original profile is any profile that is not a distributed copy. If you attempt to delete a profile manager that contains original profiles, an error message is generated and the operation fails. If the profile manager contains copies of profiles, the copies will be deleted.

You can delete profile managers from the Tivoli desktop or the command line.

Desktop

To delete a profile manager, perform the following steps:

1. In a Policy Region window, select the icon for the profile manager you want to delete.
2. From the **Edit** menu, select **Delete**.

Command line

For information about using the command line to delete a profile manager, see the **wdel** command in *Tivoli Management Framework Reference Manual*.

Creating profiles

You can create a profile from a profile manager. Because each profile type has different steps, the following procedure is the generic process for creating a profile.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Creating profiles from a profile manager	Profile manager	senior

You can create profiles from either the Tivoli desktop or from the command line.

Desktop

To create a profile, perform the following steps:

1. In a Policy Region window, double-click a Profile Manager icon to open the Profile Manager window.
2. From the **Create** menu, select **Profile** to display the Create Profile window.
3. In the **Name/Icon Label** text box, type the name for the new profile.

The name of a Tivoli resource, such as a profile, can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.

4. From the **Type** scrolling list, select the type of profile you want to create.

Note: The list of available profile types is controlled by the policy region containing the profile manager and is dependent on the applications installed. See “Modifying managed resource types in policy regions” on page 72 for information about selecting policy region resource types.

5. Click **Create & Close** to create the specified profile and return to the Profile Manager window.

Command line

For information about using the command line to create profiles in a profile manager, see the **wcrtprf** command in *Tivoli Management Framework Reference Manual*.

Distributing profiles

You can use the default distribution parameters to distribute profiles from a profile manager.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Distributing profiles from a profile manager	Profile manager	admin

You can distribute profiles using drag and drop, from the Tivoli desktop, or from the command line.

Distributing profiles using drag and drop

To distribute a profile using drag and drop, perform the following steps:

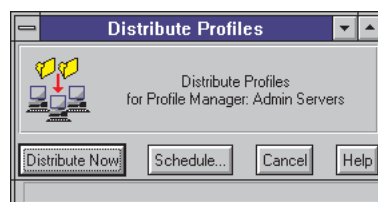
1. In the Profile Manager window, select one or more Profile icons.
2. Drag the Profile icon and drop it on the icon for the target. The icon for the target and Profile icon must be in the same Profile Manager window.

The selected profile is distributed to the target using the default distribution parameters.

Desktop

To distribute profiles using the Tivoli desktop, perform the following steps:

1. In the Policy Region window, double-click a Profile Manager icon to open the Profile Manager window.
2. Select one or more Profile icons.
3. Select one or more icons in the **Subscribers** area.
4. From the **Profile Manager** menu, select **Distribute** to display the Distribute Profiles window:



5. Distribute or schedule the distribution of profiles.
 - Click **Distribute Now** to distribute the profiles to the selected subscribers immediately and return to the Profile Manager window.
 - Click **Schedule** to schedule the distribution for a later time. For information about how to schedule a job, see Chapter 10, “Scheduling jobs,” on page 129.

Command line

For information about using the command line to distribute profiles from a profile manager, see the **wdistrib** command in *Tivoli Management Framework Reference Manual*.

Synchronizing profiles with a target

A profile might not always match the current system files and databases on a particular managed node or other target. This can happen, for example, if someone edits a system file directly instead of using Tivoli Management Framework. You can synchronize the information in a profile with the system files on a target so that the profiles accurately reflect the current configuration of the target.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Synchronizing profiles with a target	Policy region	admin

You can synchronize profiles with the target from either the Tivoli desktop or the command line.

Desktop

To synchronize profiles with the current system files and database of the target, perform the following steps:

1. In the Policy Region window, select **Synchronize** from the **Managed Node** menu to display the Synchronize Profiles window.
2. Select the type of profile you want to synchronize from the **Available Profile Types** scrolling list. The contents of this list depends on the applications installed in the Tivoli region. You can synchronize only one type of profile at a time.
3. Click **Synchronize** to display the Profile/System Discrepancies window. This window and its contents differ depending on the profile type selected in the previous step.

The Profile/System Discrepancies window displays the following differences between profiles and the files and database on the target:

- Profile items that exist in a profile database, but not in the files and database on the target
 - Items that exist in the files and database on the target, but not in a profile database
 - Items that differ between the files and database on the target and the profile database itself
4. Click **Commit Changes** to synchronize the profile databases with the files and database on the target. Items in a profile database that do not exist in the files

and database on the target are deleted from the profile database. For items that differ between the files and database on the target and the profile database itself, the profile database is modified to match the files and database on the target. For items that exist in the files and database on the target but not in a profile database, you must choose the profile to which to add the items.

5. Click **Cancel** to return to the Policy Region window.

Copying profiles from a profile manager

When you copy a profile from a profile manager, an exact copy of the original profile in the profile manager is made.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Copying profiles from a profile manager	Profile manager	senior

You can copy profiles from the Tivoli desktop using drag and drop only.

Copying profiles using drag and drop

To copy profiles from a profile manager using drag and drop, perform the following steps:

1. Open the profile manager window of both the profile manager containing the profile (source profile manager) and the profile manager to which you want to copy the profile (destination profile manager).

Note: You must have both profile manager windows open to perform this activity.

2. In the source profile manager window, select the icon or icons of the profiles you want to copy.
3. Drag the icons to the **Profiles** area of the destination profile manager window.
4. Drop the icons. The selected profiles are copied to the profile manager.

The name of the new profile is *original_profile_name.dup@dest_profile_manager*.

Cloning profiles from a profile manager

Cloning a profile creates a new profile that contains the same policy definitions as the original profile. Cloning does not replicate the information contained in individual profile items (for example, data contained in fields). You can clone a profile from the Tivoli desktop only.

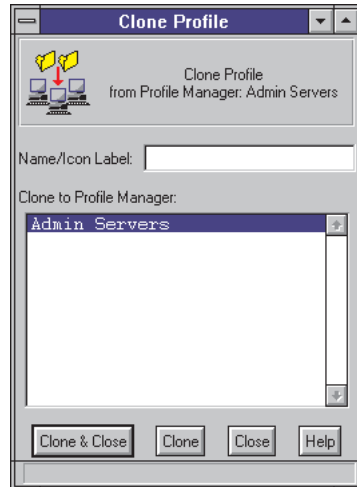
The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Cloning profiles from a profile manager	Profile manager	admin

Desktop

To clone profiles, perform the following steps:

1. In a Profile Manager window, double-click the Profile Manager icon to display the Profile Manager window.
2. Select a Profile icon.
3. From the **Edit** menu, select **Profiles → Clone** to display the Clone Profile window:



4. In the **Name/Icon Label** text box, type the name for the new profile.
The name of a Tivoli resource, such as a profile, can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.
5. Select the profile manager in which you want the copy to be placed from the **Clone to Profile Manager** scrolling list.
6. Click **Clone & Close** to clone the profile and return to the Profile Manager window. The new Profile icon is displayed in the Profile Manager window.

Moving profiles between profile managers

When you move a profile from one profile manager to another, you are actually deleting the profile from one profile manager and inserting it in another. The profile is not only deleted from the profile manager, it is deleted from *all* subscribers to the profile manager. Before moving a profile, you should consider the effects of deleting the profile from the profile manager where it is currently located.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Moving profiles from a profile manager	Profile manager	admin

You can move profiles from the Tivoli desktop using drag and drop only.

To move profiles from one profile manager to another profile manager, perform the following steps:

1. Open the profile manager window of both the profile manager containing the profile (source profile manager) and the profile manager to which you want to move the profile (destination profile manager).

Note: You must have both profile manager windows open to perform this activity.

2. In the source profile manager window, press and hold the Shift key while clicking the icon or icons of the profiles you want to move.

Note: If you do not hold the Shift key, the profiles will be copied, not moved.

3. Drag the icons to the **Profiles** area of the destination profile manager window.
4. Release the mouse button and the Shift key. The profiles are moved from the original profile manager and pasted in the destination profile manager.

Deleting profiles from a profile manager

Only original profiles can be deleted. When you delete an original profile, you also delete all copies of the profile existing lower in the hierarchy in any subsequent distributions. Also, any configuration information that was stored in the deleted profile is removed from corresponding system files and database at the targets.

Note: Exercise caution when deleting profiles. Deleting a profile can cause problems throughout the distribution hierarchy.

The safest way to delete a profile is to first move or delete all the profile items from the profile. If you move or delete a profile item that corresponds to current information in the files or database on the target, a warning is displayed so that you can confirm or cancel the move or deletion. If you delete an entire profile, no warning is displayed for profile items.

The following table provides the context and authorization role required for this operation:

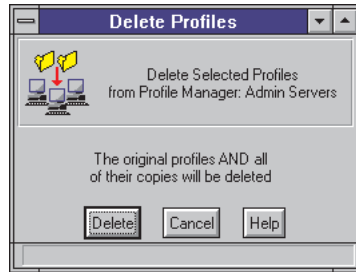
Activity	Context	Required role
Deleting profiles from a profile manager	Profile manager	admin

You can delete a profile from either the Tivoli desktop or the command line.

Desktop

To delete profiles from the profile manager, perform the following steps:

1. In the Policy Region window, double-click the Profile Manager icon to display the Profile Manager window.
2. Select one or more Profile icons.
3. From the **Edit** menu, select **Profiles → Delete** to display the Delete Profiles window:



4. Click **Delete** to delete the selected profiles and all their copies.

Command line

For information about using the command line to delete profiles from a profile manager, see the **wdel** command in *Tivoli Management Framework Reference Manual*.

Chapter 7. Queries and query libraries

The *query facility* enables you to use Structured Query Language (SQL) functions to access information in an RDBMS Interface Module (RIM) repository. A *RIM repository* is a relational database management system (RDBMS) database that a Tivoli application accesses through the RIM Application Program Interface (API). Several Tivoli applications store information in RIM repositories. For specific information about naming requirements and data stored in RIM repositories, refer to the appropriate product documentation.

The query facility consists of query libraries and queries. *Query libraries* reside in policy regions and contain queries. Use query libraries to organize similar queries into logical groups. For example, in each policy region, you could create a query library to hold the queries that select subscribers for file packages. Query libraries can contain only queries; you cannot add any other type of object to query libraries.

Queries specify which RIM repository to search, which view or table within the repository to query, and what information to retrieve. Views are created so that a group of information can be accessed easily by a query. A view can be described as a custom table, or a way to group information from related tables. For example, using Inventory, the PROCESSOR_MODEL, PROCESSOR_SPEED, HARDWARE_SYSTEM_ID, and COMPUTER_MODEL columns reside in different tables throughout the configuration repository. A view named PROCESSOR_VIEW includes all the data in these columns. Instead of running a query for each table, you can collect this information with one query by using the PROCESSOR_VIEW view.

This chapter provides instructions for creating a query library, creating a query, editing a query, and using a query.

Working with Query Library icons

Query libraries reside in policy regions and are created to contain queries.

The pop-up menu for the Query Library icon identifies the query library and includes the following options:

Open Open the Query Library window and shows all Query icons that represent queries.

Create Query
Displays the Create Query window where you can define new queries.

Working with Query icons

Queries reside in query libraries and specify which RIM repository to search, which view or table within the repository to query, and what information to retrieve.

The pop-up menu for the Query icon identifies the query and includes the following options:

Edit Query

Displays the Edit Query window where you can modify the previously defined query.

Run Query

Runs the query against the RIM repository.

Creating a query library

Queries reside in query libraries. Before you can create a query, you must first create a query library in which to store it. Each query library in the Tivoli region must have a unique name.

The following table provides the context and authorization roles required to perform this operation:

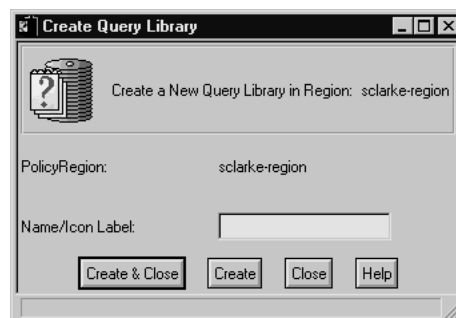
Activity	Context	Required role
Creating a query library	Policy region	senior or super

You can create a query library from the Tivoli desktop or the command line.

Desktop

To create a query library from the Tivoli desktop, perform the following steps:

1. In the Tivoli desktop, double-click the Policy Region icon that represents the policy region where you want to create the query library.
2. Ensure that this policy region allows the Query Library resource as a managed resources. For instructions on adding resource types to a policy region, refer to “Modifying managed resource types in policy regions” on page 72.
3. In the Policy Region window, select **Query Library** from the **Create** menu to display the Create Query Library window:



4. In the **Name/Icon Label** text box, type a unique name for the query library. The first character of the name must be an alphabetic character. The remaining characters can be alphanumeric, underscores (_), hyphens (-), periods (.), or spaces.
5. Click **Create & Close** to create the query library and returns to the Policy Region window. The policy region now contains an icon for the new query library.

Command line

For information about using the **wcrtqlib** command to create query libraries, see the *Tivoli Management Framework Reference Manual*.

Creating a query

When you create a query, you specify the repository in which to search for information and the set of information you want to retrieve. The repository you specify contains information provided by the Tivoli application that uses that repository. For example, the configuration repository contains information about machines in the Tivoli environment. For more information about the data stored in each repository, see the appropriate Tivoli application documentation.

The Create Query window enables you to select a subset of the columns in the view and include an SQL statement that returns the information you need from those columns. When you create a query, you must specify the following items:

- A query name that is unique in the Tivoli region
- A repository that determines which tables and views you can use for the query
- A table or view name within the repository to run the query against, which determines the columns you want to use for the query
- A set of chosen columns within the table or view to be part of the retrieved information

You can also specify a description for the query and a where clause. A *where clause* is an SQL search clause that specifies the information the query will return.

The following table provides the context and authorization roles required to perform this operation:

Activity	Context	Required role
Creating a query	Query library	senior or super

You can create a query from the Tivoli desktop or the command line.

Desktop

To create a query from the Tivoli desktop, perform the following steps:

1. In a Policy Region window, double-click the Query Library icon where you want to create the query. The Query Library window is displayed.
2. From the **Create** menu, select **Query** to display the Create Query window:

3. In the **Query Name** text box, type a unique name for the query.

Note: The name can be any set of alphanumeric characters, uppercase letters, or lowercase letters. Spaces are allowed.

4. In the **Description** text box, type a brief description of the query. This information is optional.
5. From the **Repository** drop-down list, select a RIM repository against which the query will run.
6. Either type or select a table or view name.
 - To type a name, type the name in the **Table/View Name** text box and click **Set**.
 - To select a table or view, click the ellipses (...) button. The list of views displayed depends on the Tivoli applications you have installed. See the appropriate application manual for more information.

Note: Changing the entry in the **Table/View Name** text box populates the **Available Columns** scrolling list and clears the rest of the fields on the window, including the **Chosen Columns**, **Where Clause**, and **Additional Clauses** scrolling lists.

7. Select **No Duplicates** to ensure that no duplicate information is returned in the query results.

8. In the **Available Columns** scrolling list, select the columns from which you want to retrieve information. Then click the left-arrow button to move them to the **Chosen Columns** scrolling list. If you need to use the query to select targets, include the TIVOLI_OBJECT_ID item in the **Chosen Columns** scrolling list.

The available columns are determined by the table or view specified in the **Table/View Name** text box. Click **Table Description** to view the Table Description window, which shows the structure of the data elements. This view differs between Tivoli repositories. For details, refer to the appropriate Tivoli application documentation.

Click **Close** to return to the Create Query window.

9. To add an SQL function to a column name, select a column in the **Chosen Columns** scrolling list and click **Edit**. Then type an SQL function in the **Column** text box and click **Add** or **Replace**.

Add adds the modified column as a new column while **Replace** puts the modified column in the **Chosen Columns** scrolling list in place of the original column.

10. Create a SQL search clause in the **Where Clause** text area to specify what information the query will return. Use the **Column Name** and **Column Value** text boxes with the operator buttons to create the SQL clause.

Note: Select **Not** to retrieve all information except what is specified in the where clause.

Complete the following steps:

- a. Type or select from a list the column names.
 - Type one of the column names from the **Chosen Columns** scrolling list in the **Column Name** text box.
 - Click the ellipses (...) button, and select values from the list.
- b. Select a logical operator to establish a relationship between the entry in the **Column Name** text box and the entry in the **Column Value** text box. You can select from any of the following logical operators:

= Equal to.

!= Not equal to.

< Less than.

<= Less than or equal to.

> Greater than.

>= Greater than or equal to.

IN Enables you to specify a list of column values for which to search. If you use **IN**, the items in the **Column Value** text box must be separated by commas and enclosed in parentheses.

LIKE Selects rows containing columns that match character strings specified in the **Column Value** text box. If you use **LIKE**, you must include an SQL wildcard and enclose the wildcard and character string in single quotation marks.

- c. Type or select the search criteria.
 - Type one or more values that complete the search criteria in the **Column Value** text box.
 - Select a value from a list of values that match the entry in the **Column Name** text box, click the ellipses (...) button.

This text box can contain SQL wildcard characters, such as a percent sign (%).

- d. Click **Add** to add the criteria to the **Where Clause** scrolling list.
- e. To build a compound query, select either **and** or **or** and repeat steps a through e to add clauses to the **Where Clause** scrolling list.

You can edit an existing search clause by selecting a line in the **Where Clause** scrolling list and clicking **Edit**. The clause is displayed in the **Column Name** and **Column Value** text boxes. Change the clause and click either **Replace**, **Insert**, or **Add**.

- The **Replace** button replaces the selected clause
- The **Insert** button places the new line above the selected line in the clause
- The **Add** button adds the new line to the end of the clause

You can also delete a line of the clause by selecting the line and clicking **Delete**.

11. Use the **Additional Clauses** scrolling text area if you want to use a search clause that includes the GROUP BY and ORDER BY functions. If you do not specify an operator at the beginning of the clause in the **Additional Clauses** text box, AND is used by default.
12. Click **Create & Close** to create the query and return to the Query Library window.

Command line

For information about using the **wcrtquery** command to create queries, see the *Tivoli Management Framework Reference Manual*.

Editing a query

After you have created a query, you can change the repository, the view, the columns, or the where clause.

The following table provides the context and authorization roles required to perform this operation:

Activity	Context	Required role
Editing a query	Policy region	senior, super, or Query_edit

You can edit a query from the Tivoli desktop or the command line.

Desktop

To edit a query from the Tivoli desktop, perform the following steps:

1. In a Query Library window, double-click a Query icon to display the Edit Query window. This window is the same as the Create Query window, except the Create buttons are now Save buttons.
2. Change the **Repository**, **Table/View Name**, **Chosen Columns**, **Where Clause**, **Column Name**, **Column Value**, or **Additional Clauses** field as necessary. (Refer to “Creating a query” on page 93 for an explanation of the fields on this window.)
3. Click **Save & Close** to save the changes.

Command line

For information about using the **wgetquery** and **wsetquery** commands to modify queries, see the *Tivoli Management Framework Reference Manual*.

Running a query

You can run a query and view the results or save them in a file.

The following table provides the context and authorization roles required to perform this operation:

Activity	Context	Required role
Running a query	Policy region	senior, super, Query_edit, or Query_execute

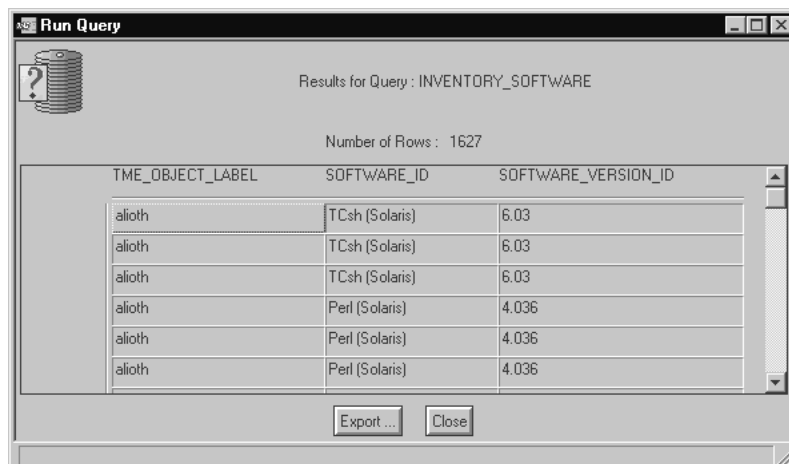
You can run a query from either the Tivoli desktop or the command line.

Desktop

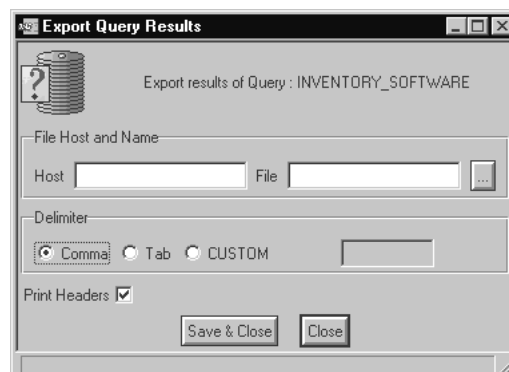
To run a query from the Tivoli desktop, perform the following steps:

1. In the Query Library window, right-click the Query icon and select **Run Query**. You can also select **Run Query** from the Create Query or Edit Query window.

The Run Query window is displayed, showing the results of the query:



2. To save the query results, perform the following steps:
 - a. Click **Export** to display the Export Query Results window:



- b. In the **Host** text box, type the name of the managed node where you want to save the file. If you do not specify a managed node, the file is saved on the local machine.
- c. In the **File** text box, type the location and name where you want to save the file.
If you do not know the location and name of the file, click the ellipses (...) button to browse the file system.
- d. In the **Delimiter** group box, specify how to separate entries in the query results file. If you want to use a delimiter other than a comma or a tab, click **Custom** and type a delimiter in the text box to the right.
- e. Select **Print Headers** if you want the output file to include the name of the query, the number of rows, and the names of the columns.
- f. Click **Save & Close** to create the file and return to the Query Library window.

Command line

For information about using the **wrunquery** command to run queries, see the *Tivoli Management Framework Reference Manual*.

Chapter 8. Notices and notice groups

A Notices icon is displayed on each Tivoli desktop. You receive notices on your bulletin board by subscribing to a notice group. (See Chapter 3, “Tivoli administrators,” on page 29 for instructions on subscribing to notice groups.)

Initially, there are no notices and the bulletin board is empty, and its icon looks as follows:



When new notices arrive, the Notices icon changes to indicate that the bulletin board now contains unread notices:



A notice is assigned the following attributes when posted:

- Unique ID
- Severity level
- Date and time stamp
- Administrator name
- Summary of the notice contents

Reading notices

You read a notice by double-clicking it from the list of unread notices in a particular notice group to which you subscribe. Each notice is described by a one-line tag, or header, that displays the notice identification number, the notice severity, the date and time of the notice, and the initial words of the notice text. Notices accumulate in the notice headers list until you read them or they expire. For information about notice expiration, see “Setting notice expiration” on page 107.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Reading notices	Tivoli desktop	user

You can read notices from the Tivoli desktop or the command line.

