Tivoli Management Framework User’s Guide

Copyright Notice
© Copyright IBM Corporation 1998, 2001. All rights reserved. May only be used pursuant to a Tivoli Systems Software License Agreement, an IBM Software License Agreement, or Addendum for Tivoli Products to IBM Customer or License Agreement. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual, or otherwise, without prior written permission of IBM Corporation. IBM Corporation grants you limited permission to make hardcopy or other reproductions of any machine-readable documentation for your own use, provided that each such reproduction shall carry the IBM Corporation copyright notice. No other rights under copyright are granted without prior written permission of IBM Corporation. The document is not intended for production and is furnished "as is" without warranty of any kind. All warranties on this document are hereby disclaimed, including the warranties of merchantability and fitness for a particular purpose.

U.S. Government Users Restricted Rights—Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corporation.

Trademarks
IBM, Tivoli, the Tivoli logo, AIX, AS/400, DB2, OS/2, RS/6000, Tivoli Enterprise, Tivoli Enterprise Console, and TME are trademarks or registered trademarks of International Business Machines Corporation or Tivoli Systems Inc. in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Intel is a registered trademark of Intel Corporation.

Java and all Java-based trademarks are 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.

Notices
References in this publication to Tivoli Systems or IBM products, programs, or services do not imply that they will be available in all countries in which Tivoli Systems or IBM operates. Any reference to these products, programs, or services is not intended to imply that only Tivoli Systems or IBM products, programs, or services can be used. Subject to valid intellectual property or other legally protectable right of Tivoli Systems or IBM, any functionally equivalent product, program, or service can be used instead of the referenced product, program, or service. The evaluation and verification of operation in conjunction with other products, except those expressly designated by Tivoli Systems or IBM, are the responsibility of the user. Tivoli Systems or IBM may have patents or pending patent applications covering subject matter 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 the IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, New York 10504-1785, U.S.A.
Contents

Preface ......................................................................................................................... xiii

Chapter 1—The Desktop

Establishing the Tivoli Environment ........................................................................ 1-1
Windows and Dialogs .............................................................................................. 1-2
  Window and Dialog Elements ............................................................................... 1-4
  File Browser Dialog ............................................................................................ 1-17
Tivoli Desktop Menus .............................................................................................. 1-19
  Desktop Menu ...................................................................................................... 1-19
  Edit Menu ........................................................................................................... 1-20
  View Menu ......................................................................................................... 1-21
  Create Menu ...................................................................................................... 1-21
Desktop Navigator .................................................................................................. 1-21
Collections ............................................................................................................ 1-23
Tivoli Icons ............................................................................................................. 1-24

Chapter 2—Tivoli Clients

Icons ......................................................................................................................... 2-2
  Managed Nodes .................................................................................................. 2-3
  Endpoints ........................................................................................................... 2-4
Moving a Client ........................................................................................................ 2-4
  Desktop, Drag and Drop .................................................................................... 2-5
  Command Line .................................................................................................. 2-5
Client Properties ..................................................................................................... 2-6
  Managed Nodes .................................................................................................. 2-6
  Endpoint Properties ......................................................................................... 2-15
Toggling a Managed Node Icon ............................................................................ 2-29

Chapter 3—Tivoli Administrators

Administrators Collection Icon ............................................................................. 3-1
Administrator Logins .................................................................................................. 3-2
Managing Multiple Logins ......................................................................................... 3-3
Viewing Tivoli Administrators ................................................................................... 3-4
  Desktop .................................................................................................................... 3-5
  Command Line ......................................................................................................... 3-6
Creating a Tivoli Administrator .................................................................................. 3-7
  Desktop .................................................................................................................... 3-7
  Command Line ......................................................................................................... 3-15
Adding Resources to an Administrator’s Desktop ..................................................... 3-15
  Desktop .................................................................................................................... 3-16
  Command Line ......................................................................................................... 3-17
Setting Administrator Properties .............................................................................. 3-17
Setting Tivoli Management Region Roles ................................................................. 3-19
  Desktop .................................................................................................................... 3-20
  Command Line ......................................................................................................... 3-21
Setting Resource Roles ............................................................................................. 3-21
  Desktop .................................................................................................................... 3-22
  Command Line ......................................................................................................... 3-24
Setting Logins ............................................................................................................. 3-24
  Desktop .................................................................................................................... 3-25
  Command Line ......................................................................................................... 3-27
Removing an Administrator Icon from the Desktop ................................................. 3-27
  Viewing Removed Administrators ............................................................................ 3-28
  Restoring a Removed Administrator ....................................................................... 3-28
Deleting an Administrator .......................................................................................... 3-28
Setting Notice Group Subscriptions ......................................................................... 3-29
  Desktop .................................................................................................................... 3-29
  Command Line ......................................................................................................... 3-31
Chapter 4—Tivoli Management Regions and Interregion Connection

Making a Secure Tivoli Management Region Connection ......................... 4-2
  Desktop .................................................................................................................. 4-2
  Command Line ..................................................................................................... 4-5
Making a Remote Tivoli Management Region Connection ......................... 4-5
  Desktop .................................................................................................................. 4-6
  Command Line ..................................................................................................... 4-10
Determining the Status of Tivoli Management Region Connections .......... 4-10
  Desktop .................................................................................................................. 4-10
  Command Line ..................................................................................................... 4-11
Tivoli Administrators and Remote Tivoli Management Region Resources .... 4-11
  Desktop .................................................................................................................. 4-12
Exchanging or Updating Resource Information ........................................ 4-13
  Desktop, Update Resources from Multiple TMRs Dialog ....................... 4-14
  Desktop, TMR Connection Status Dialog ...................................................... 4-16
  Forcing an Update to Override Time Stamps ............................................... 4-17
  Updating All Resources .................................................................................... 4-18
  Command Line ..................................................................................................... 4-18
Disconnecting Tivoli Management Regions ............................................... 4-18
  Desktop .................................................................................................................. 4-19
  Command Line ..................................................................................................... 4-20

Chapter 5—Policy and Policy Regions

Tivoli Policy Region Icon .................................................................................. 5-1
Default Policy ........................................................................................................ 5-3
Validation Policy .................................................................................................. 5-3
Creating a Top-level Policy Region ................................................................. 5-3
  Desktop .................................................................................................................. 5-4
  Command Line ..................................................................................................... 5-5
Creating a Policy Subregion ............................................................................ 5-5
### Chapter 7—Query Facility

Creating a Query Library .................................................................................... 7-2  
  Desktop ...................................................................................................... 7-2  
  Command Line ....................................................................................... 7-4  
Creating a Query ................................................................................................. 7-4  
  Desktop ...................................................................................................... 7-5  
  Command Line ......................................................................................... 7-10  
Editing a Query ................................................................................................. 7-11  
  Desktop ...................................................................................................... 7-12  
  Command Line ......................................................................................... 7-13  
Using Queries ................................................................................................... 7-14  
  Running a Query ...................................................................................... 7-15  
  Defining Subscribers and Targets ............................................................ 7-18

### Chapter 8—Notification

Reading Notices .................................................................................................. 8-2  
  Desktop ...................................................................................................... 8-2  
  Command Line ......................................................................................... 8-5  
Saving Notices .................................................................................................... 8-5  
  Desktop ...................................................................................................... 8-5  
  Command Line ......................................................................................... 8-7  
Forwarding Notices ............................................................................................. 8-8  
  Desktop ...................................................................................................... 8-8  
  Command Line ......................................................................................... 8-10  
Marking Notices as Read and Unread .............................................................. 8-11  
Sorting Notices ............................................................................................... 8-13  
Filtering Notices ........................................................................................... 8-16  
Combining Notices ........................................................................................... 8-19  
Displaying Old Notices ..................................................................................... 8-21  
Notice Expiration .............................................................................................. 8-23
Chapter 9—Task Library

Tasks ................................................................................................................... 9-2
Jobs ..................................................................................................................... 9-3
Task Information................................................................................................. 9-3
Execution Information ........................................................................................ 9-5
Distribution of Task Executable Files................................................................. 9-7
Task Library Policy............................................................................................. 9-8
  Default Policies ............................................................................................... 9-8
  Validation Policies .......................................................................................... 9-9
Creating a Task Library .................................................................................... 9-10
  Desktop......................................................................................................... 9-10
  Command Line............................................................................................... 9-11
Creating a Task .................................................................................................. 9-11
  Desktop......................................................................................................... 9-12
  Command Line............................................................................................... 9-14
Running a Task .................................................................................................. 9-14
  Desktop, Drag and Drop............................................................................... 9-15
  Desktop......................................................................................................... 9-16
  Command Line............................................................................................... 9-18
Saving Task Output to a File ............................................................................ 9-18
Editing a Task .................................................................................................... 9-19
  Desktop......................................................................................................... 9-20
  Command Line............................................................................................... 9-22
Creating a Job .................................................................................................... 9-22
  Desktop......................................................................................................... 9-22
  Command Line............................................................................................... 9-25
Running a Job .................................................................................................... 9-25
  Desktop, Drag and Drop............................................................................... 9-25
  Desktop......................................................................................................... 9-26
  Command Line............................................................................................... 9-26
Saving Job Output to a File............................................................................... 9-26
Chapter 10—Tivoli Scheduler