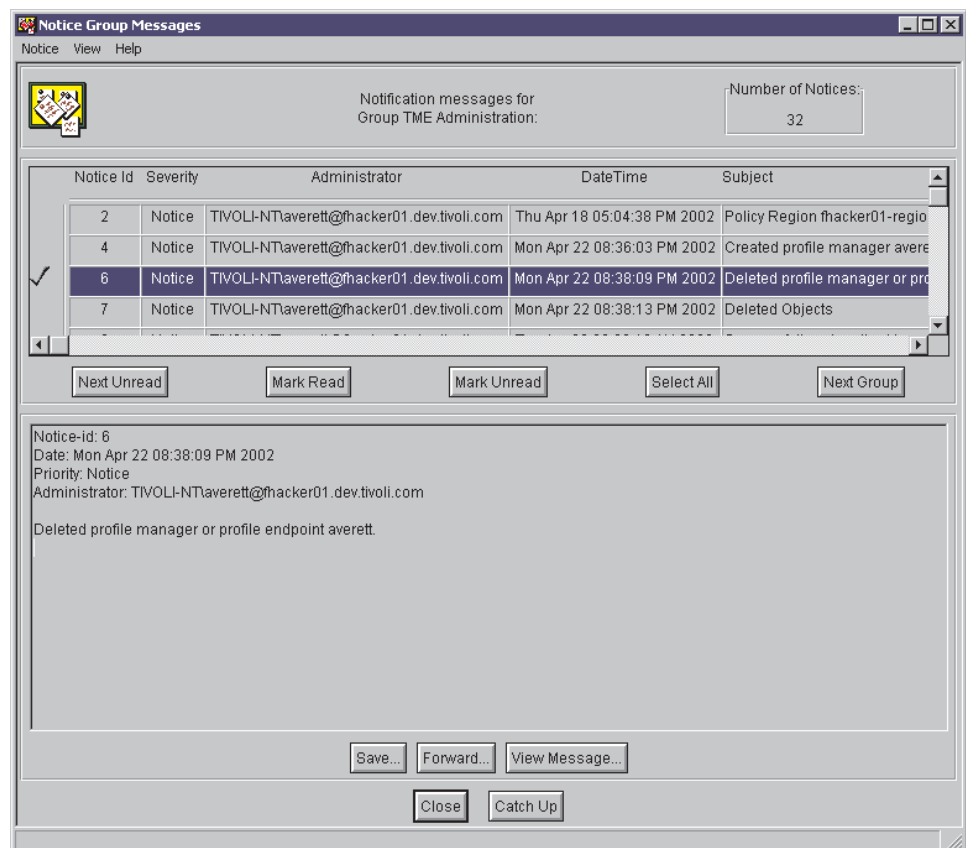
Desktop

To read notices, perform the following steps:

1. In the Tivoli desktop, double-click the Notices icon to display the Read Notices window:



2. Double-click a notice group in the scrolling list to display the Notice Group Messages window. You can select only one notice group at a time, but you can open multiple Notice Group Messages windows by double-clicking another notice group in the Read Notices window.
3. Double-click a notice header in the scrolling list to display the notice in the text area:



- a. If multiple notices for the notice group are unread, you can select one or more notice headers and click **View Message** to read them.
 - b. After reading the notices, click **Close** to return to the Notice Group Messages window.
4. Click **Close** to close the Notice Group Messages window.
 5. Click **Update** to refresh the list of unread notices, or click **Catch Up** to mark all notices as read.

Command line

For information about using the command line to read notices, see the **wlsnotif** and **wls** commands in the *Tivoli Management Framework Reference Manual*.

Saving notices

You can save a notice to a text file. For example, you can maintain a log of policy region operations in a particular policy region by saving all notices that report an operation in the policy region. You must have an account on the computer system where the file is saved.

The following table provides the context and authorization role required for this operation:

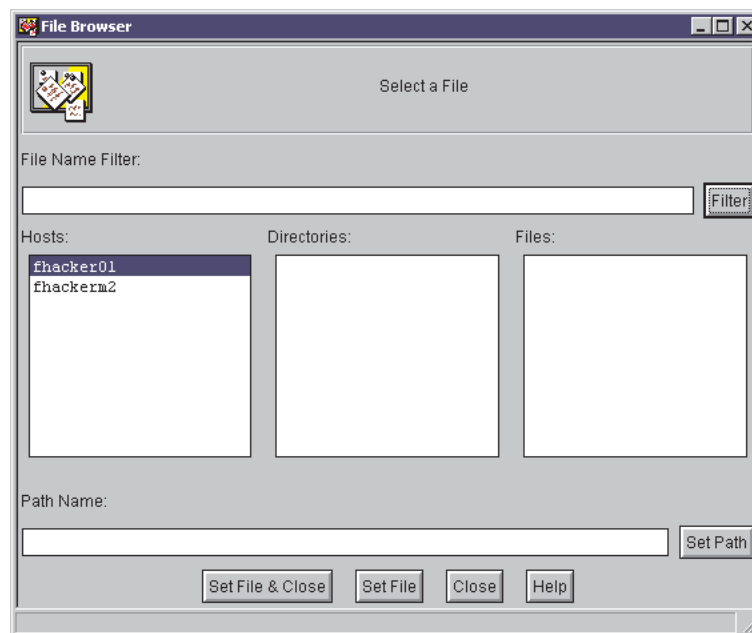
Activity	Context	Required role
Saving notices	Tivoli desktop	user

You can save a notice to a text file from the Tivoli desktop or the command line.

Desktop

To save notices to a text file, perform the following steps:

1. While reading the notice, click **Save**. The File Browser window is displayed:



2. Select the host where the file is to be saved.
3. Use the **Directories** and **Files** scrolling lists to set the directory and file names.
4. Click **Set File & Close** to save the selected notices and return to the Notice Group Messages window.
5. If finished reading all notices, click **Close** to close the Notice Group Messages window and return to the Read Notices window.

Command line

Save notices to a text file by redirecting the output of **wlsnotif**. For more information, see the *Tivoli Management Framework Reference Manual*.

Forwarding notices

You can forward a notice to one or more users. For example, you might notice that Tivoli Management Framework has made a change to a system resource and generated a notice describing the operation. You decide that a wider audience needs to know about the change, so you want to forward the notice using e-mail.

The following table provides the context and authorization role required for this operation:

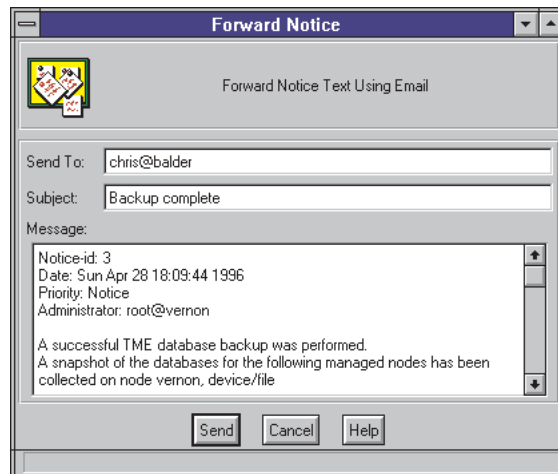
Activity	Context	Required role
Forwarding notices	Tivoli desktop	user

You can forward a notice to an e-mail alias from the Tivoli desktop or the command line.

Desktop

To forward notices, perform the following steps:

1. While reading the notice, click **Forward** to display the Forward Notice window:



2. Specify the e-mail address of the notice recipient in the **Send To** text box.
3. Specify the subject of the e-mail message in the **Subject** text box.
4. Optionally, edit the text displayed in the **Message** area.
5. Click **Send** to mail the notice to the e-mail addresses listed and return to the Notice Group Messages window.
6. If finished reading notices, click **Close** to close the Notice Group Messages window.

Command line

Forward notices by piping the output of **wlsnotif** to a mail utility. For more information, see the *Tivoli Management Framework Reference Manual*.

Marking notices as read and unread

After you view a notice, it is marked as read in the Notice Group Messages window and a check mark is placed in the left column. You can explicitly control which notices are marked as read or unread. If you view a notice or mark it as read, it is not displayed in the Notice Group Messages window the next time you open the notice group. To retain the notice, you can mark it as unread.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Marking notices as read or unread	Tivoli desktop	user

You can mark a notice as read or unread from the Tivoli desktop only.

- To mark a notice as read in a notice group, perform the following steps:
 1. In the Notice Group Messages window, select the notices you want to mark as read.
 2. Click **Mark Read** to mark the selected notices as read. The Notice Group Messages window remains open.
- To mark a notice as unread in a notice group, perform the following steps:
 1. In the Notice Group Messages window, select the notice or notices you want to mark as unread.
 2. Click **Mark Unread** to mark the selected notices as unread. The Notice Group Messages window remains open.
- To mark all notices as read in a notice group, click **Catch Up**. The selected notices are marked as read, and the Notice Group Messages window is closed.

When finished reading notices, click **Close** to return to the Read Notice window. Then click **Close** to return to the Tivoli desktop.

Sorting notices

You can specify how the notices displayed in the Notice Group Messages window are sorted. This sort order is for this session only. The next time you display this window, your last sort order is not saved.

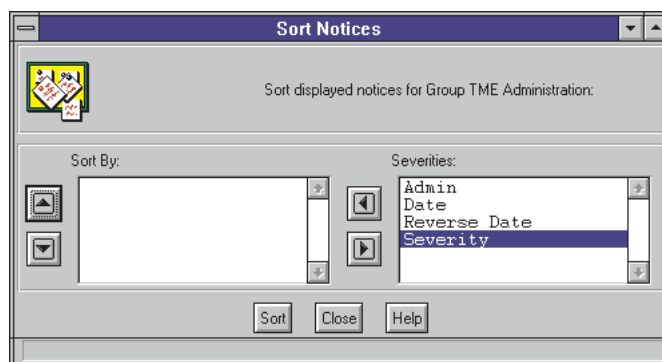
The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Sorting notices	Tivoli desktop	user

You can sort notices from the Tivoli desktop only.

To sort notices, perform the following steps:

1. In the Tivoli desktop, double-click the Notices icon to display the Read Notices window.
2. Double-click a notice group in the scrolling list to display the Notice Group Messages window.
3. From the **View** menu, select **Sort Notices** to display the Sort Notices window:



- a. Select a property from the **Severities** scrolling list and click the left-arrow button to move it the **Sort By** scrolling list. If there are additional properties by which you want to sort the notices, select each property and click the left-arrow button to move the property to the **Sort By** scrolling list.
 - b. If you have two or more **Sort By** properties, you can optionally define the sort order precedence by clicking the up-arrow or down-arrow button, as appropriate.
 - c. Click **Sort** to sort the notices and return to the Notice Group Messages window.
4. Click **Close** to close the Notice Group Messages window.

Filtering notices

You can specify the display order of notices in the Notice Group Messages window by filtering. For example, you can view all the notices generated by a specific Tivoli administrator that have a severity level of Critical.

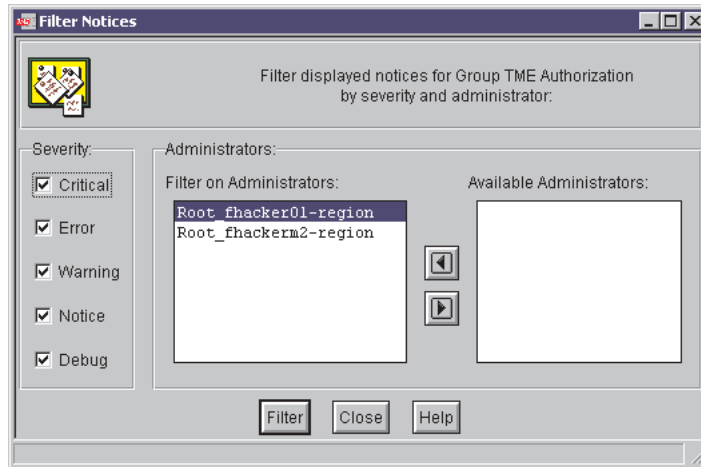
The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Filtering notices	Tivoli desktop	user

You can filter notices from the Tivoli desktop only.

To filter notices, perform the following steps:

1. In the Tivoli desktop, double-click the Notices icon to display the Read Notices window.
2. Double-click a notice group in the scrolling list to display the Notice Group Messages window.
3. From the **View** menu, select **Filter Notices** to display the Filter Notices window:



Each administrator who sent a notice in the selected notice group is listed in the **Filter on Administrators** scrolling list.

- a. For those administrators for whom you want to filter out notices, double-click the administrator to move it to the **Available Administrators** scrolling list.
- b. Select one or more severity levels from the **Severity** group box to indicate the type of notices you want to see.
- c. Click **Filter** to filter the notices and return to the Notice Group Messages window where you can view only notices matching the filtering criteria. Notices not matching the criteria remain unread.

Note: Filter setting are not saved between sessions.

4. When finished reading the notices, click **Close** to close the Notice Group Messages window.

Combining notices

You can specify that related notices displayed in the Notice Group Messages window be combined into a single entry. This is useful, for example, when many notices relate to some specific operation and you want to group them as a single notice in the notice headers scrolling list.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Combining notices	Tivoli desktop	user

You can combine notices from the Tivoli desktop only.

To combine notices, perform the following steps:

1. In the Tivoli desktop, double-click the Notices icon to display the Read Notices window.
2. Double-click a notice group in the scrolling list to display the Notice Group Messages window.
3. From the **View** menu, select **Combine Related Notices**. Any related notices are combined in the Notice Group Messages window.

4. When finished reading notices, click **Close** to close the Notice Group Messages window.

Displaying old notices

You can request to display notices that you have already read but which have not yet expired from the notice group. This is useful, for example, when you want to review one or more operations that have previously been performed.

Note: You cannot display previously read notices if there is not at least one unread notice in the notice group.

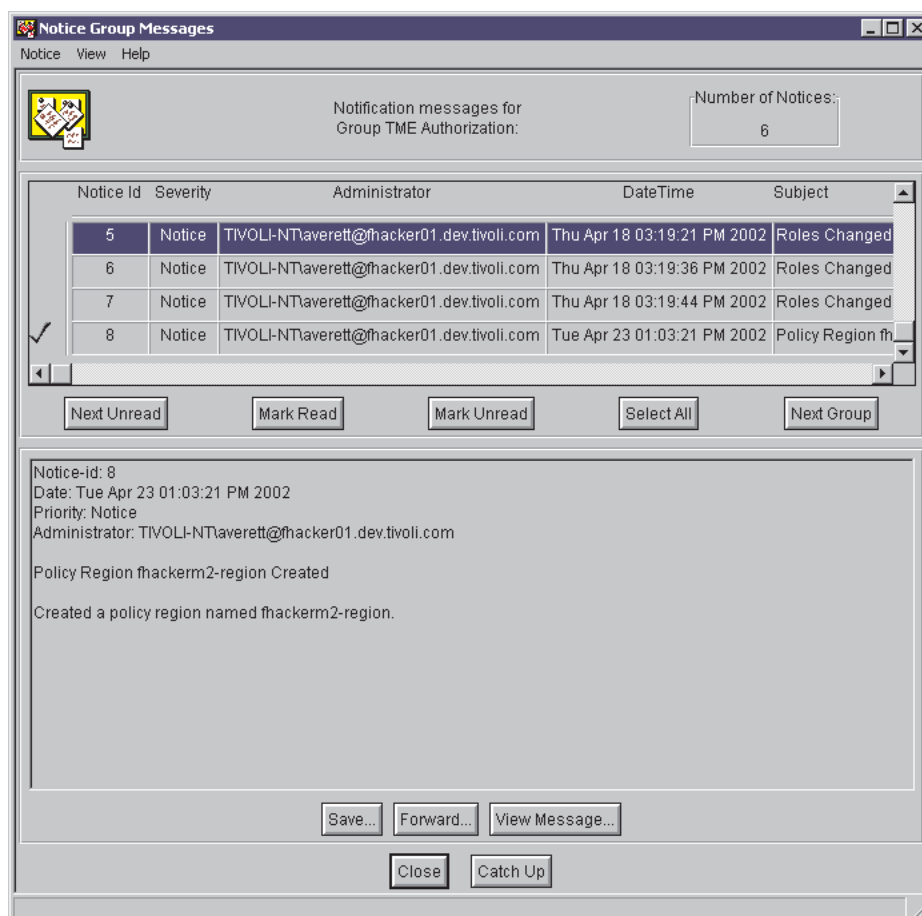
The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Displaying old notices	Tivoli desktop	user

You can display old notices from the Tivoli desktop only.

To display notices, perform the following steps:

1. In the Tivoli desktop, double-click the Notices icon to display the Read Notices window.
2. Double-click a notice group in the scrolling list to display the Notice Group Messages window.
3. From the **View** menu, select **Display Old Notices**. Any previously read notices that have not yet expired are displayed in the Notice Group Messages window:



- When finished reading notices, click **Close** to close the Notice Group Messages window.

Setting notice expiration

Each notice group has a notice expiration time associated with it. This allows you to have notices automatically removed after a certain period of time. All notices generated by Tivoli Management Framework expire after 168 hours (1 week), with the exception of Tivoli scheduler notices, which expire after 72 hours. You can also explicitly force one or more notices to expire early. (See the appropriate Tivoli application manual for the default expiration times of application-specific notices.)

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Expiring notices	Tivoli region	senior

You can set notice expiration from the command line only.

You can expire one or more notices in a notice group from the command line using **wexpnotif**. For more information, see the *Tivoli Management Framework Reference Manual*

Chapter 9. Jobs, tasks, and task libraries

You can use Tivoli Management Framework to create a task library to store tasks and jobs. Tasks and jobs allow you to set up procedures for operations and run these procedures on multiple managed resources. Using tasks and jobs can hide the complexity of managing large networks.

The Tivoli Task Library consists of the following entities:

Task libraries

Collections that allow you to create and store tasks and jobs that can be run on one or more managed resources. Task libraries can store executable files that are used by Tivoli applications. These files are invoked only by the application, not the task library. In this situation, a task library provides the application with a known location for executable files that the application uses. The task library also provides information about options that are required to run each task it contains the options required to run each of the tasks that it contains.

Tasks Definitions of operations that need to be performed on a routine basis. Each task is routinely performed on various managed resources throughout the network.

Jobs Tasks that are run on specific resources. When you create a job, you specify the task and define the information it needs to run. After you create a job, you can schedule it or run it without supplying additional information.

Notes:

- Tasks and jobs are similar in the following ways:
 - Both can be created only within a task library.
 - Both can be run on supported managed resources by dropping the Job icon or the Task icon the Job or the Task icon on the managed resource icon.
- Tasks and jobs are different in the following ways:
 - Jobs can be scheduled using the Tivoli scheduler. Tasks cannot be scheduled because they do not contain a list of targets.
 - Job icons can reside on the Tivoli desktop. Job icons are links to the jobs inside of task libraries. Task icons cannot reside on the Tivoli desktop. If you drop a Task icon on the Tivoli desktop, the entire task library is copied as a link to the originating task library.

Task libraries

In addition to containing tasks and jobs, task libraries store binaries, programs, and scripts that are generally referred to as executable files. When you create a task, an image of the files is stored in the binary tree of the Tivoli server.

Note: If you modify any executable file used in a task, you need to respecify the modified executable file in the task definition. If you do not respecify the modified file, the change is not refreshed in the binary tree.

Working with Task Library icons

A Task Library icon is displayed in the Policy Region window for each defined task library in that policy region. The pop-up menu of a Task Library icon identifies the name of the task library and includes the following options:

Open Opens the task library window and allows access to its defined tasks and jobs

Create Task

Displays the window where you can create a task

Create Job

Displays the window where you can create a job

Execute Task

Displays the window where you can specify its execution options

Execute Job

Displays the window where you can select a job and execute it

Creating a task library

You can create a task library within a policy region only. After creating a task library, you can create its tasks and jobs.

The following table provides the context and authorization role required for this operation:

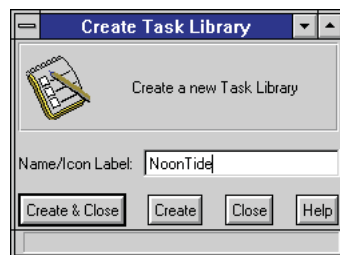
Activity	Context	Required role
Creating a task library	Policy region	senior
	Computer system hosting the executable files	root write permission to the subdirectory

You can create a task library from the Tivoli desktop or the command line.

Using the desktop to create task libraries

To create a task library, perform the following steps:

1. In a Policy Region window, select **Task Library** from the **Create** menu to display the Create Task Library window:



Note: If there is no entry on the **Create** menu for creating a task library, you need to add Task Library as a managed resource type for that policy region. See “Modifying managed resource types in policy regions” on page 72 for more information about adding and removing managed resources within policy regions.

2. Type the name of the task library in the **Name/Icon Label** text box.

The first character of the name must be an alphabetic character. The remaining characters can be alphanumeric, underscores (_), hyphens (-), periods (.), or spaces.

3. Click **Create & Close** to create the task library and return to the Policy Region window.

Using commands to create task libraries

For information about creating task libraries from the command line, see the **wcrtlib** command in *Tivoli Management Framework Reference Manual*. For information about setting the policies that control tasks and jobs within a task library, see the Task Library default and validation policies in *Tivoli Management Framework Reference Manual*.

Listing contents of a task library

After you create a task library, you can list its jobs and tasks.

The following table provides the context and authorization role required for this operation.

Activity	Context	Required role
Listing the contents of a task library	Policy region	user

You can list the contents of a task library from the command line only.

For information about listing the contents of a task library, see the **wlstlib** command in *Tivoli Management Framework Reference Manual*.

Importing and exporting task definitions

By default, you can pass arguments to a task, but you can only do this from the command line. If you need to pass arguments using a window, you need to use the Task Library Language (TLL) to create the window. The high level steps are as follows:

1. Export the library definition to American National Standard Code for Information Interchange (ASCII) using the **wtl** command
2. Modify the task library definitions
3. Import the modified library definitions using the **wtl** command

The task library has default and validation policies. The default policies set the available options of targets (endpoints, managed nodes, and profile managers) to run the task or job. The validation policies validate the creation and execution of the task or job in the task library. These policies can be customized using a shell script to set or validate data.

For additional information on the **wtl** command and the task library policies, see the *Tivoli Management Framework Reference Manual*. For additional information on the Task Library Language, see the *Tivoli Management Framework Reference Manual*.

Controlling task-binary distributions

When you create a task, you specify the files to be used when the task is run. These files are copied to the \$BINDIR directory on one of the following resources:

- The Tivoli server in the local Tivoli region, which is the default

- All file servers in the local region
- All file servers in interconnected Tivoli regions

The extent of this distribution is determined by the distribution mode specified in the **tl_def_dist_mode** default policy. See “Default policies for task libraries” on page 125 for more information about modifying the default distribution policy.

For daily use of the task library—creating tasks and jobs that are run by administrators—the default distribution mode is sufficient. Tivoli Management Framework searches for the task executable file on the Tivoli server and passes that executable file to the target. Additional distribution of the task-executable files does not increase productivity or efficiency.

Distributing task binaries to file servers either in the local Tivoli region or in connected regions is useful only when you have Tivoli applications that use executable files stored in a task library.

Some Tivoli applications include an application-specific task library. These required files are distributed when the product is installed. You can also distribute existing task binaries by using **wdisttask**. For more information about the distribution modes and on distributing task binaries, see **wdisttask** in *Tivoli Management Framework Reference Manual*.

Distributing the executable files to all the file servers in a Tivoli region gives the application faster access to the files. Having access to local tasks also makes an application more flexible and extensible in the actions it can perform. For example, the application can have access to a wider variety of tasks or can perform multiple actions, where previously it could perform only one.

Note: Do not distribute task binaries to file servers other than the Tivoli server until you begin using Tivoli applications that are capable of using this function. If you distribute task binaries to file servers that are shared among multiple Tivoli regions, file creation or editing conflicts cause the distribution to fail.