Job Scheduling ........................................................................................................ 10-1
  Jobs Scheduled to Run Once ................................................................. 10-1
  Jobs Scheduled to Run Frequently ...................................................... 10-3
  Jobs Scheduled for the Past ................................................................. 10-6
Job Restrictions ............................................................................................... 10-7
  Jobs Starting within a Given Time ...................................................... 10-9
Retry on Failed Jobs ..................................................................................... 10-11
Job Disabling .................................................................................................. 10-13
  Jobs Set for a Specified Time .............................................................. 10-13
  Jobs Set to Repeat .................................................................................. 10-13
Notification ..................................................................................................... 10-14
Scheduler across Tivoli Management Regions ........................................ 10-14
  Jobs Run in Multiple Tivoli Management Regions .......................... 10-15
  Start Times in Tivoli Management Regions ..................................... 10-15
Scheduling a Job ............................................................................................. 10-16
  Desktop, Drag and Drop ................................................................. 10-16
  Desktop ............................................................................................... 10-16
  Command Line ..................................................................................... 10-19
Changing or Viewing Scheduled Jobs ...................................................... 10-19
  Desktop ............................................................................................... 10-20
  Command Line ..................................................................................... 10-23
Controlling Display of Job Attributes ..................................................... 10-24
Sorting Jobs .................................................................................................. 10-25
Finding Jobs .................................................................................................... 10-27

Chapter 11—Application Management

Description of Application Management......................................................... 11-2
  Application Management Data................................................................. 11-3
  Application Description Files ................................................................. 11-4
Tools for Developing Management Data ....................................................... 11-4
How Tivoli Tools Use Management Data ...................................................... 11-5
How Tivoli Tools Receive Data .................................................................... 11-6
  Superseded AMS Commands ................................................................. 11-6
  New Icons on the Tivoli Desktop ............................................................. 11-7
  Data Objects ............................................................................................ 11-8
  New Notification Groups ....................................................................... 11-9
Using the winstruct Command .................................................................... 11-9
  winstruct Command Set ....................................................................... 11-9
  Uses for winstruct ................................................................................ 11-14
Additional Steps after Using winstruct ......................................................... 11-17
  Stopping and Starting the Tivoli Enterprise Console Server .................. 11-17
  Subscribing Endpoints ......................................................................... 11-18
  Iterative Instruction ............................................................................... 11-18
Using an Example AMP ................................................................................ 11-19
  Invoking winstruct .............................................................................. 11-19
  Subscribing Notice Groups .................................................................. 11-21
  Distributing the Application ................................................................ 11-21
  Monitoring the Application .................................................................. 11-24
Troubleshooting a winstruct Session ........................................................... 11-25
  Specifying Source Locations ................................................................. 11-26
  Specifying Versions for Operating Systems .......................................... 11-26
  Naming Monitors and Tasks ................................................................ 11-27

Chapter 12—Distribution Management

Before Using Multiplexed Distribution ......................................................... 12-1
Creating a Repeater .......................................................... 12-2
Configuring a Repeater .......................................................... 12-5
    MDist Service ................................................................. 12-5
    MDist 2 Service ............................................................. 12-9
Troubleshooting ............................................................... 12-15
    MDist 2 Consoles ......................................................... 12-16
        Tivoli Distribution Status Console ....................... 12-17
        Tivoli Mobile Computing Console ..................... 12-30

Glossary

Index
Preface

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

Tivoli Management Framework provides a set of common services or features that are used by the Tivoli applications 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 applications 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 tasks 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 tasks. Users of this guide should have some 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 management region using the available installation mechanisms provided by Tivoli Software Installation Service and Tivoli Management Framework. Tivoli Enterprise software includes the Tivoli management region server (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 Tivoli-provided policy scripts.