Tasks

A task is the definition of a network operation that needs to be performed on a routine basis. Tasks stored in a task library can be used any number of times. A task definition includes the following:

- The name (or label) of the task
- The platform (or interpreter type) on which the task is run
- The Tivoli authorization role required to run the task
- The user or group under which the task will be run
- Comments concerning the task

In some cases, a task requires more information before it can run. For example, you want to create a task that uses the UNIX **rdump** command to dump your file systems to tape. For **rdump** to run, you must specify which file systems should be dumped. The task, therefore, requires input from the administrator when the task is invoked.

When a task requires additional information, you can do one of the following:

- Specify this information from the command line when you invoke the task

- Use the Tivoli Task Library Language (TLL) to create another window where you can specify this information

Using the Tivoli TLL, you can define the additional arguments required by the task. When you run tasks that are defined with the TLL, a window prompts you for the task arguments. These windows are displayed after the Execute Task window. At that time you can, for example, specify the file system to be dumped. See *Tivoli Management Framework Reference Manual* for information about using the TLL to create the additional windows as well as an explanation of other TLL capabilities.

Working with Task icons

A Task icon is displayed in a Task Library window for each task created. A single Task icon, however, can represent the operational definition of multiple implementations—one for each supported platform.

The pop-up menu of a Task icon identifies the name of the task and includes the following options:

Execute Task

Displays the window where you can specify the execution parameters for a task.

Note: You can also run a task by double-clicking the Task icon or by dragging and dropping the icon on a managed resource icon.

Edit Task

Displays the window where you can modify a previously created task.

Creating a task

You can create a task in a task library. Before you create a task, one or more executable files that implement the associated operation must exist.

The following table provides the context and authorization role required for this operation:

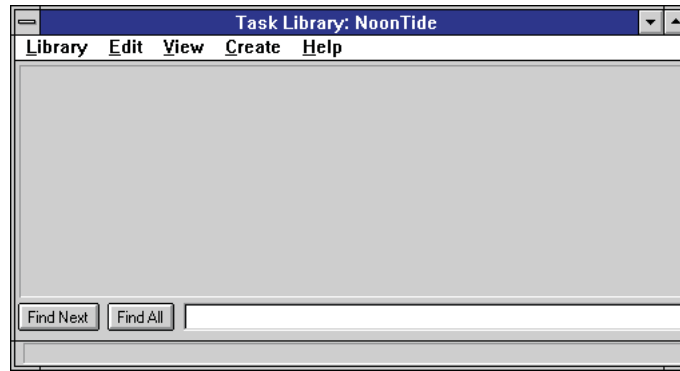
Activity	Context	Required role
Creating a task	Task library	admin

You can create a task in an existing task library from the Tivoli desktop or the command line.

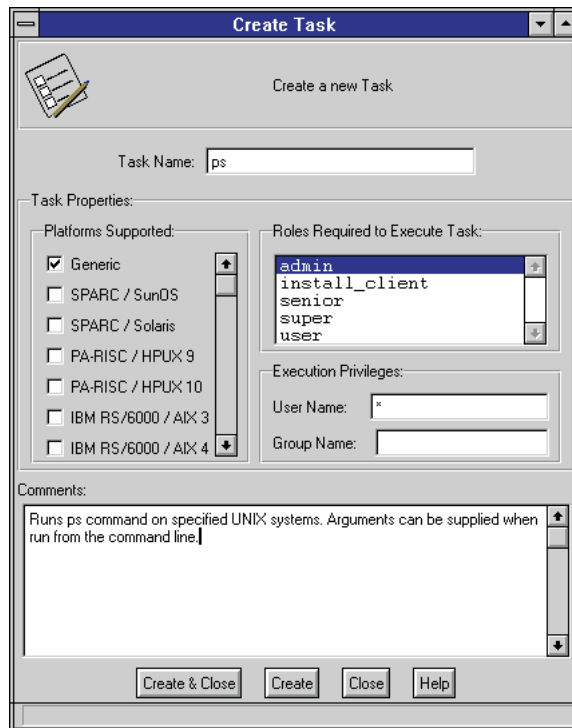
Using the desktop to create tasks

To create a task, perform the following steps:

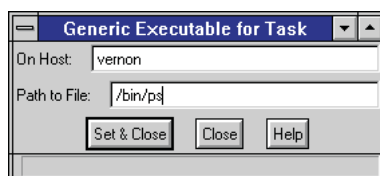
1. In a Policy Region window, double-click the Task Library icon where the task will reside to display the Task Library window:



2. From the **Create** menu, select **Task** to display the Create Task window:



3. Type the name of the task in the **Task Name** text box.
The first character of the name must be an alphabetic character. The remaining characters can be alphanumeric, underscores (_), hyphens (-), periods (.), or spaces.
4. From the **Platforms Supported** list, select the first platform on which the task is to be run. For each platform selected, the following steps apply.
For example if you have a generic executable file, such as a shell script that will run on multiple platforms, select **Generic** from the list of platforms. The Generic Executable for Task window is displayed:



- In the **On Host** text box, type the name of the managed node that contains the executable file for the selected platform.
- In the **Path to File** text box, type the full path name of the executable file for the selected platform.
- Click **Set & Close** to return to the previous window.

Repeat this step for each platform selected.

5. From the **Roles Required to Execute Task** scrolling list, select the roles that you want to require an administrator to have before they can run the task.
6. In the **Execution Privileges** area, specify the appropriate user and group IDs:
 - a. If you want the task to run under a specific user ID, type the user login name in the **User Name** text box. The default value is an asterisk (*), which specifies that the task runs under the ID of the administrator running the task.
 - b. If you want the task to run under a specific group ID, type the group name in the **Group Name** text box. By default, this text box is empty, which specifies that the task runs as **nogroup**.

Note: By default, you cannot specify root in the **User Name** or **Group Name** text box. To allow multiple administrators to create tasks that run as root, you must modify the **tl_val_set_uid** or **tl_val_set_gid** validation policy. See *Tivoli Management Framework Reference Manual* for procedures on editing policies.

7. Optionally, type a description of the task in the **Comments** scrolling list.
8. Click **Create & Close** to create the task and return to the Task Library window.

Using commands to create tasks

For information about creating a task from the command line, see the **wcrttask** command in *Tivoli Management Framework Reference Manual*.

Running a task

You can run a task after it is created in a task library. Each task is subject to the policies of the managed node or task library in the policy region where the task library is located.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Running a task	Task library	As specified when the task was created or edited

When the task is run, all task information, including the full executable file name, is passed to the task target. To locate the executable file, Tivoli Management Framework looks for a platform-specific executable file. For example, if the task is run on an AIX managed node, Tivoli Management Framework looks for an AIX executable file. If a platform-specific executable file is not found, Tivoli Management Framework looks for a generic executable file. If a generic executable file is not found, the task fails.

When the executable file is located, the executable file, user or group ID, and authorization role are passed to the task target. Tivoli Management Framework then validates the user ID and authorization role and runs the task directly from the managed resource.

Note: Each time a task is executed, the task-executable file is passed to the task target. The passing of large executable files can have a significant impact on network resources. If you have a task with a large executable file, you should consider installing the executable file on the clients. You can then create a task that passes only a small script to run the installed executable file.

You can run a task in the task library using drag and drop, from the Tivoli desktop, or from the command line.

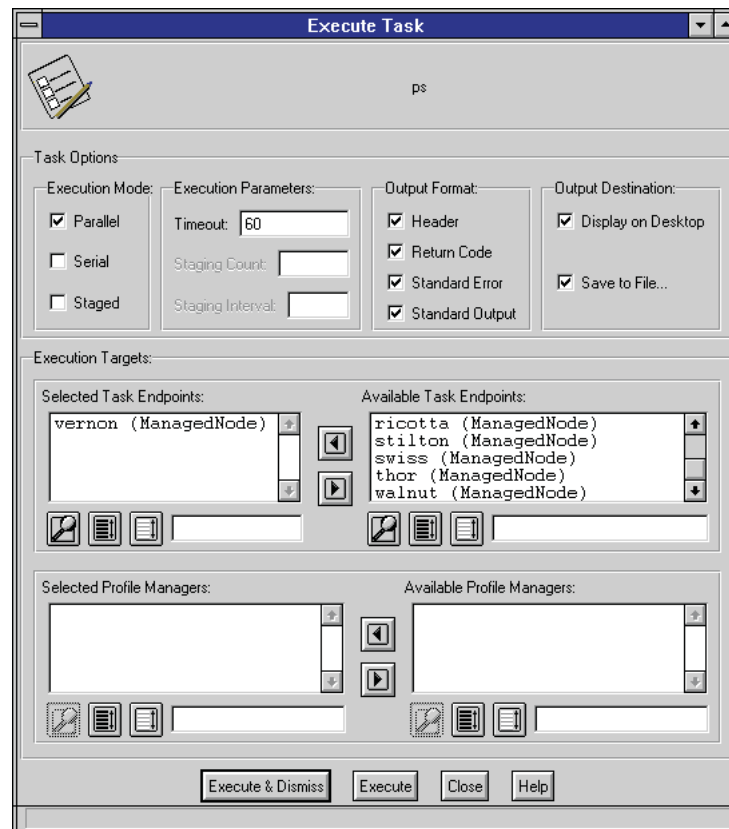
Using drag and drop to run tasks

To run a task, drag and drop the Task icon on a managed resource icon. When you drop the Task icon on any client icon, the task is run on that client. If you drop the task on a Profile Manager icon, the task is run in parallel mode on all of its subscribers.

Using the desktop to run tasks

To run a task, perform the following steps:

1. In a Task Library Window, double-click the Task icon to display the Execute Task window:



2. Specify the execution mode.
 - Select **Parallel** if the operation should run on all targets at the same time.
 - Select **Serial** if the operation should run on all targets, one at a time.

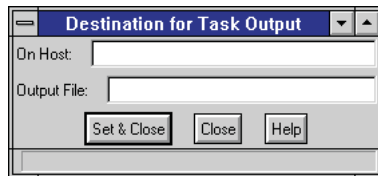
- Select **Staged** if the operation should run in staged mode on sets of targets. When you select **Staged**, you must specify the number of targets to include in each set and how many seconds to wait between each set.

When the execution mode is serial or staged, the operation is run on the targets in alphabetic order.

3. In the **Timeout** text box, type the number of seconds before the operation times out. If the operation does not complete within the specified amount of time, all output from the operation is lost. If the operation does not start within the specified time, it is canceled.

Note: For tasks run against endpoints, the timeout value for the task must be greater than the timeout value for the gateway. For example, if the task timeout is 600 and the gateway timeout is 300, the task times out after 300 seconds.

4. In the **Output Format** group box, select the types of output you want to return. The output types are **Header**, **Return Code**, **Standard Error**, and **Standard Output**.
5. In the **Output Destination** group box, select where the output is written.
 - Select **Display on Desktop** if you want the output to be displayed on the Tivoli desktop on completion.
 - Select **Save to File** to save the output to a file and display the Destination for Task Output window. Skip to the next step if you do not want output saved to a file.



- a. In the **On Host** text box, type the name of the managed node on which to save the output. The machine must be a managed node.
- b. In the **Output File** text box, type the full path name of the file where the output is to be written.

Note: Use a different file for the output of each operation. If multiple operations are performed around the same time and use the same output file, the output from all the operation is written to this one file.

- c. Click **Set & Close** to return to the Execute Task window.
6. In the **Execution Targets** area, specify the targets for the operation:
 - For specific clients, select the targets from the **Available Task Endpoints** scrolling list and click the left-arrow button. The selected targets are moved to the **Selected Task Endpoints** scrolling list.
 - For all subscribers of specific profile managers, select the profile managers from the **Available Profile Managers** scrolling list and click the left-arrow button. The selected profile managers are moved to the **Selected Profile Managers** scrolling list.
 7. Click **Execute & Dismiss** to run the task as specified and return to the Task Library window.

Using commands to run tasks

For information about running task from the command line, see the **wruntask** command in *Tivoli Management Framework Reference Manual*.

Saving task output to file

If you run a task that displays output on the Tivoli desktop, you can still save the output to file.

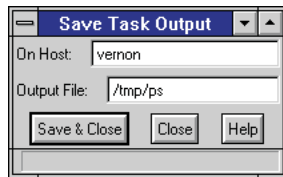
The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Saving displayed task output to a file	Task	As specified when the task that the job is based on was created or edited

You can save task output to file only from the Tivoli desktop.

To save task output to file, perform the following steps:

1. After the task completes and displays the output window, click **Save to File** to display the Save Task Output window:



2. In the **On Host** text box, type the name of the managed node on which to save the output. The machine must be a managed node.
3. In the **Output File** text box, type the full path name of the file to which the output is to be written.

Note: If the specified file already exists, the output is appended to the end of that file.

4. Click **Save & Close** to save the task output in the specified file and return to the output window. The file is written with the user ID and group ID of the administrator who invoked the task.

Editing a task

You can edit an existing task.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Editing a task	Task library	admin

You can edit an existing task from the Tivoli desktop or the command line.

Using the desktop to edit tasks

You can edit a previously created task. Editing a task is similar the creating task procedure described in “Using the desktop to create tasks” on page 113. The changes to the procedure are as follows:

- Instead of selecting to create a task from the Task Library window, select **Edit Task** from the Task icon menu.
- The Edit Task window is similar to the Create Task window, with the following changes:
 - The **Comments** text area of the Create Task window is changed to the **Text History and Comments** text area. You cannot add new comments in this text area.
 - The **New Comments** text area is where you can provide comments that apply to your modification.
 - The buttons on the Edit Task window apply to changing tasks instead of creating tasks.

Using commands to edit tasks

For information about editing a task from the command line, see **wgettask** and **wsettask** in *Tivoli Management Framework Reference Manual*.

Deleting a task

You can delete a task.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Deleting a task	Task library	admin

You can delete a task from the task library from either the Tivoli desktop or the command line.

Using the desktop to delete tasks

To delete a task from a task library, perform the following steps:

1. In a Task Library Window, select the icon of the task to be deleted.
2. From the **Edit** menu, select **Delete**. The selected task is deleted from the task library.

Using commands to delete tasks

For information about deleting a task form the command line, see the **wdeltask** command in *Tivoli Management Framework Reference Manual*.

Disabling notices for tasks

Every time a task runs, a notice is sent to the Administrators notice group. To disable the sending of notices regarding tasks, set the following system environment variable:

DONOTLOG=YES

Jobs

A job is a task that contains a number of run-time options, which includes the following:

- The list of targets where the task is run
- The execution mode of the task—serial or parallel
- The output format—Tivoli desktop or file

Note: You must create a task before you can create a job.

Working with Job icons

A Job icon is displayed in a Task Library window for each job created. You can copy a single Job icon onto a Tivoli desktop without copying the entire task library. The administrator can then run that job as necessary.

The pop-up menu of a Job icon identifies the name of the job and includes the following options:

Execute Job

Runs the job and sends the output to the specified destination

Note: You can also run a job by double-clicking the Job icon or, if you have the **admin** authorization role, by dragging and dropping the icon on a managed resource icon. When you drop the Job icon on a target, the job is run on only that target.

Edit Job

Displays the window where you can modify a job that was previously created

Creating a job

Before you create a job, the task for the job must exist within a task library. Jobs are subject to the task library policies of the policy region.

The following table provides the context and authorization role required for this operation:

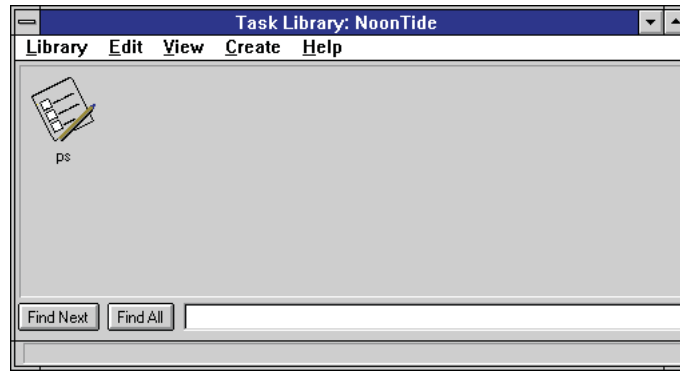
Activity	Context	Required role
Creating a job	Task library	admin

You can create a job from the Tivoli desktop or the command line.

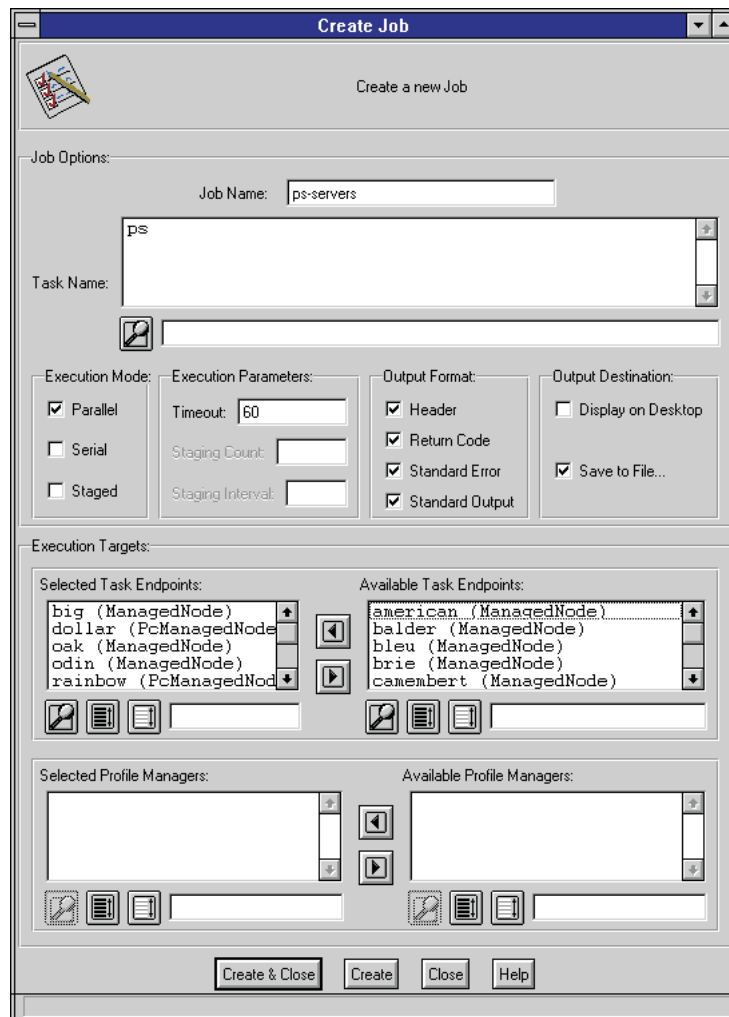
Using the desktop to create jobs

To create a job, perform the following steps:

1. In a Policy Region window, double-click the icon of the task library in which the job will reside to display the Task Library window:



2. From the **Create** menu, select **Job** to display the Create Job window:



3. In the **Job Name** text box, type the job name.

The first character of the name must be an alphabetic character. The remaining characters can be alphanumeric, underscores (_), hyphens (-), periods (.), or spaces.

4. From the **Task Name** scrolling list, select the task that the job will execute.

5. Specify the execution mode.

- Select **Parallel** if the operation should run on all targets at the same time.
- Select **Serial** if the operation should run on all targets, one at a time.

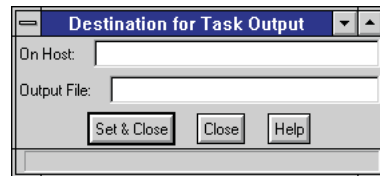
- Select **Staged** if the operation should run in staged mode on sets of targets. When you select **Staged**, you must specify the number of targets to include in each set and how many seconds to wait between each set.

When the execution mode is serial or staged, the operation is run on the targets in alphabetic order.

6. In the **Timeout** text box, type the number of seconds before the operation times out. If the operation does not complete within the specified amount of time, all output from the operation is lost. If the operation does not start within the specified time, it is canceled.

Note: For tasks run against endpoints, the timeout value for the task must be greater than the timeout value for the gateway. For example, if the task timeout is 600 and the gateway timeout is 300, the task times out after 300 seconds.

7. In the **Output Format** group box, select the types of output you want to return. The output types are **Header**, **Return Code**, **Standard Error**, and **Standard Output**.
8. In the **Output Destination** group box, select where the output is written.
 - Select **Display on Desktop** if you want the output to be displayed on the Tivoli desktop on completion.
 - Select **Save to File** to save the output to a file and display the Destination for Task Output window. Skip to the next step if you do not want output saved to a file.



- a. In the **On Host** text box, type the name of the managed node on which to save the output. The machine must be a managed node.
- b. In the **Output File** text box, type the full path name of the file where the output is to be written.

Note: Use a different file for the output of each operation. If multiple operations are performed around the same time and use the same output file, the output from all the operation is written to this one file.

- c. Click **Set & Close** to return to the Execute Task window.
9. In the **Execution Targets** area, specify the targets for the operation:
 - For specific clients, select the targets from the **Available Task Endpoints** scrolling list and click the left-arrow button. The selected targets are moved to the **Selected Task Endpoints** scrolling list.
 - For all subscribers of specific profile managers, select the profile managers from the **Available Profile Managers** scrolling list and click the left-arrow button. The selected profile managers are moved to the **Selected Profile Managers** scrolling list.
 10. Click **Create & Close** to create the job and return to the task library window.

Using commands to create jobs

For information about creating a job from the command line, see the **wcrtjob** command in *Tivoli Management Framework Reference Manual*.

Running a job

You can run a job after it is created in a task library.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Running a job	Task library	As specified when the task that the job is based on was created or edited

You can run a job using drag and drop, from the Tivoli desktop, or from the command line.

Using drag and drop to run jobs

To run a job, drag the Job icon onto the icon of the managed resource on which you want the job to run.

Note: Using the drag and drop operation requires the **admin** authorization role.

Using the desktop to run jobs

To run a job, double-click the Job icon. The job is run and the output is displayed on the Tivoli desktop or sent to the file designated in the job specification.

Note: When you choose to display the output on the Tivoli desktop, output is displayed when the job completes on all target resources. If you schedule a job that displays its output to the Tivoli desktop, an output window is not displayed when the task runs. You should save the output to file when you schedule a job. For details on scheduling a job, see Chapter 10, “Scheduling jobs,” on page 129.

Using commands to run jobs

For information about running a job from the command line, see the **wrunjob** command in *Tivoli Management Framework Reference Manual*.

Saving job output to file

If you run a job that displays the output to the Tivoli desktop, you can still save the output to file.

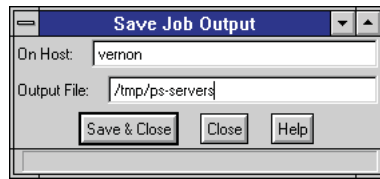
The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Saving displayed job output to file	Job	As specified when the task that the job is based on was created or edited

You can save displayed job output to file from the Tivoli desktop only.

To save the job output to file, perform the following steps:

1. After the task completes and displays the output window, click **Save to File** to display the Save Job Output window:



2. In the **On Host** text box, type the name of the managed node on which to save the output. The machine must be a managed node.
3. In the **Output File** text box, type the full path name of the file to which the output is to be written.

Note: If the specified file already exists, the output is appended to the end of that file.

4. Click **Save & Close** to save the task output in the specified file and return to the output window. The file is written with the user ID and group ID of the administrator who invoked the task.

Editing a job

You can edit a previously created job.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Editing a job	Task library	admin

You can edit a job in the task library from either the Tivoli desktop or the command line.

Using the desktop to edit jobs

You can edit a previously created job. Editing a job is similar the creating a job procedure described in “Creating a job” on page 120. The changes to the procedure are as follows:

- Instead of selecting to create a job from the Task Library window, select **Edit Job** from the Job icon menu.
- The Edit Job window is similar to the Create Job window, with the following changes:
 - The Edit Job window does not contain the **Job Name** text box.
 - The buttons on the Edit Job window apply to changing jobs instead of creating jobs.

Using commands to edit jobs

For information about editing jobs from the command line, see the **wgetjob** and **wsetjob** commands in the *Tivoli Management Framework Reference Manual*.

Deleting a job

You can delete a job.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Deleting a job	Task library	admin

You can delete a job from the task library from the Tivoli desktop or the command line.

Using the desktop to delete jobs

To delete a job, perform the following steps:

1. In a Task Library Window, select the icon of the job to be deleted.
2. From the **Edit** menu, select **Delete**. The selected job is deleted.

Using commands to delete jobs

For information about deleting jobs from the command line, see the **wdeljob** command in *Tivoli Management Framework Reference Manual*.

Task library policies

A task library uses default and validation policies to control the tasks and jobs within the library. Administrators with the **senior** and **policy** authorization roles can modify the policy to reflect the operational requirements of an organization. See *Tivoli Management Framework Reference Manual* for procedures on editing policies.

Default policies for task libraries

The default policies for task libraries define the list of entries displayed in the **Available Task Endpoints** and **Available Profile Managers** scrolling lists on the Execute Task window. From these lists, administrators select the resources on which a task or job can run.

Following is a list of the default policies used by a task library:

tl_def_dist_mode

Provides the distribution mode, which determines where task binaries are distributed when a task is created. The default setting is **ALI**. The following are valid modes:

ALI Copies task binaries to the Tivoli server only

LOCAL

Copies task binaries to all file servers in the local Tivoli region

GLOBAL

Copies task binaries to all file servers in connected Tivoli regions

tl_def_man_nodes

Provides the list of targets displayed on the Execute Task and Create Job windows. From this list, you select the targets on which the task or job will run.

tl_def_prof_mgrs

Provides the list of profile managers displayed on the Execute Task and Create Job windows. From this list, you select the profile managers on which a task or job will run.

tl_def_set_gid

Provides the default setting for the **Group Name** text box of the Create Task window. The default is empty.

tl_def_set_uid

Provides the default setting for the **User Name** text box of the Create Task window. The default is an asterisk (*).

Validation policies for task libraries

The validation policies for task libraries control the creation and execution of tasks and jobs. The following policies validate the resources on which the task or job executes. As a rule, the contents of these validation policies are identical to the contents of the default policies.

tl_val_man_nodes

Validates the list of targets on which a task or job will run.

tl_val_prof_mgrs

Validates the profile managers on which a task or job will run.

Note: Although these policies provide control over the resources for which an administrator can create tasks, they do not entirely limit where a task can be executed. If an administrator's desktop includes more resources than those listed in these validation policies, the administrator can drag and drop the task or job onto the additional resource. The task or job then runs on that resource.

The following policies validate the user or group ID specified on the Create Task window. By default, these policies do not allow a task to be created with the root permissions.

tl_val_set_gid

Validates the effective group ID assigned to a task or job

tl_val_set_uid

Validates the effective user ID assigned to a task or job

Task libraries on OS/400 systems

Tivoli Management Framework provides an OS/400 task library to automate tasks that are performed frequently by an OS/400 operator. As with all OS/400 commands or jobs, these commands must be run under the explicit authority of an OS/400 user profile that is specified for the task. If no profile is specified, the user ID running the Tivoli desktop is used.

Tasks for OS/400 can be any supported executable file, such as a QSH script, REXX script, or any OS/400 compiled program (*.PGM). To run a PGM files in a task, the program must be stored in a save file and moved using binary FTP to the source host. When creating the task the task points to the file that was moved to the source host. When the task is run, the program in the save file is restored and run on the OS/400 endpoints.

The following OS/400 tasks are provided:

Command

Enables you to enter any OS/400 control language (CL) command, valid in batch mode, for which all parameters are known. Prompting is not supported.

Send_Reply

Uses the OS/400 command **SNDRPLY** to send a reply to a message on a specific message queue.

Run_Backup

Uses the OS/400 command **RUNBKUP** to start to save information about your OS/400 system.

Start_cleanup

Uses the OS/400 command **STRCLNUP** to start cleaning up information about your OS/400 system, such as spool files or temporary libraries.

Power_Down_System

Uses the OS/400 command **PWRDWN SYS** to end all subsystems, power down the system, and optionally re-initial program load (IPL) a remote OS/400 system.

Vary_Configuration

Uses the OS/400 command **VRYCFG** to reset lines, controllers, and devices attached to an OS/400 system.

Note: Ensure that the maximum length of each line in any source script file does not exceed 92 characters.

For more information about these and other control language commands, see *IBM OS/400 Control Language Reference Manual*.

Chapter 10. Scheduling jobs

Using the scheduler enables you to control the timing and automation of regular system operations, known as jobs. You can use the scheduler to do the following:

- Schedule predefined jobs to run at specific times and within a specified time frame
- Schedule predefined jobs to run a specified number of times at specified time intervals
- Schedule predefined jobs to run on a predefined schedule indefinitely
- Restrict scheduled jobs to run under specified conditions only
- View a list of scheduled jobs
- Disable and enable scheduled jobs
- Delete schedule jobs

The scheduler cannot be used to define jobs. The scheduler allows you to schedule previously defined jobs only. However, you can edit scheduled jobs, disable or enable scheduled jobs, and remove scheduled jobs.

Note: Because the scheduler is a distinguished resource (only one per Tivoli region), see “Using the Scheduler across region boundaries” on page 137 to understand how the scheduler works and scheduled jobs work within connect Tivoli regions.

The pop-up menu of the Scheduler icon includes the following options:

Browse/Edit

Opens the Browse Scheduled Jobs window where you can view a list of scheduled job and select a scheduled job to edit.

Scheduling a job

You can schedule a job to run at a later time by using the scheduler. However, you can only schedule a job that was previously created in a task library or from within an application. You cannot use the scheduler to create a job.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Scheduling a job	Scheduler	admin

You can schedule a job using drag and drop, from the Tivoli desktop, or using the command line.

Using drag and drop to schedule jobs

To schedule a job using drag and drop, drag and drop a Job icon onto the Scheduler icon. The Add Scheduled Job window is displayed. See “Using the desktop to schedule jobs” on page 130 for details about scheduling a previously defined job from a Tivoli desktop.

Using the desktop to schedule jobs

To schedule a job, perform the following steps:

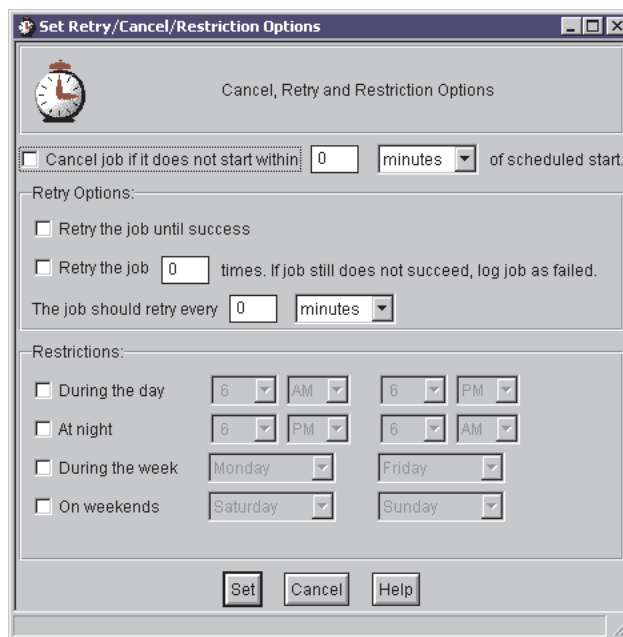
1. To schedule a job, either drag and drop a Job icon on the Scheduler icon or click **Schedule** from a window to display the Add Scheduled Job window:

The screenshot shows the 'Add Scheduled Job' dialog box. It has a title bar with the text 'Add Scheduled Job' and a clock icon. The main area is divided into several sections. The first section is 'Job Name' with a value of 'Check Policy' and a 'Job Label' text box. There is a checkbox labeled 'Disable the Job.' The second section is 'Description' with a text box containing 'Scheduled Check Policy'. The third section is 'Schedule Job For' with date (12/5/1996) and time (6:00 AM) fields. The fourth section is 'Repeat The Job' with options for indefinite or limited repetition and an interval of 0 minutes. The fifth section is 'When Job Complete' with checkboxes for notifications and email, and fields for host and file. At the bottom are buttons for 'Schedule Job & Close', 'Schedule Job', 'Close', and 'Help'.

2. In the **Job Label** text box, type the job label. If you do not specify a job label, the job name is used by default.
The name of a scheduled job can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.
3. If you do not want to enable the job as scheduled, select the **Disable** check box. Generally, you do not want to select this check box while scheduling a job.
4. In the **Description** text box, type a brief description of the job being scheduled.
5. In the **Schedule Job For** text boxes, specify the date and time that the job should be run.
6. In the **Repeat The Job** group box, specify how a repeating job is to be run. The following options are mutually exclusive:
 - To repeat a job indefinitely, select **Repeat the job indefinitely**.
 - To repeat the job a limited number of times, select **Repeat the job *n* times** and type the number of times the job should run.

With both of these options, specify the time interval between runs. Type the time interval in the **The job should start every** text box and select the increment (minute, hour, or day) from the drop-down list.

7. In the **When Job Complete** group box, select which actions occurs when the scheduled job finishes:
 - Select **Post Tivoli Notice** and select a notice group, to post a notice to a notice group other than the **Tivoli Scheduler** notice group. A notice is posted to the **Tivoli Scheduler** notice group by default.
 - Select **Post Status Dialog on Desktop**, to display a window containing the completion status of the job.
 - Select **Send email to**, to send an email to the specified recipients containing the completion status of the job.
 - Select **Log to File** and specify where the file is to be written in the **Host** and **File** text boxes.
8. If you want to specify retry, cancel, or restriction options for the job, click **Set Retry/Cancel/Restriction Options** to display the Set Retry/Cancel Options window. If you do not want to specify these options, skip to step 9 on page 132.



In this window, you can do the following:

- Select **Cancel job if it does not start within** and specify the how much time to allocate before the job is canceled.
- Specify how many times to retry the job if it cannot start at the scheduled time. The following options are mutually exclusive:
 - To retry the job until it is successful, select **Retry the job until success**.
 - To retry a job a specified number of times, select **Retry the job** and specify the number of retries. If the job cannot be started after the specified number of retries, the job fails.

With both of these options, specify the time interval between retries. Type the time interval in the **The job should retry every** text box and select the increment (minute, hour, or day) from the drop-down list.

- Specify restrictions about when the job can be run. Select any combination of the following
 - **During the day**
 - **At night**
 - **During the week**

– **On weekends**

Use the appropriate drop-down lists to select a sequence of hours or days during which the job is allowed to run.

- Click **Set** to accept the specified options and return to the Add Scheduled Job window.

9. Click **Schedule Job & Close** to schedule the job and return to the Tivoli desktop.

Using commands to schedule jobs

For information about scheduling a job using the command line to schedule a job, see the **wschedjob** command in *Tivoli Management Framework Reference Manual*.

Viewing scheduled jobs

You can view scheduled jobs.

The following table provides the context and authorization roles required for this operation:

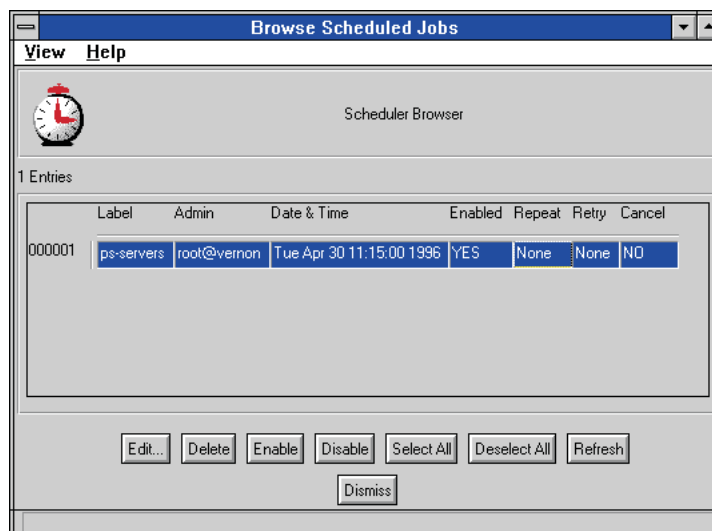
Activity	Context	Required role
Viewing scheduled jobs	Scheduler	user

You can view scheduled jobs from either the Tivoli desktop or the command line.

Using the desktop to view jobs

To view scheduled jobs, perform the following steps:

1. In the Tivoli desktop, right-click the **Scheduler** icon and select **Browse/Edit** to display the Browse Scheduled Jobs window:



The queue of scheduled jobs is displayed as a table. Each row contains a separate job, and each column displays a particular job attribute. By default, the job attributes displayed are the job ID, the job label, the administrator who scheduled the job, the date and time the job is scheduled to start, and whether the job is enabled, repeating, retrying, or under a deadline for starting. See “Controlling the display of job attributes” on page 133 for information about controlling how the attributes and layout are displayed.

You can also edit, delete, enable, and disable a scheduled job from the Browse Scheduled Jobs window.

2. Click **Dismiss** to close the window.

Using commands to view jobs

For information about viewing information about a scheduled job, see the **wgetsched** command in the *Tivoli Management Framework Reference Manual*

Controlling the display of job attributes

You can control the job attributes displayed in the Browse Scheduled Jobs window. You can choose to show one or more attributes of each currently scheduled job.

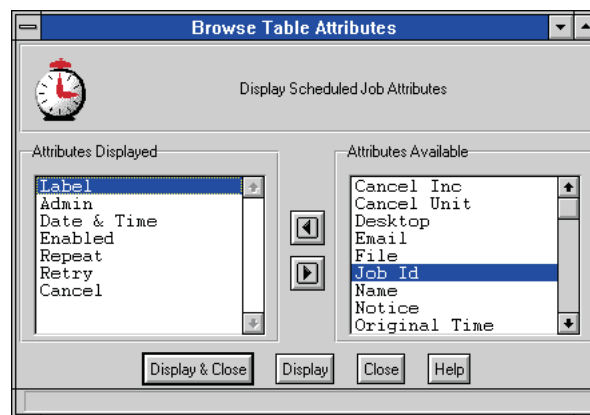
The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Specifying displayed job information	Scheduler	user

You can specify job display information from the Tivoli desktop only.

To set the information displayed about each job, perform the following steps:

1. In the Tivoli desktop, right-click the Scheduler icon and select **Browse/Edit** to display the Browse Scheduled Jobs window.
2. From the **View** menu, select **Columns** to display the Browse Table Attributes window:



The available options are displayed in the **Attributes Displayed** scrolling list.

3. Add or remove attributes.
 - To add an attribute to those displayed for a job, select an entry from the **Attributes Available** scrolling list and click the left-arrow button. The selected attribute is moved to the **Attributes Displayed** scrolling list.
 - To remove an attribute from those displayed for a job, select an entry in the **Attributes Displayed** scrolling list and click the right-arrow button. The selected attribute is moved to the **Attributes Available** scrolling list.
 - Double-click an entry to move it from one list to another.
4. Click **Display & Close** to accept your changes and return to the Browse Scheduled Jobs window.

Sorting jobs

You can sort jobs by any job attribute displayed in the Browse Scheduled Job window. You can also sort by an attribute whether that attribute is displayed in the Browse Scheduled Job window.

You can organize a sort in ascending or descending order. You can also choose multiple sort options. For example, you can sort scheduled jobs first by the scheduling administrator, and then by job label for each scheduling administrator.

The default sort order is by job label in ascending order.

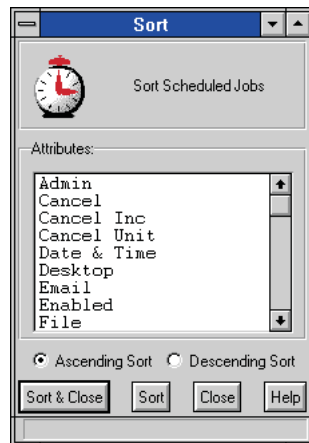
The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Sorting job information	Scheduler	user

You can sort job information from the Tivoli desktop only.

To sort job information, perform the following steps:

1. In the Tivoli desktop, right-click the Scheduler icon and select **Browse/Edit** to display the Browse Scheduled Jobs window.
2. From the **View** menu, select **Sort** to display the Sort window:



3. From the **Attributes** scrolling list, select an attribute to determine the sort criteria.
4. Click **Ascending Sort** or **Descending Sort** to determine how the information will be organized.
5. Either sort and return or perform multiple sorts.
 - Click **Sort & Close** to return to the **Browse Scheduled Jobs** window. The job rows are displayed as sorted by the selected attributes. The headers for the columns themselves are not changed.
 - Click **Sort**. The selected sort attribute is used to sort the list of jobs in ascending or descending order, as specified.

Note: You can sort by multiple attributes by selecting different sort attributes and clicking **Sort** after each selection.

Finding jobs

You can find one or more jobs by any job attribute displayed in the Browse Scheduled Jobs window. You can find a job by an attribute whether the attribute is displayed in the Browse Scheduled Jobs window.

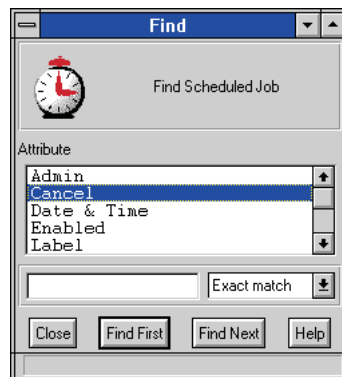
The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Finding job information	Scheduler	user

You can find a job from the Tivoli desktop only.

To find a specific job, perform the following steps:

1. In the Tivoli desktop, right-click the Scheduler icon and select **Browse/Edit** to display the Browse Scheduled Jobs window.
2. From the **View** menu, select the **Find** option to display the Find window:



3. Select an attribute from the **Attribute** scrolling list to determine the search criteria.
4. Click **Find First** to use the selected attribute to find the first job in the scheduled list that matches the selection criteria, or click **Find Next** to use the selected attribute to find the next job in the scheduled list that matches the selection criteria.
5. Click **Close** to return to the Browse Scheduled Jobs window.

Disabling or enabling scheduled jobs

You can enable or disable scheduled jobs.

The following table provides the context and authorization roles required for this operation:

Activity	Context	Required role
Disabling or enabling a job	Scheduler	admin

You can enable and disable schedule job using the Tivoli desktop or command line.

Using the desktop to enable and disable jobs

To disable or enable a job, perform the following steps:

1. In the Tivoli desktop, right-click the Scheduler icon and select **Browse/Edit** to display the Browse Scheduled Jobs window.
2. Select the job row. You can select more than one job by holding the **Shift** key while selecting a job row.
3. Click **Enable** to enable the job, or click **Disable** to disable the job.
4. Click **Dismiss** to close the window.

Using commands to enable and disable jobs

For information about enabling or disabling a scheduled job, see the **wenblsched** command in *Tivoli Management Framework Reference Manual*

Editing scheduled jobs

You can edit scheduled jobs.

The following table provides the context and authorization roles required for this operation:

Activity	Context	Required role
Editing a job	Scheduler	admin

You can edit a scheduled job using the Tivoli desktop or command line.

Using the desktop to edit jobs

To edit a job, perform the following steps:

1. In the Tivoli desktop, right-click the Scheduler icon and select **Browse/Edit** to display the Browse Scheduled Jobs window.
2. Select the job row. You can edit only one job at a time.
3. Click **Edit**. The current job options are displayed in the Edit Scheduled Job window.
4. Edit the options as appropriate. For details, see “Scheduling a job” on page 129.
5. Click **Update & Close** to accept the job changes and return to the Browse Scheduled Jobs window.
6. Click **Dismiss** to close the window.

Using commands to edit jobs

For information about editing scheduled jobs from the command line, see the **wgetsched** and **wsetsched** commands in *Tivoli Management Framework Reference Manual*.

Deleting scheduled jobs

You can delete scheduled jobs.

The following table provides the context and authorization roles required for this operation:

Activity	Context	Required role
Deleting a job	Scheduler	admin

You can delete scheduled jobs using the Tivoli desktop or command line.

Using the desktop to delete jobs

To delete a job, perform the following steps:

1. In the Tivoli desktop, right-click the Scheduler icon and select **Browse/Edit** to display the Browse Scheduled Jobs window.
2. Select the job row. You can select more than one job by holding the Shift key while selecting a row.
3. Click **Delete**.
4. Click **Dismiss** to close the window.

Using commands to delete jobs

For information about deleting a scheduled job, see the **wdelsched** command in *Tivoli Management Framework Reference Manual*.

Using the Scheduler across region boundaries

Each Tivoli region contains its own Scheduler. Each Scheduler has identical functions but is in a different location and contains different jobs.

A scheduled job is stored in the scheduler of the Tivoli region in which the job was scheduled. For example, a job scheduled in region Baltimore is stored in the Scheduler of region Baltimore.

In Figure 6, there are two Tivoli regions, Baltimore and Seattle, each containing a Scheduler. Region Baltimore contains two clients, Bulldog and Fox. Region Seattle contains two clients, Weimaraner and Beagle.



Figure 6. Multiple regions with no cross Scheduler operations

Most Scheduler actions, such as editing or removing a job, occur only within the Scheduler of the Tivoli region. However, you can run jobs across multiple regions.

Jobs across region boundaries

A job that is run in a Tivoli region can cross region boundaries. In Figure 7 on page 138, there are two Tivoli regions, Baltimore and Seattle. Region Baltimore contains one client, Bulldog. Region Seattle contains one client, Beagle. you can use Bulldog,

which resides in region Baltimore, to schedule a job to be run on Beagle, which resides in region Seattle. The scheduler in region Baltimore then runs the job on Beagle.

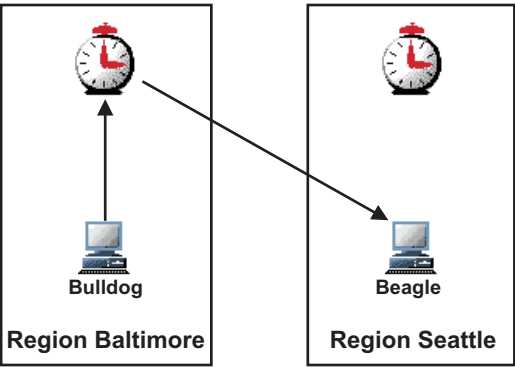
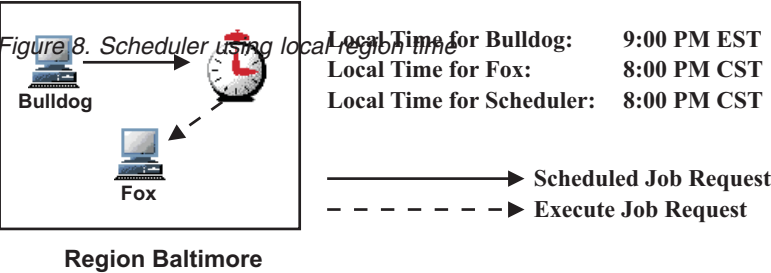


Figure 7. Multiple regions with cross Scheduler operations

Specifying job start times among regions

The start times for jobs residing in a Tivoli region are specified using the local time of the region.