■ **Tivoli Management Framework Maintenance and Troubleshooting Guide**
  Explains how to maintain the 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 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, “The Desktop”
  Explains the graphical user interface (GUI), including the window controls and icons when using Tivoli Management Framework
Preface

■ Chapter 2, “Tivoli Clients”
Discusses Tivoli clients and how to view their properties

■ Chapter 3, “Tivoli Administrators”
Discusses Tivoli administrators and delegation of Tivoli authority

■ Chapter 4, “Tivoli Management Regions and Interregion Connection”
Discusses Tivoli management regions, the connection of Tivoli management regions, and exchanging information between connected regions

■ Chapter 5, “Policy and Policy Regions”
Discusses policy, policy resources, and policy regions

■ Chapter 6, “Configuration Management”
Discusses Tivoli profiles, profile managers, and profile manager operations

■ Chapter 7, “Query Facility”
Discusses query libraries and queries

■ Chapter 8, “Notification”
Discusses Tivoli notices and notice groups

■ Chapter 9, “Task Library”
Discusses jobs and tasks

■ Chapter 10, “Tivoli Scheduler”
Discusses scheduling jobs

■ Chapter 11, “Application Management”
Discusses how to use the winstruct command to set up the Tivoli environment to distribute, install, and maintain applications

■ Chapter 12, “Distribution Management”
Discusses how to create and configure repeaters. It also explains how to use the consoles, available only to Tivoli applications using the MDist 2 service.
Conventions Used in This Manual

The manual uses several typeface conventions for special terms and actions. These conventions have the following meaning:

**Bold**

Commands, keywords, file names, authorization roles, URLs, or other information that you must use literally appear in **bold**. Names of buttons and other controls also appear in **bold**.

**Italics**

Variables and values that you must provide appear in **italics**. New terms appear in **italics** when they are defined in the text. Words and phrases that are emphasized also appear in **italics**.

**Monospace**

Code examples, output, and system messages appear in a **monospace** font.

Accessing Publications Online

The Tivoli Customer Support Web site (**http://www.tivoli.com/support/**) offers a guide to support services (the **Customer Support Handbook**); frequently asked questions (FAQs); and technical information, including release notes, user’s guides, redbooks, and white papers. You can access Tivoli publications online at **http://www.tivoli.com/support/documents/**. The documentation for some products is available in PDF and HTML formats. Translated documents are also available for some products.

To access most of the documentation, you need an ID and a password. To obtain an ID for use on the support Web site, go to **http://www.tivoli.com/support/ getting/**.

Resellers should refer to **http://www.tivoli.com/support/smb/index.html** for more information about obtaining Tivoli technical documentation and support.

Business Partners should refer to “Ordering Publications” for more information about obtaining Tivoli technical documentation.
Ordering Publications

Order Tivoli publications online at http://www.tivoli.com/support/Prodman/html/pub_order.html or by calling one of the following telephone numbers:

- U.S. customers: (800) 879-2755
- Canadian customers: (800) 426-4968

Providing Feedback about Publications

We are very interested in hearing about your experience with Tivoli products and documentation, and we welcome your suggestions for improvements. If you have comments or suggestions about our products and documentation, contact us in one of the following ways:

- Send e-mail to pubs@tivoli.com.
- Fill out our customer feedback survey at http://www.tivoli.com/support/survey/.

Contacting Customer Support

The Tivoli Customer Support Handbook at http://www.tivoli.com/support/handbook/ provides information about all aspects of Tivoli Customer Support, including the following:

- Registration and eligibility
- How to contact support, depending on the severity of your problem
- Telephone numbers and e-mail addresses, depending on the country you are in
- What information you should gather before contacting support
The Tivoli desktop is a user interface that provides point-and-click access to Tivoli Management Framework features and components. The desktop provides a central control point for you to organize, manage, and delegate system management tasks.

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, see the Tivoli Management Framework Reference Manual.

Establishing the Tivoli Environment

Before you can access the desktop and CLI for Tivoli Management Framework, you must set up the Tivoli environment. Tivoli Management Framework includes the setup_env.sh and setup_env.csh files, which enable you to establish the correct search paths and environment variables. These setup files are available on any server or client in the Tivoli management region.

To set up the Tivoli environment, follow these steps:

1. Log in to a Tivoli client or the Tivoli management region server (Tivoli server) on which your Tivoli administrator has an alias with the super role for the Tivoli management region. See Chapter 3, “Tivoli Administrators” for more information about creating...
Tivoli administrators with authorization roles for the Tivoli management region.