For example, you use Bulldog to schedule a job to be run on Bulldog, which is in the Eastern Standard Time (EST) zone. The scheduler, however, resides on Fox, which is set up for Central Standard Time (CST). The scheduler runs the job at 8:00 p.m. CST; therefore, the job run on Bulldog occurs at 9:00 p.m. EST.

Chapter 11. Distribution management

Tivoli Management Framework provides multiplexed distribution services to enable distributions of large amounts of data to multiple targets in the enterprise. A number of profile-based applications uses these services to maximize data throughput across large, complex networks.

Multiplexed distribution is the general distribution mechanism provided by Tivoli Management Framework and used by Tivoli applications. There are two distribution services—MDist and MDist 2. Both services use a hierarchy of repeaters to fan out to a large number of targets. Each service limits its own use of the network, as configured through repeater parameters, to help prevent intense network activity that can stress network bandwidth for periods of time.

This chapter provides information and procedures for using the multiplexed distribution services, including the following topics:

- Creating a repeater
- Configuring, or tuning, repeaters for distributions
- Using the consoles supported by the MDist 2 service

For detailed information about the multiplexed distribution services, information about planning repeater hierarchies, and information about network communication, refer to *Tivoli Management Framework Planning for Deployment Guide*.

Before using a distribution service

Before submitting a distribution ensure that the following conditions are met:

- The repeater hierarchy meets the networking needs of your environment. To determine which distribution service an application uses, refer to the documentation for that application.
- The repeaters in the repeater hierarchy are correctly configured. Although an application uses only one service for each distribution, both services share the same repeater hierarchy and can be active at the same time. If an application uses both services, configure each repeater for both services.
- If an application uses the MDist 2 service, ensure that the following components are installed:
 - An RDBMS database, which stores distribution and target status. For details about creating the database for the MDist 2 database and for disk space requirements, refer to *Tivoli Enterprise Installation Guide* and *Tivoli Management Framework Release Notes*.
 - The Distribution Status console, which provides administrators with reporting and control over software distributions. For details about installing the consoles, refer to *Tivoli Enterprise Installation Guide*.
 - The Mobile Computing console, which provides users with notification of pending distributions and enables them to control the receipt of distributions.

Creating a repeater

Repeaters relay the distribution, collect status, and return status to the Tivoli server, as well as offset the network load on other repeaters. The procedure for creating a repeater is the same whether an application uses MDist or MDist 2.

You need to create repeaters during the initial design of your repeater hierarchy. You might also need to create repeaters to service additional targets in your Tivoli region. Repeaters can be hosted on managed nodes and gateways. When you create a gateway, a repeater is automatically created. When you create a repeater on a managed node, using the **wrpt** command, the repeater depot and queue used by the MDist 2 service are created.

Note: If you create a gateway on a managed node and that managed node is already configured as a repeater, the repeater inherits the repeater configuration settings from the gateway.

Repeaters on gateways and managed nodes differ as shown in Table 1.

Table 1. Repeaters, hosting resource, network availability, targets, and log location

Host	Availability	MDist targets	MDist 2 targets	Log file
Managed node	Stops 20 minutes after the queue is empty	Repeaters and managed nodes	Repeaters	\$DBDIR/rptlog (MDist 2 only)
Gateway	Always available	Repeaters, managed nodes, and endpoints	Repeaters and endpoints	\$DBDIR/gatelog

The following table provides the context and authorization role required for this operation.

Activity	Context	Required role
Create a repeater	Tivoli region	senior or super

To create a repeater on a managed node, follow these steps.

1. Ensure that your system environment is set correctly. For details, refer to “Setting Tivoli environment variables” on page 1.

2. Create the repeater:

```
wrpt -n repeater_name range=value
```

where *repeater_name* is the name of the repeater, and *value* specifies the dispatcher numbers in the distribution range for the new repeater.

To obtain a dispatcher number, follow these steps:

- a. Enter the following command:

```
odadmin odlist
```

- b. Specify the **range** values in ascending order as follows:

- For nonconsecutive dispatcher numbers, separate each number with a comma, such as range=5,7,33.
- For consecutive dispatcher numbers, enter a range of dispatcher numbers, such as range=5-7,33,35-38.

Because the Tivoli server is a repeater by default, it can distribute data to the new repeater. In turn, the repeater distributes the data to the targets specified in **range=value**.

3. Verify that the repeater was created successfully:

wrpt

The system displays the host numbers for all repeaters, gateways, and managed nodes in a region.

Output similar to the following is displayed:

```
fuji      [1]  wd []
lazzaro   [2]  -- [2-14,18,20-40]
```

where the first column displays the repeater name followed by its dispatcher number in square brackets ([]). The first entry in the second column can be a **w** or a hyphen (-). A **w** indicates that the entry is a wide area network (WAN) entry site. If the second entry in the second column is a **d**, the entry is the default repeater for the region. The third column contains the range of hosts that are served by the repeater. If no range is specified ([]), the repeater is the only repeater in the region.

After you create a repeater, you must configure it. MDist and MDist 2 services share the same repeater hierarchy but have different configuration options. This means that if Tivoli applications are running both MDist and MDist 2 in your Tivoli region, a repeater for both distribution services must be configured.

Configuring repeaters for MDist

To configure a repeater for MDist distributions, set the tuning options to adjust the flow of the data distribution. You can adjust these options to set the amount of system resources that the repeater can use (disk space, memory, open connections, and so on). You also can configure the disk threshold, working directory, and disk usage rate for each repeater.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Configure a repeater for MDist	Tivoli region	senior or super

To configure a repeater for MDist, use the **wrpt** command. The syntax for this command is as follows:

```
wrpt -t name [-k dist_id] [reinit | key=value ...]
```

where:

-k *dist_id*

Causes the specified keyword values to affect only the active distribution specified by *dist_id*, the unique process number of an active distribution. To obtain the *dist_id*, enter:

```
wrpt -L
```

name Specifies the label, object ID, or managed node ID of the repeater.

reinit Resets options to their default values.

-t When no other options are listed, returns the configurations currently in use.

key=value

Changes one or more keywords to the specified values. If you do not specify a value, existing values for the specified repeater are displayed. Refer to the following sections for descriptions of the keywords. You can specify more than one keyword and value.

The following list describes the keywords and values used by the **wrpt** command to configure repeaters for distributions:

net_load

The maximum amount of data, in kilobytes per second, that a repeater sends to the network for each distribution. Although the maximum value for **net_load** is 32 megabytes per second, most operating systems cannot process data this fast.

You can specify a negative value for **net_load** to enable the net load for *each* target, rather than for the entire distribution. If you set **net_load** to -25 (negative 25), data transfers to each target are limited to writing no more than 25 kilobytes per second.

net_spacing

The delay, in milliseconds, to insert between each write to the network. For most networks, a value of 0 (zero) is acceptable. If network collisions occur, use this keyword to evenly space transfers.

The **wrpt -t** command does not display a value for the **net_spacing** keyword unless you change the default configuration for a repeater.

stat_intv

The timeout value, in seconds, after which a blocked connection is considered inactive. This keyword is valid for repeaters on managed nodes only. Use the **wgateway** to set session timeout values for repeaters on gateways.

max_conn

The maximum number of simultaneous connections initiated by the repeater during a distribution.

mem_max

The maximum amount of memory allocated to the repeater during a distribution.

disk_max

The maximum amount of disk space allocated to the repeater during a distribution.

disk_dir

The temporary paging space allocated for a distribution.

disk_hiwat

The speed at which disk space is used by a distribution.

disk_time

The time delay between disk allocations for a distribution.

Use the **wrpt -T** command to set a final timeout value for the repeater. This timeout value is the maximum time (in seconds) that a repeater node waits after a distribution for final processing on the target to complete before an error forces the

termination of the connection. A final timeout value of 0 indicates that there is no final timeout for the repeater, meaning that it will wait forever.

For complete information about the **wrpt** and **wgateway** commands, refer to *Tivoli Management Framework Reference Manual*.

Configuring repeaters for MDist 2

MDist 2 enables you to control the total amount of resources used by a repeater. This makes distributing data fast and efficient, improving performance and throughput. This section describes how to configure repeater parameters for MDist 2. You can set the network load, target network load, number of priority connections, packet size, debug level, maximum memory, and maximum disk space. You also can set intervals for how often the database is updated and the frequency and length of time that a repeater retries unavailable or interrupted targets.

Note: Total resource limits for memory, disk space, and connections apply to all distributions active on a repeater. In the MDist service, these limits are only per distribution.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Configure a repeater for MDist 2	Tivoli region	senior or super

To configure a repeater for MDist 2, use the **wmdist** command. The syntax for this command is as follows:

```
wmdist -s [name | default | all] [key=value ...]
```

where:

name Specifies the label, object ID, or managed node ID of the repeater.

default

Sets values for any newly created repeaters. This option does not change existing repeater configuration parameters.

all

Sets values for existing repeaters. This option does not change new repeater default values. It enables you to set duplicate repeater parameters on all repeaters in your Tivoli region with one command. For example, you can set the cache size for all repeaters in your Tivoli region.

-s

When no other options are listed, returns the configurations currently in use.

key=value

Changes one or more configuration keywords to the specified values. If you do not specify a value, existing values for the specified repeater are displayed.

The following list describes the keywords and values used by the **wmdist -s** command to configure repeaters for distributions:

net_load

The maximum amount of network bandwidth that a repeater can allocate. The default is 500.

Note: When the distribution is over a slow link (where **slow_link=TRUE**), the network load is measured in bytes per second (bytes/sec) instead of kilobytes per second (KB/sec).

target_netload

The maximum amount of network bandwidth that a repeater can send to an individual target

Note: Both **net_load** and **target_netload** can be active at the same time.

send_timeout

The timeout, in seconds, between network writes

conn_retry_interval

The interval, in seconds, before an attempt is made to resend the distribution in the repeater queue. The default is 300.

This keyword replaces the gateway **session_timeout** keyword used by MDist.

execute_timeout

The timeout, in seconds, between when all the data is sent and the method returns. The default is 600.

This keyword replaces the **final_timeout** keyword used by MDist.

max_session_high

The maximum number of connections that the repeater can open for high-priority distribution.

max_sessions_medium

The maximum number of connections that the repeater can open for medium-priority distribution.

max_sessions_low

The maximum number of connections that the repeater can open for low-priority distribution.

Note: For the maximum connections keywords to take effect, restart the repeater. These keywords replace the **max_conn** keyword of the **wrpt** command.

disk_max

The maximum amount of disk space allocated to the repeater depot. If set to zero, no limit is enforced. The default is 500 megabytes.

mem_max

The maximum amount of memory used to buffer data being sent to targets. The memory is shared among all active distributions. The default is 64 megabytes.

Note: For **disk_max** or **mem_max** to take effect, restart the repeater. These keyword replaces the **disk_max** and **mem_max** keywords of the **wrpt** command.

notify_interval

The frequency, in minutes, that a repeater reports status to the distribution manager to update the database. The default is 30.

conn_retry_interval

The frequency, in seconds, that a repeater retries unavailable or interrupted targets. The default is 900.

retry_ep_cutoff

The length of time, in seconds, that a repeater continues to retry unavailable or interrupted targets. The default is 7200.

packet_size

The number of kilobytes written to the network during each distribution.

Note: When the distribution is over a slow link (where **slow_link=TRUE**), the network load is measured in bytes per second (bytes/sec) instead of kilobytes per second (KB/sec).

debug_level

The level of messages written to the log file on a managed node repeater (the `$DBDIR/rpt2log` file), where 0 represents the least information and 9 represents the most information. The default is 3.

Logging for a gateway repeater is controlled by the **debug_level** keyword of the **wgateway** command.

For more information about the **wmdist**, **wrpt**, and **wgateway** commands, refer to *Tivoli Management Framework Reference Manual*.

Setting the depot directory

Use the **wmdist** command with the **-s rpt_dir** option to specify the parent directory used to hold the depot directory and the states directory. The depot directory contains all the segments stored in the database and must have enough free space to hold the **disk_max** value. The states directory contains the database that holds the persistent state of the repeater queue.

Note: You must restart the repeater for any change to take effect.

The default directories for the depot and states directories are the `rpt_dir/depot` directory and the `rpt_dir/states` directory respectively.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Configure a repeater depot	Tivoli region	senior or super

Setting permanent storage

Use the **wmdist** command with the **-s permanent_storage** option to store data segments in a depot for an indefinite period of time. If set to **TRUE** (the default value), the depot retains segments marked for permanent storage by applications after their distribution completes. If set to **FALSE**, the distribution segments are deleted after the repeater finishes sending the distribution to all its targets.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
Set permanent storage in a repeater depot	Tivoli region	senior or super

The following examples depict typical scenarios:

- To set **permanent_storage** to TRUE for all repeaters on a Tivoli region, enter the following command:

```
wmdist -s all permanent_storage=TRUE
```

where **-s all** specifies all repeaters, including the default settings.

- To disable permanent storage in the depot of a repeater named lazzaro, enter the following command:

```
wmdist -s lazzaro permanent_storage=FALSE
```

Configuring repeaters for multicast

Configuring a repeater for multicast involves the **wmcast** and **wmdist** commands. Use the **wmdist** command to enable the repeater for multicast distribution. Use the **wmcast** command to set the configuration parameters for multicast distributions. For complete details on the commands and keywords used throughout this section, refer to *Tivoli Management Framework Reference Manual*.

To enable a repeater for multicast, use the **wmdist -s** command with the following keywords:

repeater_multicast

Whether the repeater sends distributions to other repeaters using multicast. The default is false.

endpoint_multicast

Whether the repeater sends distributions to endpoints using multicast. The default is false.

default_multicast

Whether the default distribution behavior is multicast. The default is false.

fail_unavailable

Whether the repeater will resend failed distribution to endpoints using unicast. The default is true.

To set ports and addresses, use the **wmcast -s** command with the following keywords:

mcadvert

The address used to send multicast advertisements. The default is 224.0.1.118.

port The port number used for multicast advertisements and data. The default is 9499.

mclo

The lowest address used to send multicast data. The default is 224.2.128.0.

mchigh

The highest address used to send multicast data. The default is 224.2.255.255.

ifsrcaddr

The IP address of the source host interface that is used to send multicast packets. The default is 0.0.0.0.

ifrcvaddr

A semicolon-separated list of IP addresses that the receivers use when listening for multicast packets. The default is 0.0.0.0.

returnIP

The IP address on the server to which receivers communicate. The default is 0.0.0.0.

To set timeouts, use the **wmcast -s** command with the following keywords:

connwtout

The time, in milliseconds, that a multicast sender waits for a receiver to establish a connection. The default is 2000.

dtwtout

The time, in milliseconds, that a receiver waits before timing out if a data transmission is interrupted. The default is 3000.

relwtout

The time, in milliseconds, that a sender waits for the receiver to release the connection after all data is transmitted. The default is 2000.

backofftm

The maximum interval, in milliseconds, that a sender waits before sending more packets. The default is 100.

To specify the retry settings before the multicast operation is abandoned, use the **wmcast -s** command with the following keywords:

connrtry

The number of times a multicast sender will rebroadcast a connection message to receivers. The default is 5.

dtrtry The number of times a multicast sender will resend dropped packets to receivers. The default is 10.

pollrtry

The maximum number of times a multicast receiver will poll receivers to determine their final status. The default is 5.

relrtry The number of times a multicast receiver will broadcast the connection-release message to receivers. The default is 5.

To limit the number of hops, use the **wmcast -s** with the following keyword:

tll The time-to-live integer, which is the number of times a packet can be forwarded by routers. The default is 5.

To set message, block, and buffer sizes, use the **wmcast -s** command with the following keywords:

blocksize

The size, in bytes, of the block used by the sender when writing data to the network. The default is 1460.

rcvbufsz

The size, in bytes, of the receive buffer of the UDP socket. The default is 250000.

sndbufsz

The size, in bytes, of the send buffer of the UDP socket. The default is 250000.

repeat The number times the server sends the same control packets. The default is 2.

Configuring endpoints for multicast

By default, all endpoints can receive multicast distributions. The settings that an endpoint uses for receiving multicast distributions are stored in the `last.cfg` file of an endpoint.

These settings can be modified using the **wep** command with the **set_config** option with the following keywords:

depot_dir

The directory where multicast distributions are stored until they are installed. The default is `$LCF_DATDIR/depot`.

log_threshold

The level of detail written to trace files for the endpoint. The default is 1.

For details about the **wep** command, refer to *Tivoli Management Framework Reference Manual*.

Use a text editor to modify the `$LCF_DATDIR/mcast/mcast_receiver.cfg` file. Set the value for **timeout** to specify the time, in milliseconds, that the receiver waits for the next incoming data or request after receiving the previous one. When the time period elapses, the connection from receiver to sender is closed.

Configuring endpoints to install from file servers

If an administrator wants a user to install a distribution from a file server, the `$LCF_DATDIR\remote.dir` file must exist on the target computer system. The `remote.dir` file contains a list of file servers, one per line.

For example, you can configure all computer systems in one branch office to use one file server, while other branch offices use different file servers. The following is an example of the contents of a `remote.dir` file:

```
\\lethe.dallas.ibm.com\scratch
\\styx.houston.ibm.com\share
\\acheron.waco.ibm.com\data
```

The MDist 2 service first looks for contents of the distribution on the `lethe` server in the `scratch` directory. If it does not find the file it is looking for, it searches the `styx` server in the `share` directory. If it is still not found, it searches the `acheron` server in the `data` directory.

Using the Distribution Status console

The Distribution Status console provides administrators with real-time reporting and control of profile distributions. Administrators can track the progress of a distribution, intervene (if necessary), and analyze the details of a distribution. The console provides color-coded charts and graphs to enable administrators to identify

patterns and relationships in the data. These views are helpful when identifying items of interest to be focused on, such as unavailable targets, which prevent a distribution from completing successfully.

Figure 9 illustrates the main areas of the console.

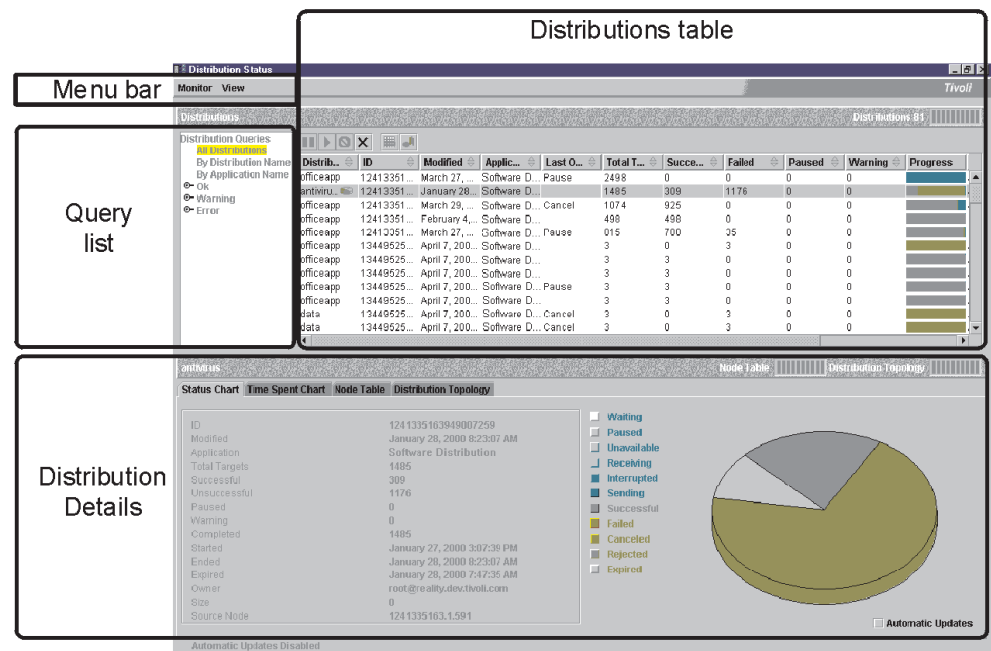


Figure 9. Distribution Status console

Note: To monitor status and control distributions, a database is required. For MDist 2 installation information, refer to *Tivoli Enterprise Installation Guide*.

Starting the Distribution Status console

Use the Distribution Status console to track a distributions, view their progress, and intervene, if necessary. You can log in to any managed node that has a Tivoli desktop and has access to the database.

Although the Distribution Status icon appears on all desktops, it is only available when the console is installed on the same system where the Tivoli desktop is running. On UNIX operating systems, this is the system where you started the Tivoli desktop. If you are running Tivoli Desktop for Windows, this is the system where Tivoli Desktop for Windows is installed, not the managed node where it logs in.

The following table provides the context and authorization role required for this operation.

Activity	Context	Required role
Start the Distribution Status console	Tivoli region	RIM_view or senior

You can start the Distribution Status console from the Tivoli desktop or the command line. However, before you start the console, check the following:

- If you start the console on a UNIX operating system, you must enable connections to the X Window System. This is necessary even if the console runs on the same machine as the X Window System display. To do this, follow these steps:
 1. Set the DISPLAY variable to the computer system that you want to display the Distribution Status console.
For example, to open the console on the X Window System display named zeus:0.0, a Bourne or Korn shell user would enter:

```
DISPLAY=zeus:0.0
export DISPLAY
```
 2. Enable remote connections to the X Window System. For example, to start the Distribution Status console on the zeus display, enter:

```
xhost +zeus
```
- Ensure that remote logins are enabled. To ensure that remote logins are enabled, enter:

```
odadmin odinfo
```

The following message is displayed:

Remote client login allowed = *value*

where *value* is TRUE, FALSE, or version_2.

If this value is FALSE, set the value using the following command:.

```
odadmin set_allow_rconnect value
```

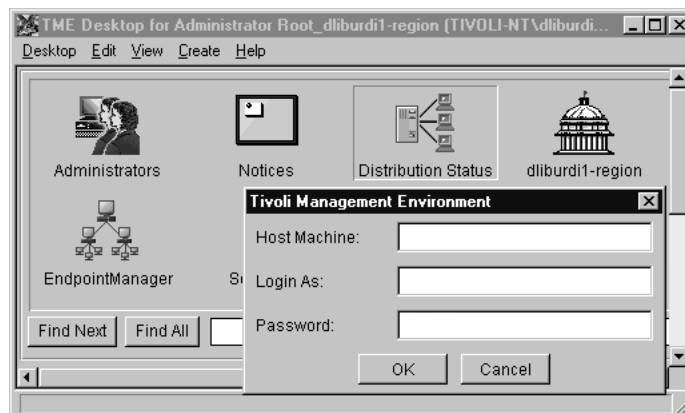
where *value* is TRUE or version_2. For more information about the **odadmin** command and options, see *Tivoli Management Framework Reference Manual*

For installation instructions, see *Tivoli Enterprise Installation Guide*.

Desktop

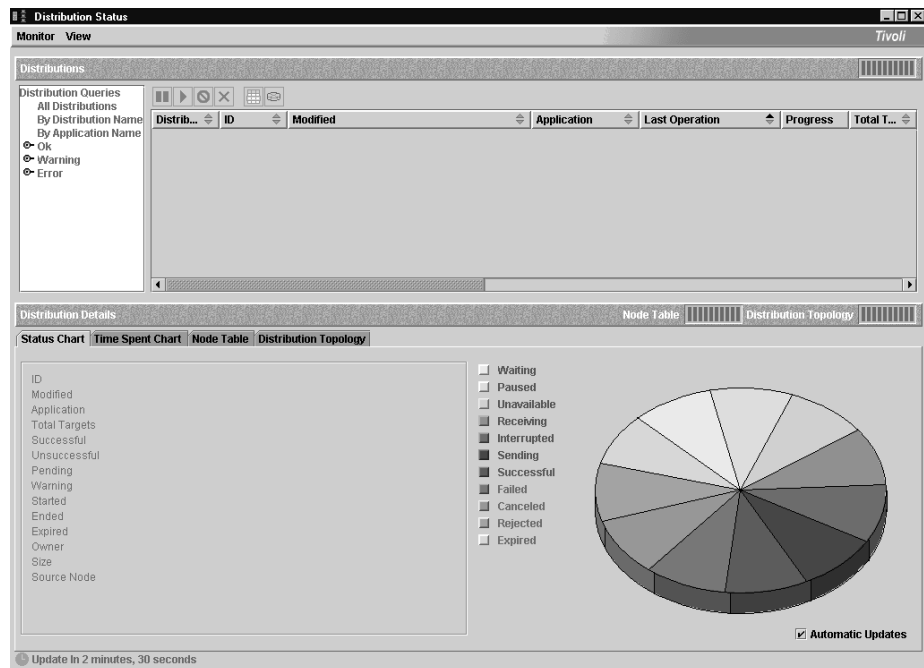
To start the Distribution Status console, perform the following steps:

1. From the Tivoli desktop, double-click the Distribution Status icon to display the login.



2. In this window, perform the following steps:
 - a. In the **Host Machine** field, type the fully qualified host name of the managed node. Do not type the IP address.
 - b. In the **Log In As** field, type your domain-qualified user name (Windows) or account name (UNIX) for the managed node. This field is case sensitive.
 - c. In the **Password** field, type the password for the specified user or account. This field is case sensitive.

- d. Click **OK** to display the Distribution Status console.



Notice that the interface does not contain distribution data when you initially start it. This is so that you do not have to wait for your system to load all distributions. With sometimes thousands of distributions in one state or another, this default setting enables you to query only the distributions you want to view.

Command line

Use the **wmdistgui** command to start the Distribution Status console from the command line.

To start the Distribution Status console, perform the following steps:

1. Ensure that your system environment is set correctly. For details, refer to “Setting Tivoli environment variables” on page 1.
2. Enter the following command to start the console:
`wmdistgui`
3. In this window, perform the following steps:
 - a. In the **Host Machine** field, type the fully qualified host name of the managed node. Do not type the IP address.
 - b. In the **Log In As** field, type your domain-qualified user name (Windows) or account name (UNIX) for the managed node. This field is case sensitive.
 - c. In the **Password** field, type the password for the specified user or account. This field is case sensitive.
 - d. Click **OK** to display the Distribution Status console.

Note: For information about the **wmdistgui** command, refer to *Tivoli Management Framework Reference Manual*.

Viewing distribution status

You can submit a distribution and later check to see whether the distribution completed on its targets. The database associated with MDist 2 enables you to view the status of a distribution.

The following table provides the context and authorization role required for this operation:

Activity	Context	Required role
View one or more distributions	Tivoli region	RIM_view or senior

You can view distribution status from the Distribution Status console, command line, or a custom SQL script.

Desktop

To view one or more distributions in the Distribution Status Console, select a query from the query list. For example, select **All Distributions** to display distributions in the Distributions table as shown.

The screenshot shows the Tivoli Distribution Status console. The top section displays a table of distribution queries with columns: Name, Last Operation, Progress, Total T..., Successful, Unsuccessful, Pending, and Warning. The 'All Distributions' query is selected, showing a progress bar at 95.7% Successful. The bottom section shows a detailed view of the 'All Distributions' query, listing nodes and their status (e.g., reality, zyrus-4, futura-30, etc.). The console includes a sidebar with navigation options like 'Monitor', 'View', and 'Tivoli'. The bottom status bar indicates 'Update in 2 minutes, 5 seconds' and 'Automatic Updates'.

Note: To rearrange columns in the table, select the column heading and drag it to the desired position. If you want to sort a column, click the arrow next to the column heading. An up arrow indicates ascending order; a down arrow indicates descending order.

Command line

For information about using the **wmdist** command to view the status of one or more distributions, refer to *Tivoli Management Framework Reference Manual*.

Viewing details of a distribution

Use the Distribution Status console to view details of a specific distribution. Double-click the distribution you want to view or select the distribution and click the Display Selected Distribution Details icon.

You can display only one distribution at a time. For example, to view details of the antivirus distribution, double-click the distribution in the Distributions table. Notice that a pie-chart icon appears next to the name of the distribution. This name is displayed on the title bar of the Distribution Details dialog as shown in Figure 10.

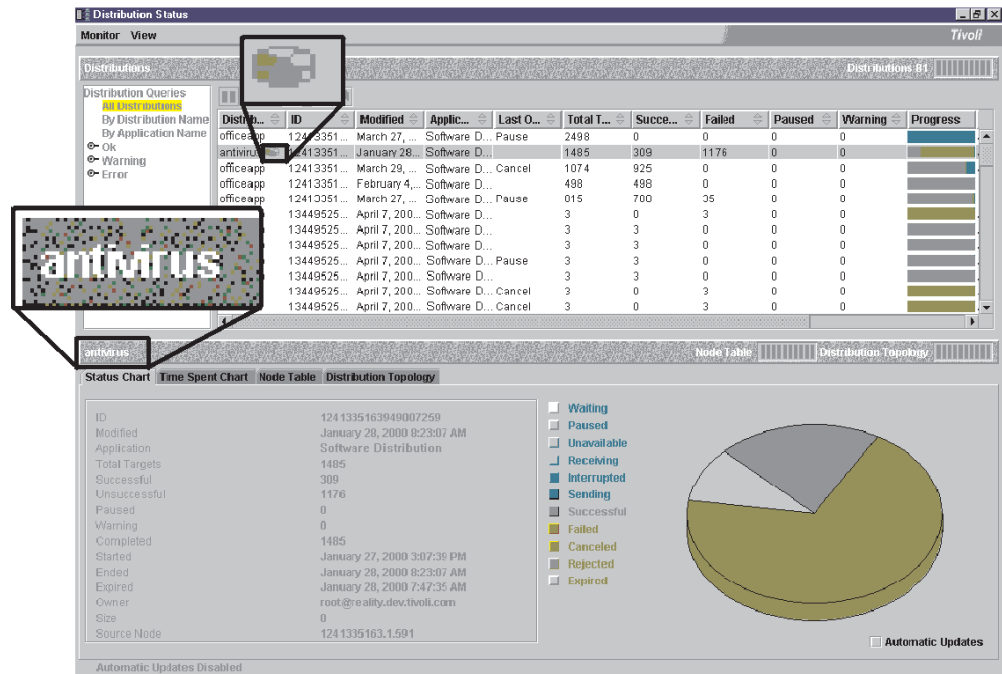


Figure 10. Viewing distribution details

When you select a tab, the Distribution Details area of the console displays a view. The sections that follow describe the following Distribution Details views:

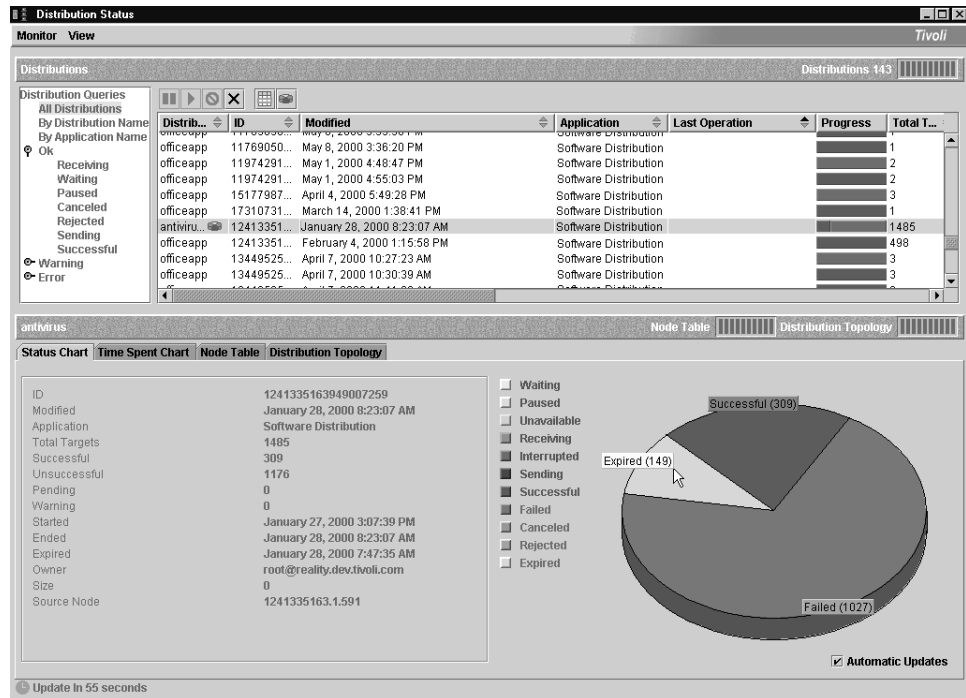
- Status Chart
- Time Spent Chart
- Node Table
- Distribution Topology

Status Chart view

The Status Chart view displays a color-coded pie chart representing the states of targets for a selected distribution. You can identify the overall status of the distribution or move the cursor over a section of the chart to view the total number of targets in that particular state. Distribution statistics are also displayed, such as the date the distribution was started and the administrator who started it.

To view the status of targets for a specific distribution, follow these steps:

1. Double-click a distribution in the Distributions table. The Status Chart view is displayed by default.



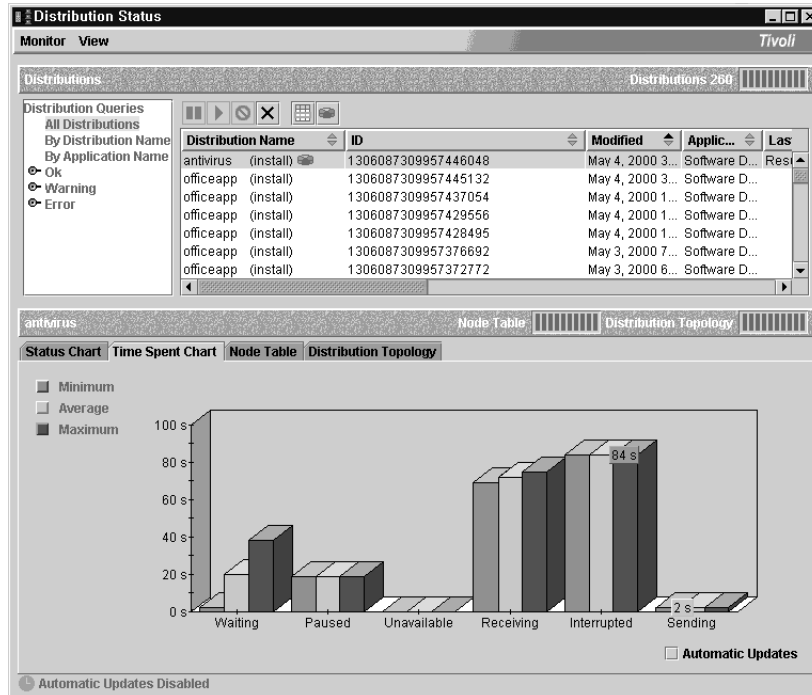
2. To display the name of the state and the total number of targets in each state, move your cursor over sections of the pie chart.

Time Spent Chart view

The Time Spent Chart view displays a bar chart, which indicates the amount of time spent in each stage of the completed distribution. This view displays the minimum, average, and maximum amount of time (in seconds) a distribution was in a given state.

To display the amount of time spent in a specific state, follow these steps:

1. Double-click a distribution in the Distributions table.
2. Click the **Time Spent Chart** tab. The Time Spent Chart view is displayed.



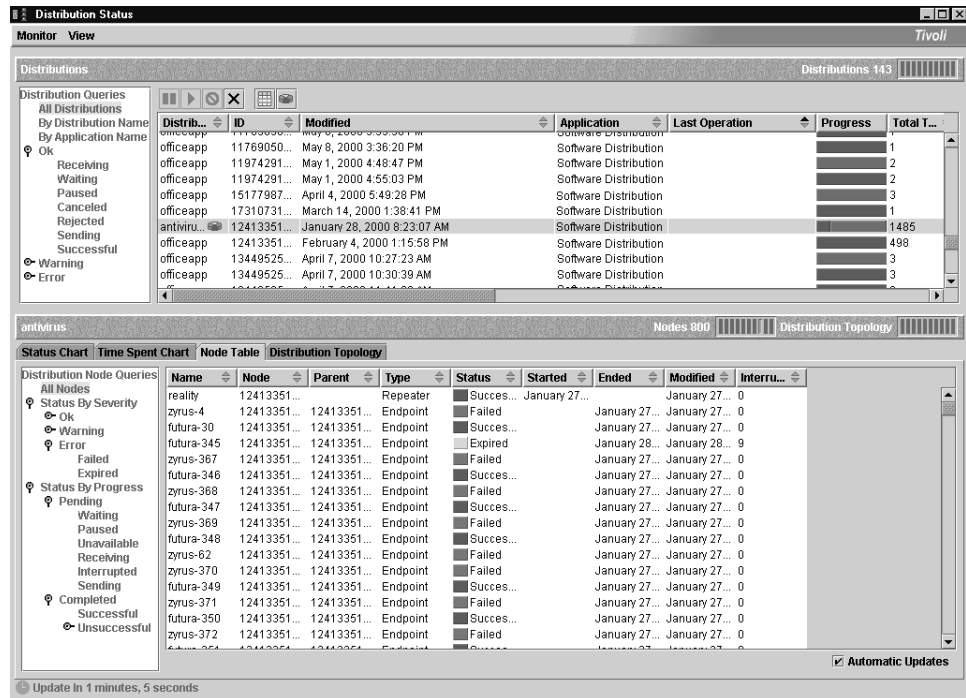
3. To display the number of seconds that the targets were waiting, move your cursor over the bars in the chart.

Node Table view

The Node Table view works the same way as the Distributions table. However, instead of querying distribution status, it queries the states of repeaters or endpoints associated with a specific distribution.

To display target information for a specific distribution, follow these steps:

1. Double-click a distribution in the Distributions table.
2. Click the **Node Table** tab. The Node Table view is displayed.



3. To display data for the selected distribution, select one of the distribution node queries from the list. For example, click **All Nodes** to display a table that shows information about each target in the selected distribution. You also can use the query list to filter target data displayed in the table. For example, to view only failed targets in the selected distribution, click **Error** and then click **Failed**.

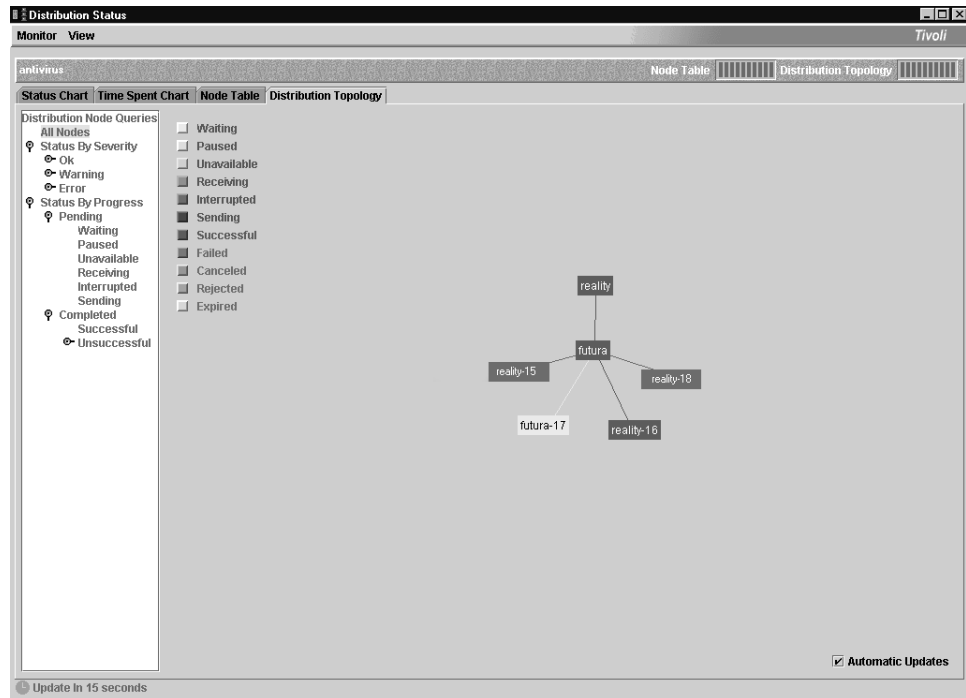
Distribution Topology view

The Distribution Topology view displays a tree view showing the data structured as nodes and links. *Nodes* refer to repeaters and endpoints in the currently selected distribution. *Links* show the relationship between the nodes in the distribution hierarchy. These objects are color-coded so that you can quickly identify the state of a node. The lines that link nodes in the hierarchy are also colored to display relationships between connecting nodes.

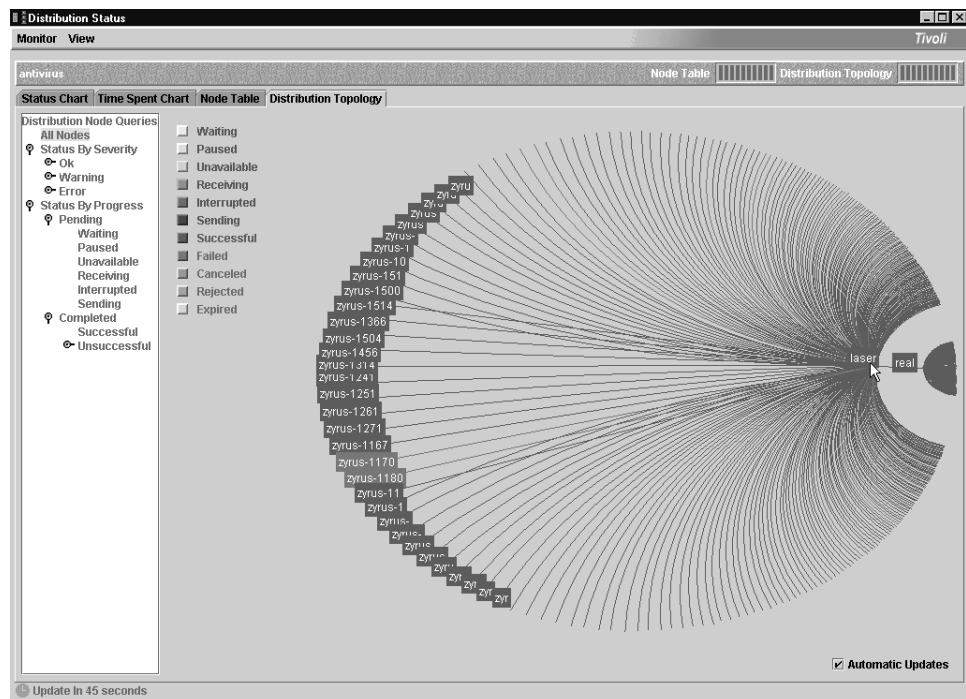
Use this view to gain an understanding of the distribution route and to show relationships that help identify items to focus on. For example, you can identify bottlenecks that prevent a distribution from completing.

To display all targets in a distribution, follow these steps:

1. Double-click a distribution in the Distributions table to view detailed information about it.
2. From the **View** menu, select **Distribution Details** to display only the Distribution Details views. This step is optional.
3. Click the **Distribution Topology** tab. Target objects are displayed with the source host at the center as shown. To move another node to the center of the tree view, click on it.



4. To display data for the selected distribution, select one of the distribution node queries from the list. For example, click **All Nodes** to display all targets in the selected distribution.
5. To view other targets, navigate the tree by dragging its objects.



6. To view information about a specific node, double-click the object. The Node Properties dialog is displayed.

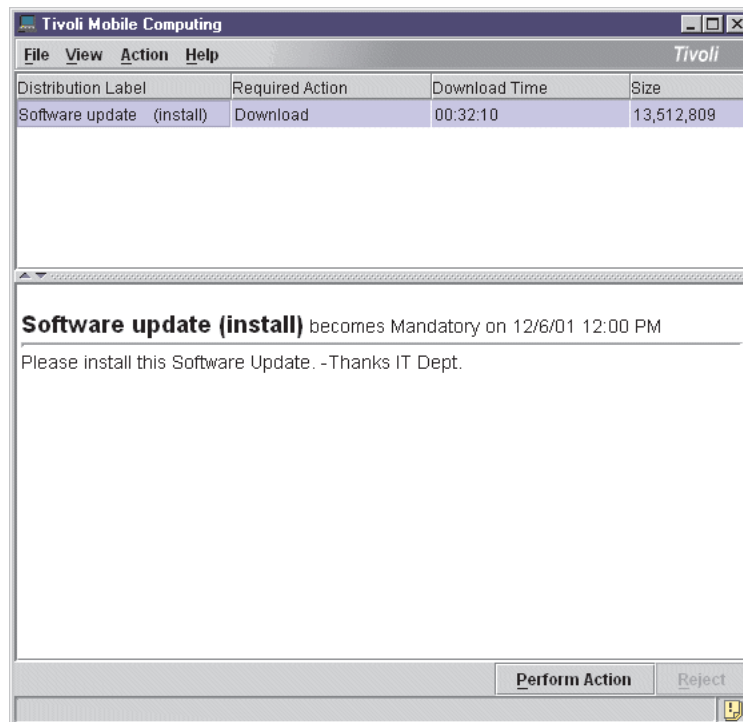


Mobile Computing console

The Mobile Computing console provides users with notification and control of distributions sent to their Windows endpoints. This console enables mobile users the flexibility to install distributions at their convenience.

The following illustration shows the two main panes of the console. The top pane, called the distributions table, lists information in a table about distributions waiting to be installed. This table displays distributions stored on the network or saved locally in a storage directory.

The bottom pane enables users to view important messages that are attached to specific distributions. For example, the user might be required to insert a CD or install a distribution by a specific date. Users also can select from the **View** menu to add columns to or remove columns from the distributions table.



Users can view distributions queued at the gateway, sort them by different criteria, and perform actions on the distributions, such as the following:

- Install and run distributions that are on a network, file server, or CD.
- Download and store distributions locally, for installation at a later date.

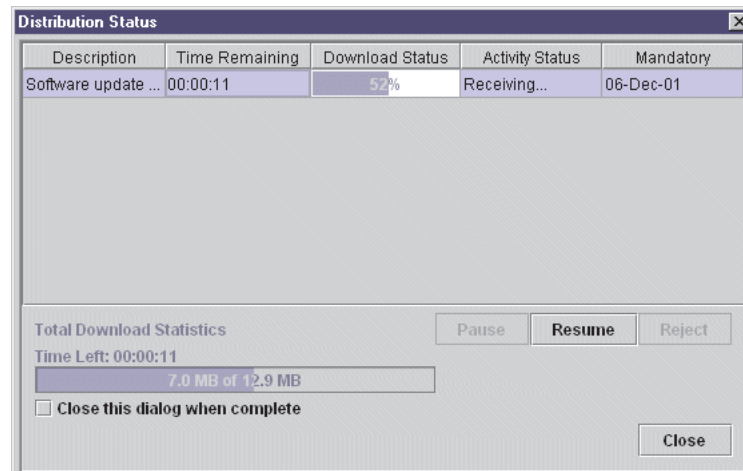
- Install distributions if and when they want to (unless the distribution is mandatory).
- Reject pending distributions that are not mandatory.
- View the status of current distributions.
- Set user preferences, such as playing sound when a new distribution arrives.
- View distribution properties, such as a distribution's label, size, and expiration date.
- View messages sent by the administrator.
- View the history of past user actions.