2. Do one of the following:
   
   On UNIX systems only, do one of the following:
   
   ■ If you are using the Bourne shell, enter the following script:
     
     . /etc/Tivoli/setup_env.sh
   
   ■ If you are using the C shell, enter the following script:
     
     source /etc/Tivoli/setup_env.csh
   
   On Windows NT or Windows 2000 systems only, do one of the following:
   
   ■ From a bash shell, enter the following command:
     
     %SystemRoot%/system32/drivers/etc/Tivoli/setup_env.sh
   
   ■ From a command prompt, enter the following command:
     
     %SystemRoot%/system32/drivers/etc/Tivoli/setup_env.sh
   
   ■ To configure the Windows command line to automatically source the Tivoli environment, follow these steps:
     
     a. Right-click the Command Prompt (MS-DOS) shortcut to the Tivoli desktop.
     
     b. Click Properties.
     
     c. Click the Shortcut tab.
     
     d. In the Target text box, enter the following commands:
     
     %SystemRoot%/system32/cmd.exe /k c:\%SystemRoot%/system32\drivers\etc\Tivoli\setup_env.cmd
   
   You now have an environment ready to perform Tivoli maintenance operations.

Windows and Dialogs

Windows and dialogs provide controls for modifying resource information and properties.

A window, such as the Tivoli desktop, graphically displays icons and their associated labels. A menu bar is displayed at the top of windows.
You can use a window to move and copy resources. The following screen image of a Tivoli administrator’s desktop is an example of a window:

Dialogs open as a result of an action performed in a window—for example, clicking an icon or selecting an option from a menu in the menu bar. Unlike windows, dialogs are text-oriented, have no menu bar, and usually contain one or more text boxes and command buttons. You can use dialogs to manipulate resource properties. Following is an example of a dialog:
Window and Dialog Elements

Windows and dialogs consist of several elements. Each element is associated with a particular function. Window and dialog elements include the following:

- Menus
- Pull-down Menus
- Mnemonics
- Submenus
- Pop-up Menus
- Tear-off Menus (UNIX Only)
- Buttons
- Text Boxes
- Check Boxes
- Radio Buttons
- Option Menus
- Scrolling Lists
- Regular Expressions
- Browser Dialog
- Status Lines
- Status Messages

Menus

You can access two types of menus from the desktop:

- Pull-down menus, which may also contain submenus
- Pop-up menus

You can access resources and perform a variety of tasks from menus and their associated submenus.

Some menu items display additional windows or dialogs. If a menu item displays an ellipsis (…), selecting the item displays another window or dialog.
Pull-down Menus

Pull-down menus are displayed from the menu bar at the top of windows. Use pull-down menus to access menu items. To open a pull-down menu, press and hold the left mouse button over the menu name at the top of a window. To select an item from a pull-down menu, move the mouse over the entry you want to select and release the mouse button.

For example, you can pull down the Edit menu and choose Select All to select all icons on the desktop, as shown in the following window:
Mnemonics

Pull-down menu items display a mnemonic indicated by an underlined letter. You can use this letter to select menu items without having to use the mouse.

In these menus, the first letter of each item is underlined. To access the Desktop menu, for example, without using the mouse, press the Alt+d key combination. When the menu is displayed, press the t key to access the TMR Connection menu, and then press the s key to select Secure Connect from the submenu. Case is not important when using mnemonics.

You can also use the arrow keys to move up and down the list of menu items.

Note: For Sun Microsystems machines, use the meta-key (with the diamond symbol) instead of the Alt key.
Submenus

Some pull-down menus contain submenus. If a menu item displays a right arrow, the menu contains a submenu.

You can access a submenu by selecting the menu item containing the right arrow. Submenus can also contain other submenus. Select an item in a submenu by releasing the left mouse button on the menu item.

Pop-up Menus

Each resource icon on the Tivoli desktop has an associated pop-up menu. You can use the pop-up menu to access the resource’s associated information, windows, and dialogs. To open a pop-up menu, move the mouse over a resource icon, and press and hold the right mouse button. To select a pop-up menu item, move the mouse over the menu item you want to select and release the mouse button.
Following is an example of a pop-up menu in a window:

![Image of a pop-up menu in a window]

**Tear-off Menus (UNIX Only)**

A tear-off menu has a dashed line across the top. You can “tear off” this type of menu and leave it open on your desktop. Tear-off menus are convenient for situations in which you expect to perform a number of operations in sequence, all accessed from the same pop-up or pull-down menu.