For instructions on how to perform these operations in the console, consult the online help.

Notes:

1. To install and run a distribution immediately, the required authorization is the same as for an installation that does not use the Mobile Computing console.
2. When a mobile user chooses to download a distribution and install it later, the operating system determines the authorization required for the installation. Depending on the software being installed, administrator privileges might be required. The user who starts the installation (not the user who originally downloaded the distribution) must have the required privileges for the installation.

The Mobile Computing console enables users to control distributions during download. For example, the following distribution was paused in the middle of a download. When the system reconnects, the user can resume downloading the distribution from where it was stopped.



Remember that although the console gives users the ability to control distributions, the administrator can choose to retain control of a distribution by specifying that it be hidden or mandatory. The administrator also can disable functionality in the console by editing the `mobile.cfg` file, located on the endpoint (refer to “Configuring the Mobile Computing console” on page 160).

Hidden distributions are automatically downloaded and run when its targets connect. The distribution is hidden in that the distribution is invisible to the user. For example, an administrator can send an inventory scan that gathers information about hardware and software on a specific workstation.

In contrast to hidden distributions, users are informed when they receive a *mandatory distribution*. A notification message is displayed each time the console starts, informing the user of any mandatory distributions that are pending. Administrators also can send escalation messages, reminding users that a mandatory distribution requires their attention. If the distribution is not installed by the date specified, it is installed automatically, regardless of whether the mandatory distribution resides on the gateway or in a storage directory.

Note: For more information about sending MDist 2 distributions to systems with the Mobile Computing console installed, consult the documentation that came with your Tivoli application.

Configuring the Mobile Computing console

After you install the console on specified endpoints, you can configure the console to set limits on the operations that the users can perform. This is accomplished by editing the `mobile.cfg` file, installed on the endpoint in the system root directory (`../Tivoli/mobile/mobile.cfg`).

An example of the `mobile.cfg` file is as follows:

```
From=true
Priority=true
connectionSpeed=7
upcallTimeout=60
allowColumn=true
maxHistory=100
NoteIcon=true
confirmCancel=true
allowAdvanced=true
Mandatory=true
agentPort=2644
alwaysReceive=false
pollInterval=10
Escalation=true
displayIcon=true
ID=true
lastMeasuredKey=64.34165360527052
playSound=false
epHostname=anbose.dev.tivoli.com
allowReject=true
showMessage=true
Sent=true
allowGeneral=true
depotDirectory=d:\\data\\anbose\\0205\\dat\\3\\depot
Expires=true
logsize=1000
disconnectedMessage=true
showCloseCheckBox=false
guiStartTimeout=30
clientBootDelay=1
supressMandatoryPopUps=true
disableTimeRemainingColumn=true
showMenu=true
allowCloseMandatory=false
extraStatus=true
showPauseOnly=true
```

Note: These statements can be in any order.

Descriptions of statements that administrators can include in the `mobile.cfg` file are as follows.

agentPort

Specifies the port on which the console contacts the mobile computing agent. It is important that you do not change this value. If this value is changed, reboot the computer to reinstate the original value.

allowAdvanced

If true, the user can select the **Advanced** tab on the Preferences notebook. If false, the **Advanced** tab is inaccessible to the user.

allowCloseMandatory

If set to false, and if a mandatory distribution has not been installed by its due date, this option suppresses the normal “new distribution available” message that would ordinarily display, and launches the GUI and waits for users to install the past-due, mandatory distribution. Users cannot close the GUI until the package is installed. If the user attempts to exit the GUI, a message is displayed to inform them which distributions must be installed. The message content is specified on the **closeMandatoryMessage=** option in the mobile.cfg file. The message text can include simple HTML tags to format the message. A sample message could be as follows:

```
closeMandatoryMessage="The following distributions <strong>must<strong>  
be installed before you can exit the mobile computing GUI:"<br>
```

Note: the GUI is not necessarily updated in real time. Due to its distributed nature, the GUI cannot always be aware of jobs that might be pending on a gateway. If the GUI is not aware of a job, it cannot determine if the past due date has expired and enforce the **allowCloseMandatory=false** setting.

The default is true, meaning that users can close the mobile GUI, even if there are past-due mandatory distributions waiting.

allowColumn

If true, the user can select column check boxes in the **View** menu. If false, the column check boxes in the **View** menu are inaccessible to the user. These check boxes enable the user to add columns to or remove columns from the distributions table.

allowGeneral

If true, the user can select the **General** tab on the Preferences notebook. If false, the following settings apply:

- The **General** tab is inaccessible to the user.
- The **Don't show this again** checkbox does *not* appear on the Mobile Computing dialog box that displays when a new distribution arrives.

allowReject

If true, the user can use the **Reject** button on the main console window to reject non-mandatory distributions. If false, the **Reject** button is inaccessible to the user.

alwaysReceive

If true, the console automatically downloads and installs all distributions sent to the computer. If false, normal distributions remain on the gateway until the user resumes it.

clientBootDelay

Mobile clients might receive spurious messages telling them that “A new distribution is available” immediately following a reboot, when the reboot was triggered by a distribution that has already been received. This parameter sets the delay time, in seconds (an integer), that the Tivoli agent

must wait before it restarts. A brief boot delay (1 or 2 seconds) will prevent these spurious messages from being displayed.

confirmCancel

If true, displays a prompt before rejecting a distribution. If false, does not display a confirmation.

connectionSpeed

Specifies the dial-up connection of your computer so that the console can accurately determine the download time of a distribution. The default is 56 kilobytes.

depotDirectory

Specifies the storage directory where distributions are downloaded for installation at a later date.

disableTimeRemainingColumn

Set to **true** to hide the Time Remaining Column that ordinarily is displayed in the Progress information shown on mobile clients. Set to **false** to re-enable the time remaining column.

disconnectedMessage

If this statement is set to false, the console displays no message if it is unable to connect to the gateway.

If this statement is set to true, the console displays the following message if it is unable to connect to the gateway:

Server connection could not be established.

Only distributions stored in the local depot will be available.

To see new distributions, please establish a network connection.

You can customize this message by entering a text string rather than true, for example:

disconnectedMessage=A server connection could not be established. Contact the help desk for more information.

You can also enter HTML, such as a link to a URL. You cannot include any hard returns in the text you provide in this statement; all text must appear on one line.

displayIcon

If true, displays an icon on the Windows taskbar to notify the user of pending distributions. If false, the icon is not displayed on the taskbar.

epHostname

If true, this column is displayed in the distributions table. If false, this column is not displayed in the table. This column indicates the name given to the distribution by the administrator. Note that a distribution label might include an operation, such as accept, commit, install, remove, undo, or verify. These operations indicate tasks performed by the distribution.

Escalation

If true, this column is displayed in the distributions table. If false, this column is not displayed in the table. This column indicates if the administrator sent an escalation message with the distribution.

Expires

If true, this column is displayed in the distributions table. If false, this column is not displayed in the table. This column indicates the date that the selected distribution expires.

extraStatus=true

The mobile GUI Progress Dialog screen has a column "Activity Status" which currently gives status such as Waiting, Paused, Receiving, and Error Messages. Setting this to **true** adds additional state messages to the Activity Status column, such as "Installing". The default is **false**. The additional messages are not translated.

From If true, this column is displayed in the distributions table. If false, this column is not displayed.

guiLogLevel

Specifies the level of the GUI trace messages (0 to 4) in the mobile.log file.

guiStartTimeout

When you start mobile clients (either from Start Menu, Desktop Icon, or System Tray), this parameter determines the length of time to allow for the GUI is to start. If the GUI does not start in this time period, a message is displayed, indicating that the Mobile Computing Agent did not detect the start of the console within the required time period, and that you should reboot the computer.

On older laptops with less than 500 megs ram or less than 1GigHZ CPU, this timeout might need to be increased. If you are receiving this error, even after a reboot, and you think it is related to slow hardware, increase this timeout value.

ID If true, this column is displayed in the distributions table. If false, this column is not displayed in the table. This column indicates a unique internal tracking number associated with the selected distribution.

lastMeasuredKey

Specifies the speed of the last download. This value is used when the **Last Measured Value** choice is selected from the Preferences notebook. The console uses this value to estimate the download time displayed in the distributions table.

logLevel

Specifies the level of the agent trace messages (0 to 4) in the mobile.log file.

logsize

Specifies the maximum size in kilobytes of the mobile.log file. The mobile.log file is located in the directory where you installed the Mobile Computing console.

Mandatory

If true, this column is displayed in the distributions table. If false, this column is not displayed in the table. This column indicates the date that the distribution must be installed on your computer. The user can download and install the distribution before the specified date or do nothing and let the console download the distribution on the indicated date. Mandatory distributions run on the date specified, regardless of whether a distribution resides on the network or is stored locally in the storage directory.

maxHistory

Specifies the maximum number of entries stored in the history file, which records actions performed on the console.

NoteIcon

If true, this column is displayed in the distributions table. If false, this

column is not displayed in the table. This column indicates whether the administrator attached a note with the distribution.

playSound

If **true**, notifies the user with an audible beep when the console detects a new distribution. If **false**, this notification is not sent.

pollInterval

Specifies the length of time, in minutes (from 1 to 30), that the console checks to see if your computer has reconnected. The default is 1 minute. This enables the console to return results back to the gateway if, for example, you installed a distribution while your computer was disconnected.

Priority

If **true**, this column is displayed in the distributions table. If **false**, this column is not displayed in the table. This column indicates the priority of the distribution. Values are High, Medium, and Low.

Sent

If **true**, this column is displayed in the distributions table. If **false**, this column is not displayed in the table. This column indicates the date that the distribution was sent to the computer.

showCloseCheckBox

If **true**, the **Close this dialog when complete** check box is displayed on the console, and the console does not automatically close after distributions have downloaded. If **false**, the check box is hidden and the console automatically closes after the displayed distributions have downloaded.

showMenu

Controls whether the Mobile Computing console is displayed when the console is started. The default is **true**, which causes the console GUI to display when the console is started. Choose **false** to suppress the GUI display. If it is suppressed at start up, activate it by selecting the icon on the task bar.

showMessage

If **true**, notifies the user with a visual prompt when the console detects a new distribution. If **false**, this pop-up window is not displayed.

showPauseOnly

If **true**, this option suppresses all New Distribution pop-up messages, except for distributions in the paused state. The default is **false**, and pop-up messages are displayed for all distribution states. Set this to **true** to if you do not want to see other pop-up status messages on the mobile console when installing distributions that require one or more reboots to complete. The Mobile Computing console's **General Preferences** setting for **Display a pop-up window when a new distribution arrives** must be selected for the **showPauseOnly=true** option to work.

suppressMandatoryPopUps

If set to **true**, messages telling mobile clients which mandatory distributions waiting, are not displayed in the client GUI. **true** also prevents these messages from being recorded in the client history log. This is useful in environments where all distributions to mobile clients are mandatory, and no value is obtained from the "mandatory distribution" messages. Set to **false** to allow the messages to be displayed on the mobile clients.

upcallTimeout

Specifies the repeater timeout, in seconds (from 30 to 300), which is the

length of time that the console waits for the gateway to return the list of waiting distributions or start a distribution. The default is 1 minute. If you have a slow modem or a bad connection to the Internet, it is recommended that you increase the default value.

Starting the Mobile Computing console

To use the Mobile Computing console, the administrator first must issue the **wep** command with the **set login_mode** option to designate the endpoint as mobile. This allows a user to receive and control MDist 2 distributions through the Mobile Computing console. For information about installing and enabling an endpoint for mobile computing, refer to *Tivoli Enterprise Installation Guide*.

To start the console after it is installed, double-click the Mobile Computing icon on your Windows desktop or the Windows taskbar:



The taskbar icon changes to the following icon when there is a pending distribution:



You also can access the console from the pop-up window, the **Start** button, or add the console to the Windows **Startup** folder so that the console opens each time you start your operating system.

Appendix. Notices

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

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, 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 might 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
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

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.

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.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

AIX, AS/400, DB2, IBM, MVS, OS/2, OS/400, S/390, Tivoli, Tivoli Enterprise, Tivoli Enterprise Console, TME, TME 10, WebSphere, WIN-OS/2, and z/OS are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States, other countries, or both.

ActionMedia, LANDesk, MMX, Pentium, and ProShare are trademarks of Intel Corporation in the United States, other countries, or both. For a complete list of Intel trademarks, see <http://www.intel.com/sites/corporate/tradmarx.htm>.



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

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Glossary

A

authorization roles. A role assigned to Tivoli administrators to enable them to perform their assigned systems management tasks. A role can be granted over the entire Tivoli region or over a specific set of resources, such as those contained in a policy region. Examples of authorization roles include **super**, **senior**, **admin**, and **user**.

B

bulletin board. The mechanism by which the Tivoli Management Framework and Tivoli applications communicate with Tivoli administrators. The bulletin board collects notices in notice groups. Administrators can access the bulletin board from the Tivoli desktop. The bulletin board is an audit trail for important operations that the administrators perform.

C

Configuration Change Management System (CCMS). In a Tivoli environment, a data store of profiles that contain configuration data that is used by system management applications to make configuration changes on groups of systems. See also profile manager.

collection. A container that provides a single view of related resources.

configuration repository. The relational database that contains information collected or generated by inventory or software distribution operations.

D

default policy. A set of resource property values assigned to a resource when the resource is created. Contrast with validation policy.

Distribution Status console. An MDist 2 interface provided by Tivoli Management Framework that enables administrators to monitor and control distributions across a network. See also MDist 2.

downcall. A method call from the gateway to an endpoint. Contrast with upcall.

E

endpoint. In a Tivoli environment, the computer system that is the ultimate target for most Tivoli operations. Contrast with managed node.

endpoint list. In a Tivoli environment, A list of all endpoints in a Tivoli region with their assigned gateways. See endpoint manager.

endpoint manager. In a Tivoli environment, a service that runs on the Tivoli server, assigns endpoints to gateways, and maintains the endpoint list.

endpoint method. In a Tivoli environment, a method that runs on an endpoint as the result of a request from another managed resource. Results of the method are forwarded to the gateway and then to the calling managed resource.

F

fanout. In communications, the process of creating copies of a distribution to be delivered locally or sent over the network.

G

gateway. Software that provides services between endpoints and the rest of the Tivoli environment.

I

instance. A single occurrence of a resource.

J

job. In a Tivoli environment, a resource consisting of a task and its preconfigured execution parameters. Among other things, the execution parameters specify the set of hosts on which the job is to run.

L

lcmd. The Tivoli service that is used by an endpoint to communicate with a gateway. Contrast with oserv.

M

managed node. In a Tivoli environment, a computer system where Tivoli Management Framework is installed. Contrast with endpoint.

MDist. A multiplexed distribution service provided by Tivoli Management Framework that enables efficient transfer of data to multiple targets. Another distribution service, MDist 2, provides additional management features. See also MDist 2.

MDist 2. A multiplexed distribution service provided by Tivoli Management Framework that enables efficient transfer of data to multiple targets. Administrators can monitor and control a distribution throughout its life cycle. Another multiplexed distribution service, MDist, lacks these management features. See also Distribution Status console.

member. The contents of a collection. See also collection.

multiplexed distribution. The mechanism used by Tivoli Enterprise applications to transfer data to multiple targets. Tivoli Management Framework provides two multiplexed distribution services, MDist and MDist 2. See also MDist and MDist 2.

N

name registry. See Tivoli name registry.

notice. In a Tivoli environment, a message generated by a systems management operation that contains information about an event or the status of an application. Notices are stored in notice groups. See also bulletin board.

notice groups. In a Tivoli environment, an application- or operation-specific container that stores and displays notices pertaining to specific Tivoli functions. The Tivoli bulletin board is comprised of notice groups. A Tivoli administrator can subscribe to one or more notice groups; the a bulletin board contains only the notices that reside in a notice group to which the administrator is subscribed. See also bulletin board and notice.

NT repeater. The first Windows managed node where Tivoli Remote Execution Service is installed. Using fanout, the NT repeater distributes Tivoli Remote Execution Service to all other Windows managed nodes during the installation process.

O

object path. In a Tivoli environment, an absolute or relative path to a Tivoli object, similar to a path in a file system.

object reference. In a Tivoli environment, the object identifier (OID) that is given to an object during its creation.

object request broker (ORB). In object-oriented programming, software that serves as an intermediary by transparently enabling objects to exchange requests and responses.

oserv. The Tivoli service that is used as the object request broker (ORB). This service runs on each Tivoli server and managed node. Contrast with lcfd.

P

policy. A set of rules that are applied to managed resources. A specific rule in a policy is referred to as a policy method.

policy region. A group of managed resources that share one or more common policies and which model the management and organizational structure of a network computing environment. Administrators use policy regions to group similar resources, to define access to the resources, and to associate rules for governing the resources.

policy subregion. In a Tivoli environment, a policy region created or residing in another policy region. When a policy subregion is created, it initially used the resource and policy properties of the parent policy region. A Tivoli administrator can later change or customize these properties to reflect the specific needs and differences of the subregion.

profile. In a Tivoli environment, a container for application-specific information about a particular type of resource. A Tivoli application specifies the template for its profiles, which includes information about the resources that can be managed by that Tivoli application.

profile manager. In a Tivoli environment, a container for profiles that links the profiles to a set of resources, called subscribers. Tivoli administrators use profile managers to organize and distribute profiles. A profile manager can operate in dataless mode or database mode. created in the context of a policy region and is a managed resource in that policy region. See also Configuration Change Management System (CCMS).

proxy endpoint. In a Tivoli environment, a representation of an entity (such as a network device or a host) that functions as a subscriber for profile distribution. The proxy endpoint is created on a managed node, which performs the proxy role during profile distribution. Multiple proxy endpoints can be created on the same managed node.

pull. An operation that initiates an action by requesting it of a resource.

push. An operation that sends information to other resources.

Q

query. In a Tivoli environment, a combination of statements that are used to search the configuration repository for systems that meet certain criteria. The query object is created within a query library. See also query library.

query facility. In a Tivoli environment, a facility that enables the use of SQL functions to access information in an RDBMS Interface Module (RIM) repository.

query library. In a Tivoli environment, a facility that provides a way to create and manage Tivoli queries. See also query.

R

RDBMS. See relational database management system (RDBMS).

RDBMS Interface Module (RIM). In Tivoli Management Framework, the module in the distributed object database that contains information about the installation of the relational database management system (RDBMS).

region. See Tivoli region.

registered name. In a Tivoli environment, the name by which a particular resource is registered with the name registry when the resource is created.

relational database management system (RDBMS). A collection of hardware and software that organizes and provides access to a relational database.

repeater. In a Tivoli environment, a managed node that is configured for multiplexed distribution. A repeater receives a single copy of data and distributes it to the next tier of clients.

resource. A hardware, software, or data entity that is managed by Tivoli software products.

resource type. In a Tivoli environment, one of the properties of a managed resource. Resource types are defined in the default policy for a policy region.

RIM. See RDBMS Interface Module (RIM).

RIM repository. In a Tivoli environment, the relational database that contains information that is collected or generated by Tivoli software products. Examples of a RIM repository include the configuration repository and the event database.

root administrator. In a Tivoli environment, the account for the initial Tivoli administrator that is created during the installation of Tivoli Management Framework. This account is the equivalent of the root

user on UNIX operating systems and a member of the administrator group on Microsoft Windows systems.

S

subscriber. In a Tivoli environment, a resource that is subscribed to a profile manager.

subscription. In a Tivoli environment, the process of identifying the subscribers to which profiles are distributed.

subscription list. In a Tivoli environment, a list that identifies the subscribers to a profile manager. A profile manager can be included in a subscription list to subscribe several resources simultaneously rather than adding each resource individually.

T

TAP. See Tivoli Authentication Package.

task. In a Tivoli environment, the definition of an action that must be routinely performed on various targets throughout the network. A task defines the executable files to be run when the task is initiated, the authorization role required to execute the task, and the user or group name under which the task runs.

task library. In a Tivoli environment, a container in which a Tivoli administrator can create and store tasks and jobs.

Tivoli administrator. In a Tivoli environment, a system administrator that is identified by system account maps who is authorized to perform systems management tasks and manage policy regions in one or more networks.

Tivoli Application Development Environment (ADE). A toolkit that contains the complete application programming interface (API) for Tivoli Management Framework. This toolkit enables customers and Tivoli Partners to develop their own applications for a Tivoli environment.

Tivoli Application Extension Facility (AEF). A toolkit that enables customers to extend the capabilities of Tivoli applications. For example, they can add fields to a dialog, create custom attributes and methods for application resources, or create custom icons and bitmaps.

Tivoli Authentication Package. A dynamically linked library (DLL) installed by Tivoli Management Framework, that is capable of creating Windows security tokens for a different user context. These tokens can be used for accessing network resources or creating processes in a different user context.

Tivoli client. A client of a Tivoli server. See Tivoli management region client (managed node) and Tivoli server.

Tivoli desktop. In a Tivoli environment, the desktop that system administrators use to manage their network computing environments.

Tivoli Event Integration Facility (EIF). A toolkit that provides a simple application programming interface (API) to enable customers and Tivoli Partners to develop new event adapters that can forward events. A customer can also translate events from third-party or in-house applications.

Tivoli environment. The Tivoli applications, based upon Tivoli Management Framework, that are installed at a specific customer location and that address network computing management issues across many platforms.

Tivoli Management Framework. The base software required to run many Tivoli software applications. This software infrastructure enables the integration of systems management applications from Tivoli and the Tivoli Partners. Tivoli Management Framework includes the following components:

- Object request broker (oserv service)
- Distributed object database
- Basic administration functions
- Basic application services
- Basic desktop services, such as the graphical user interface (GUI)

Tivoli client (managed node). In a Tivoli environment, any computer system—except the Tivoli server—on which Tivoli Management Framework is installed. The object dispatcher (or oserv service) runs on each client, and each client maintains a local object database. See Tivoli server.

Tivoli name registry. In a Tivoli environment, the table that map names of managed resources to resource identifiers (and the corresponding information) with a Tivoli region.

Tivoli region. In a Tivoli environment, a Tivoli server and the set of clients it serves. An organization can have more than one region. A Tivoli region addresses the physical connectivity of resources whereas a policy region addresses the local organization of resources.

Tivoli Remote Execution Service. The service that enables a Tivoli environment to perform remote operations on machines. These operations include remotely installing clients, connecting Tivoli management regions, and starting the object request broker from a remote machine.

Tivoli server. In a Tivoli environment, the server for a specific Tivoli region that holds or references the complete set of Tivoli software, including the full object database.

transaction. A specific set of input data that triggers a specific process or job.

U

upcall. A method invocation from an endpoint to the gateway. Contrast with downcall.

user login map. A mapping that associates a single user login name with user accounts on various operating systems. User login maps enable Tivoli administrators to log in to the Tivoli environment and perform operations within the Tivoli environment with a single user login name, independent of system accounts used on the various operating systems.

V

validation policy. In a Tivoli environment, the policy that ensures that all resources in a policy region comply with the established policy for the policy region. A validation policy prevents Tivoli administrators from creating or modifying resources that do not conform to the policy of the policy region in which the resources were created. Contrast with default policy.

virtual user. A user ID (UID) mapping set up in Tivoli Management Framework. A single UID can be mapped to different actual users on different types of architectures. For example, the virtual user \$root_user can be mapped to root on UNIX operating systems and **Administrator** on Windows operating systems. See user login map.

Index

Special characters

\$root_group map 33
\$root_user map 32

A

accessibility ix
Administrator icon
 pop-up menu options 29
 removing with commands 50
 removing with Tivoli desktop 50
administrators
 access to resources 40
 adding region roles 37, 44
 adding resources to desktops
 using the Tivoli desktop 41
 with commands 41
 creating 35
 database object 50
 deleting 51
 description 29
 editing
 logins 47
 with commands 47
 group names 36, 43
 icon 5
 logins 30
 names 30
 remote Tivoli region resources 62
 removing region roles 37, 44
 removing resources from desktops
 with commands 41
 with Tivoli desktop 41
 restoring 51
 setting
 logins 37, 46
 notice group subscriptions 48
 notice groups 40, 48
 properties 42
 resource roles 38, 45
 Tivoli region roles 36, 43
 subscribing to notice groups 40, 48
 viewing
 as data objects 51
 names with commands 49
 procedure 49
 removed administrators 51
 using the Tivoli desktop 49
Administrators Collection icon 5
after_install_policy script 9
applications using multiplexed
 distribution 139
audit trail, system administrator
 activity 99
authorization roles
 administrators
 adding resources 41
 changing Tivoli region roles 43
 creating 35
 setting logins 46

authorization roles (*continued*)
 administrators (*continued*)
 setting notice group
 subscriptions 48
 setting properties 42
 setting resource roles 45
 viewing 49
clients
 adding IP interfaces 13
 editing IP interfaces 14
 moving clients 11
 removing IP interfaces 15
 toggling icons 27
expiring notices 107
jobs
 creating 120
 deleting 124, 137
 editing 124, 136
 enabling/disabling 135
 running 123
 saving output 123
 scheduling 129
 sorting 134
 viewing 132
notices
 combining 105
 displaying 106
 filtering 104
 forwarding 102
 marking as read 103
 reading 99
 saving 101
 sorting 103
opening an xterm session 26
policies
 assigning policy to resource
 types 73
 creating policy subregions 71
 creating top-level policy
 regions 70
 modifying managed resource types
 in policy regions 72
profile managers
 adding subscribers 81
 creating 80
 editing 83
 removing subscribers 81
profiles
 cloning 87
 copying 87
 creating 84
 distributing 85
 moving 88
 moving to another profile
 manager 89
 synchronizing with targets 86
queries
 creating 92, 93
 editing 96
 running 97

authorization roles (*continued*)
 task libraries
 creating 110
 listing contents 111
tasks
 creating 113
 deleting 119
 editing 118
 running 115
 saving output 118
Tivoli region connections
 determining status 61
 disconnecting 66
 remote 59
 secure 56
 updating resources 63

B

bold typeface, meaning of x
books
 See publications
BuiltinNTAdministrator accounts 32
bulletin board 99

C

ciphers, setting 55
clients
 endpoints 10
 moving to another policy region 11
 properties 12
collections
 creating 4
 description 4
 icons 6
 populating 4
commands
 ENDTMEEPT 25
 lcf (NetWare) 22
 lcf 15, 20, 21
 lcf.sh start 23
 lcf.sh stop 23
 lcfstop (NetWare) 22
 net start lcf 22
 net stop lcf 22
 odadmin 57
 STRTMEEPT 23
 wchkdb 66
 wchkpol 77
 wconnect 58, 61
 wcrtdadmin 40
 wcrtdjob 122
 wcrtdpr 71
 wcrtdprf 85
 wcrtdprfmgr 80
 wcrtdqlib 92
 wcrtdquery 96
 wcrtdtask 115
 wcrtdtlib 111

- commands (*continued*)
 - wdel 51, 84, 90
 - wdeljob 125
 - wdelsched 137
 - wdeltask 119
 - wdisconn 67
 - wdistrib 86
 - wdisttask 111
 - wenblsched 136
 - wep 21
 - wexpnotif 107
 - wgetadmin 41, 44, 46, 47, 49
 - wgetjob 124
 - wgetpr 73, 75
 - wgetquery 97
 - wgetsched 133
 - wgettask 119
 - whostid 13
 - widmap 31, 32
 - wifconfig 13, 14, 15
 - wln 51
 - wlookup 49
 - wls 49, 51, 101
 - wlsconn 62
 - wlsnotif 101, 102
 - wmannode 13
 - wmdist 152
 - wmdistgui 151
 - wmemsize 13
 - wmv 9, 11
 - wrm 50
 - wrpt 140
 - wrunjob 123
 - wrunquery 98
 - wruntask 118
 - wschedjob 132
 - wsetadmin 41, 44, 46, 47, 49
 - wsetjob 124
 - wsetpm 84
 - wsetpr 73, 75
 - wsetquery 97
 - wsetsched 136
 - wsettask 119
 - wsub 83
 - wuname 13
 - wunsub 83
 - wupdate 65, 66
 - wxterm 26

- communications, SSL 53
- configuration management, overview 79
- connections, Tivoli region
 - description 53
 - determining status 61
 - disconnecting 66
 - using the Tivoli desktop 66
 - wdisconn command 67
 - displaying status
 - using the Tivoli desktop 61
 - wlsconn command 62
 - one-way and two-way 57
 - remote
 - using the Tivoli desktop 59
 - wconnect command 61
 - resource exchange or update
 - description 63
 - scheduling 64
 - using the Tivoli desktop 65

- connections, Tivoli region (*continued*)
 - secure
 - wconnect command 58
- connections, Tivoli regions
 - encryption 57, 59
 - secure
 - using the Tivoli desktop 56
- console
 - Distribution Status 148
 - Mobile Computing 158
- copying profiles 87
- creating
 - administrators
 - with commands 40
- csh, initializing Tivoli environment
 - variables 1
- customer support
 - See* software support

D

- data objects
 - administrators 50
 - deleting 51
- data transfer, setting ciphers 55
- default policies 11, 73, 125
- desktop
 - description 1
 - Navigator 3
- Desktop Navigator 3
- destination profile manager 87
- Distribution Status console 148
- Distribution Topology 156
- Node Table 155
- starting 149
- Status Chart 153
- Time Spent Chart 154
- distributions
 - management of 139
 - scheduling for profiles 86
 - viewing details of 153
 - viewing status 152
- domain controllers 34

E

- editing
 - profile managers 83
 - tasks 118
- electronic mail, forwarding notices 102
- emulators 26
- encryption, connected Tivoli regions 57, 59
- Endpoint Manager icon 6
- endpoints
 - assigned gateway 18, 19
 - configuration settings 19
 - description 9, 10
 - icons 6
 - interpreter type 18
 - last restart 19
 - log file 19
 - method cache 19
 - network address configuration 19
 - operating system 18

- endpoints (*continued*)
 - properties
 - description 15
 - modifying from command line 21
 - viewing from endpoint manager 16
 - viewing from Web browser 17
 - statistics 19
 - status 18
 - trace log 19
 - version number 18
- ENDTMEEPT command 25
- environment variables
 - See* variables
- error messages, tap_call_init failed 34
- exchange of resource information 63
- expiration of notices 107
- expression characters, regular 4

F

- filter 4

G

- gateways
 - viewing properties from a Web browser 21
- gateway names 36, 43

I

- icons
 - changing 27
 - examples and descriptions
 - Administrators 5
 - Administrators Collection 5
 - Collection 6
 - Distribution Status 149
 - Endpoint 6
 - Endpoint Manager 6
 - Job 6
 - Managed Node 6
 - Notification Bulletin Board 6
 - Policy Region 6
 - Profile Manager (Database) 6
 - Profile Manager (Dataless) 6
 - Query 7
 - Query Library 7
 - Scheduler 7
 - Task 7
 - Task Library 7
 - Tivoli 5
 - Unknown 7
 - labels, changing 5
 - togglng 27
- instances of resource types 66
- interpreter type viii
- IP interfaces
 - adding 13
 - editing 13, 14
 - removing 15
- italic typeface, meaning of x

J

- Job icon 6
- jobs
 - creating
 - using the Tivoli desktop 120
 - using wcrjob command 122
 - deleting
 - using the Tivoli desktop 125
 - using wdeljob command 125
 - editing
 - using the Tivoli desktop 124
 - using wgetjob command 124
 - using wsetjob command 124
 - execution mode 121
 - in multiple Tivoli regions 137
 - overview 120
 - running
 - using drag and drop 123
 - using the Tivoli desktop 123
 - using wrunjob command 123
 - saving output 123
 - scheduling
 - across regions 137
 - description 129
 - using drag and drop 129
 - using the Tivoli desktop 130
 - with commands 132
 - setting timeout value 122
 - specifying display of job
 - attributes 133
 - start times across Tivoli regions 138
- jobs, scheduled
 - deleting
 - using the Tivoli desktop 137
 - with commands 137
 - editing
 - using the Tivoli desktop 136
 - with commands 136
 - enabling/disabling
 - using the Tivoli desktop 136
 - with commands 136
 - finding 135
 - sorting 134
 - viewing
 - using the Tivoli desktop 132
 - with commands 133

L

- labels, icons 5
- lcf command (NetWare) 22
- lcf command 15, 20, 21
- lcf.cfg file 19
- lcf.log file 19
- lcf.sh script 21
- lcf.sh start 23
- lcf.sh stop 23
- lcfstop command (NetWare) 22
- legal notices 167
- links 156
- logical operators, in queries 95
- login names
 - adding 38
 - administrator and user 30
 - editing 47
 - managing 31

- login names (*continued*)
 - removing 38, 47
 - setting 37, 46
- loopback interfaces 13

M

- making
 - remote Tivoli region connections 59
 - secure Tivoli region connections 56
- managed nodes
 - changing icons 27
 - description 9
 - icons 6
 - IP interfaces
 - adding 13
 - editing 14
 - removing 15
 - mapping Windows accounts 32
 - moving to another policy region
 - description 11
 - using drag and drop 11
 - wmv command 11
 - properties 12
 - setting environment variables 1
 - viewing properties 12
 - Xterminal sessions 26
- managed resources
 - See* resources
- manuals
 - See* publications
- MDist
 - before using this service 139
 - configuring repeaters 141
- MDist 2
 - before using this service 139
 - configuring repeaters 143
 - Distribution Status console 149
 - setting depot directory 145
 - setting permanent storage 145
 - viewing distribution details 153
- Mobile Computing console 158
 - configuring 160
 - starting 165
- monospace font, meaning of x
- multiple logins 31

N

- name registry
 - time stamps 66
 - updating "All" resources 66
- naming conventions
 - special characters 36, 42, 80, 83, 84, 88, 94, 121
- Navigator 3
- net start lcf command 22
- net stop lcf command 22
- network security level, setting SSL 54
- nodes 156
- notice groups
 - editing subscriptions 48
 - modifying subscriptions
 - with commands 49
 - setting for administrators 40, 48
 - subscribing 40, 48

- notice groups (*continued*)
 - unsubscribing 40, 48
- notices 167
 - attributes 99
 - combining 105
 - description 99
 - displaying previously read 106
 - displaying unread 99
 - expiring 107
 - filtering 104
 - forwarding with electronic mail 102
 - marking
 - as all read 103
 - as read 103
 - as unread 103
 - reading
 - description 99
 - using the Tivoli desktop 99
 - wlsnotif and wls commands 101
 - receiving 99
 - removing, automatically 107
 - saving
 - using the Tivoli desktop 101
 - wlsnotif command 102
 - sorting 103
 - viewing 99
- Notification Bulletin Board icon 6

O

- odadmin command 57
- one-way Tivoli region connections 57
- online publications
 - accessing viii
- ordering publications ix
- output
 - saving for jobs 123
 - saving for tasks 118

P

- pattern matching 4
- performance, exchanging resources 63
- policies
 - after_install_policy 9
 - assigning 73
 - checking 75
 - description 69
 - scheduling checking 76
 - task library 125
 - validation 74
- policy methods
 - default
 - moving clients 11
 - tl_def_dist_mode 125
 - tl_def_man_nodes 125
 - tl_def_prof_mgrs 125
 - tl_def_set_gid 125
 - tl_def_set_uid 125
 - validation
 - moving clients 11
 - tl_val_man_nodes 126
 - tl_val_prof_mgrs 126
 - tl_val_set_gid 126
 - tl_val_set_uid 126

- policy regions
 - changing name 72
 - checking policy
 - description 75
 - using the Tivoli desktop 75
 - wchkepol command 77
- creating
 - subregions 70, 71
 - top-level 70
 - using the Tivoli desktop 70
 - wcrtpr 71
- description 69
- icons 6, 69
- menu options 69
- subregions 71
- top-level 70
- viewing managed resources 69
- primary IP interfaces 13
- profile managers
 - adding subscribers
 - wsub command 83
 - creating 79
 - wcrtprfmgr command 80
 - deleting 84
 - using the Tivoli desktop 84
 - wdel command 84
 - editing
 - using the Tivoli desktop 83
 - wsetpm command 84
 - icons
 - Database 6
 - Dataless 6
 - modifying subscribers 81
 - removing subscribers
 - wunsub command 83
 - subscribing using drag and drop 81
- profiles
 - cloning from profile manager 87
 - copying from profile manager 87
 - creating
 - from profile managers 85
 - using the Tivoli desktop 84
 - deleting
 - from profile manager 89
 - using the Tivoli desktop 89
 - wdel command 90
 - description 79
 - differences 86
 - distributing 85
 - using drag and drop 85
 - using the Tivoli desktop 85
 - wdistrib command 86
 - hierarchies 89
 - moving from profile manager 88
 - synchronizing
 - with a target 86
- properties
 - administrators 42
 - clients 12
 - endpoints 15
 - endpoints, from Tivoli desktop 16
 - managed nodes 12
 - modifying
 - endpoints, from command line 21
 - viewing 16
 - endpoints, from Web Browser 17
 - gateways, from Web Browser 21

- properties (*continued*)
 - viewing (*continued*)
 - managed node 12
- publications
 - accessing online viii
 - ordering ix

Q

- queries
 - creating
 - description 93
 - using commands 96
 - using the Tivoli desktop 93
 - editing
 - description 96
 - using commands 97
 - using the Tivoli desktop 96
 - icons 7
 - logical operators 95
 - organizing in query libraries 92
 - RIM 91
 - running
 - description 97
 - from the Tivoli desktop 97
 - using commands 98
 - saving results 97
 - searching RIM repositories 91
 - viewing results 97
 - views 91
 - where clauses 93, 94
 - wildcard characters 96
- query facility 91
- query libraries
 - creating 92
 - creating using the Tivoli desktop 92
 - creating with commands 92
 - description 92
 - icons 7
 - organizing queries 92

R

- reading notices 99
- receipt of notices 99
- regular expressions 4
- removal of
 - Administrator icon
 - using commands 50
 - using the Tivoli desktop 50
 - resources 41
- removal of notices 107
- repeaters
 - configuring 141
 - creating 140
- reports, system administration
 - activity 99
- resource roles
 - adding 39, 45
 - editing
 - using the Tivoli desktop 45
 - with commands 46
 - removing 39, 46
 - setting 38
 - setting for administrators 45

- resource types
 - assigning policy 73
 - modifying in policy regions 72
 - time stamps 66
- resources
 - adding 41
 - adding to desktop 40
 - collections 4
 - exchanging 53, 63
 - locating 3
 - modifying in policy regions 9, 72
 - removing 41
 - updating 63
- restoration, removed administrator 51
- RIM
 - description 91
 - searching repositories 91, 93
- root_group login map 33
- root_user login map 32

S

- scheduled jobs 129
 - deleting
 - using the Tivoli desktop 137
 - with commands 137
 - editing
 - using the Tivoli desktop 136
 - with commands 136
 - enabling/disabling
 - using the Tivoli desktop 136
 - with commands 136
 - finding 135
 - sorting 134
 - viewing
 - using the Tivoli desktop 132
 - with commands 133
- scheduler
 - across regions 137
 - description 129
 - icon 7
 - scheduling jobs
 - description 129
 - using drag and drop 129
 - using the Tivoli desktop 130
 - with commands 132
- scripts
 - setup_env.cmd 2
 - setup_env.csh 1
 - setup_env.sh 1
- search strings, regular expressions 4
- Secure Socket Layer
 - See SSL
- secure Tivoli region connections
 - making 56
 - using the Tivoli desktop 57
 - wconnect command 58
- setup_env.cmd script 2
- setup_env.csh script 1
- setup_env.sh script 1
- sh, initializing Tivoli environment
 - variables 1
- shell service 60
- software support
 - contacting ix
- source profile manager 87

- special characters, names of Tivoli
 - resources 36, 42, 80, 83, 84, 88, 94, 121
- SSL
 - enabling communications 53
 - network security layer 54
- status
 - Tivoli region connections 61
- STRTIMEPT command 23
- subregions, creating 71
- subscribers
 - modifying 80
 - validation policies 80
- subscription
 - notice groups 40, 48
 - validation policies 81
- system
 - management operations,
 - administrators 29
- system administrator activity log 99

T

- tap_call_init failed error message 34
- task libraries
 - creating 110
 - using the Tivoli desktop 110
 - using wcrttlib command 111
 - icons 7
 - listing contents 111
 - overview 109
 - policy 125
 - working with icons 110
- Task Library Language (TLL) 113
- tasks
 - creating
 - using the Tivoli desktop 113
 - using wcrttask command 115
 - deleting 119
 - using the Tivoli desktop 119
 - using wdeltask command 119
 - distributing executables 111
 - editing
 - using the Tivoli desktop 119
 - using wgettask command 119
 - using wsettask command 119
 - execution mode 116
 - icons 7
 - overview 112
 - running
 - using drag and drop 116
 - using the Tivoli desktop 116
 - using wruntask command 118
 - saving output 118
 - timeout setting 117
- terminal emulators 26
- Time Spent Chart 154
- time stamp in name registry 66
- Tivoli administrators
 - mapping Windows accounts 32
- Tivoli Desktop for Windows 9
- Tivoli environment variables
 - initializing for managed node 1
 - initializing for Tivoli server 1
- Tivoli regions
 - adding resources 41
 - connections
 - determining status 61

- Tivoli regions (*continued*)
 - connections (*continued*)
 - encryption 57, 59
 - one-way and two-way 57
 - remote 59, 61
 - secure 56, 58
 - updating resources 63
 - creating administrators 35
 - description 53
 - disconnecting
 - description 66
 - using the Tivoli desktop 66
 - wdisconn command 67
 - displaying status 61
 - wlsconn command 62
 - icons 5
 - jobs
 - run across boundaries 137
 - start times 138
 - mapping roles 43
 - number 57
 - remote region number 57
 - resource exchange or update
 - description 63
 - using the Tivoli desktop 64, 65
 - setting roles 36, 43
 - updating "All" resources 66
 - viewing administrators 49
- Tivoli server
 - setting environment variables 1
- Tivoli software information center viii
- Tivoli_Admin_Privileges group
 - account 34
 - tl_def_dist_mode default policy 125
 - tl_def_man_nodes default policy 125
 - tl_def_prof_mgrs default policy 125
 - tl_def_set_gid default policy 125
 - tl_def_set_uid default policy 125
 - tl_val_man_nodes validation policy 126
 - tl_val_prof_mgrs validation policy 126
 - tl_val_set_gid validation policy 126
 - tl_val_set_uid validation policy 126
 - tmersrvd user account 33
- top-level policy regions 70
- topology
 - distribution 156
- trusted host facility 59
- two-way Tivoli region connections 57
- typeface conventions x

U

- UNIX
 - group names 36, 43
 - opening an Xterminal session 26
- Unknown icon 7
- user accounts
 - BuiltinNTAdministrator 32
 - mapping, Windows operating
 - systems 32
 - tmersrvd 33
- user login maps 31
 - root_group 33
 - root_user 32
- Windows accounts 32
- user login names
 - adding 38

- user login names (*continued*)
 - description 30
 - mapping 36, 42
 - removing 38, 47
 - setting
 - description 46
 - using the Tivoli desktop 47
 - with commands 47

V

- validation policies 126
 - for managed resource types 74
 - subscription 80
 - task library 125
 - when moving clients 11
- variables
 - initializing
 - managed nodes 1
 - Tivoli server 1
- variables, notation for x
- views, within RIM 91

W

- wchkdb command 66
- wchkpol command 77
- wconnect command 58, 61
- wcrtdadmin command 40
- wcrtjob command 122
- wcrtpr command 71
- wcrtprf command 85
- wcrtprfmgr command 80
- wcrtqlib command 92
- wcrtquery command 96
- wcrttask command 115
- wcrttlib command 111
- wdel command 51, 84, 90
- wdeljob command 125
- wdelsched command 137
- wdeltask command 119
- wdisconn command 67
- wdistrib command 86
- wdisttask command 111
- Web browser, viewing endpoint
 - properties 17
- Web browser, viewing gateway
 - properties 21
- wenblsched command 136
- wep command 21
- wexpnotif command 107
- wgetadmin command 41, 44, 46, 47, 49
- wgetjob command 124
- wgetpr command 73, 75
- wgetquery command 97
- wgetsched command 133
- wgettask command 119
- where clauses, in queries 93, 94
- whostid command 13
- widmap command 31, 32
- wifconfig command 13, 14, 15
- wildcard characters, in queries 96
- windows
 - Add Scheduled Job 130
 - administrators
 - Create Administrator 35

- windows (*continued*)
 - administrators (*continued*)
 - Set Login Names 47
 - Set Notice Groups 40, 48
 - Set TMR Roles 44
 - Administrators 49
 - clients
 - Add IP Interface 13
 - Client/Server Icon Toggle 27
 - Endpoint List 16
 - Endpoint Properties 16
 - Gateway List 16
 - Managed Node 12
 - Create Collection 4
 - Desktop Navigator 3
 - jobs
 - Create Job 121
 - Save Job Output 123
 - notices
 - Filter Notices 104
 - Forward Notice 102
 - Read Notices 100
 - Sort Notices 103
 - policies
 - Check Policy 75
 - Create Policy Region 70
 - Policy Region Properties 72
 - Set Managed Resources 73
 - Set Managed Resources Policies 74
 - profiles
 - Clone Profile 88
 - Create Profile Manager 80
 - Delete Profiles 89
 - Edit Profile Manager 83
 - queries
 - Create Query Library 92
 - Execute a Query 97
 - Task Library 113
 - tasks
 - Create Task 114
 - Create Task Library 110
 - Destination of Task Output 117
 - Execute Task 116
 - Save Task Output 118
 - Tivoli region connections
 - Connect to a Remote TMR 59
 - Securely Connect to a Remote TMR 57
 - TMR Connection Status 61
 - Update Resources from Multiple Tivoli regions 64
- wln command 51
- wlookup command 49
- wls command 49, 51, 101
- wlsconn command 62
- wlsnotif command 101, 102
- wmannode command 13
- wmdist command 152
- wmdistgui command 151
- wmemsize command 13
- wmv command 9, 11
- wrm command 50
- wrpt command 140
- wrunjob command 123
- wrunquery command 98
- wruntask command 118
- wschedjob command 132
- wsetadmin command 41, 44, 46, 47, 49
- wsetjob command 124
- wsetpm command 84
- wsetpr command 73, 75
- wsetquery command 97
- wsetsched command 136
- wsettask command 119
- wsub command 83
- wuname command 13
- wunsub command 83
- wupdate command 65, 66
- wxterm command 26

X

- Xterminal sessions, opening 26



Printed in USA

GC32-0805-02