**Note:** Tear-off menus are not available through Tivoli Desktop for Windows, including Tivoli Management Framework installed on Windows systems.
Following is an example of a tear-off menu:

To tear off a menu, pull down the menu by clicking on the menu name. Then click the dashed line at the top of the menu with the left mouse button. The menu becomes a separate item. You can then place the menu anywhere on your desktop. Following is an example of a menu that has been torn off the Tivoli desktop:

To close a menu that was previously torn off, select Close from the window manager menu in the upper-left corner of the tear-off menu or press the Esc key.

**Buttons**

Buttons perform the action associated with the button label. For example, clicking the Close button discards any unsaved changes that were made in the window and closes the window.

You can also use buttons to access window- or dialog-related information. Buttons that display ellipses (...) open other windows or dialogs.
Windows and Dialogs

For example, a button labeled **Edit**... opens an edit dialog. The following dialog contains several buttons:

![Create Administrator Dialog](image)

To perform the action associated with a button, select the button by clicking the left mouse button.

Following is a list of the most commonly used buttons in Tivoli Management Framework:

- **action & Close** Performs the specified action and closes the dialog. For example, the **Create & Close** button in the preceding dialog creates an administrator and then closes the **Create Administrator** dialog.

- **action** Performs the specified action but does not close the dialog. The **Create** button in the preceding dialog creates the administrator. The dialog remains open so that you can add additional administrators.

- **Close** Closes the dialog without performing any action. Clicking the **Close** button cancels any entries or edits made since the last time the **action** button was clicked. For example, suppose you need to add two administrators, Travis and Mary. You enter the information for Travis in the **Create Administrator** dialog and click the **Create** button. The new administrator is added to the Tivoli database and the dialog remains open. While entering the information for
administrator Mary, you realize the information is incorrect. Click the Close button. All of the information you entered for Mary is discarded. The second administrator is not added. The first administrator, Travis, remains in the database, unaffected by the close operation.

Help Displays online help for the dialog.

Text Boxes
You can use the keyboard to enter resource values in text boxes. To activate a text box, click the left mouse button over the text box. When a text box is active, a cursor is displayed in the box. You can enter values in a text box only when it is active. Following is an example of a text box:

```
Administrator Name/Icon Label
```

Press the Enter key to validate the new value. To move the cursor forward through the text boxes in a window or dialog, press the Tab key. To move the cursor backward through the text boxes in a window or dialog, press the Shift+Tab key combination.

Check Boxes
You can toggle a value on or off in a check box. The check box is filled when a feature is on and empty when a feature is off. To turn a feature on or off, click the feature’s associated check box. The feature is turned on if it was previously off, or turned off if it was previously on.

Radio Buttons
You can select one item from a group of items with a radio button. Radio buttons are mutually exclusive; clicking a radio button clears any previously selected radio button.
Windows and Dialogs

To select a radio button item, click the radio button to the left of the item.

![Radio Button Example]

A radio button that is selected appears to be filled; a radio button that is not selected appears to be unfilled.

Option Menus

An option menu displays the currently selected value for a particular field. A small button or down arrow is displayed beside the selected value.

![Option Menu Example]

Clicking the button or down arrow shows the acceptable values for the field.

![Option Menu Example]

When you select an item from an option menu, the item is displayed as the menu option’s button label. For example, if you select the Simple item from the Encryption Level menu, the button label changes to Simple.

Scrolling Lists

You can use a scrolling list to view a group of items and to select one or more items on which to perform an operation. Some lists allow only one selection; others allow multiple selections.

![Scrolling List Example]
To select an item in the list, move the mouse over the item and click the left mouse button. The item is selected if it was not previously selected, or deselected if it was previously selected. All other items are deselected.

To select multiple contiguous items, click the left mouse button on the first item and drag the mouse down the list. You can also select more than one group of contiguous items by pressing the **Ctrl** key before selecting the second group of items. If you do not press the **Ctrl** key, the first group of items will be deselected.

To select multiple discontiguous items, press the **Ctrl** key and click the left mouse button over the items to be selected.

Some dialogs have two scrolling lists with entries that you can move from one list to the other list.

To move one or more entries between scrolling lists, double-click each entry to be moved or select the entries you want to move. Then click the left or right arrow button, as appropriate.

Buttons are displayed at the bottom of some scrolling lists.

These buttons enable you to perform the following actions:

- Open a **Browser** dialog
Windows and Dialogs

- Select all items in the list
- Deselect all items previously selected
- Enter a regular expression in a text box to find an entry

After entering the regular expression, press the **Enter** key to select the next list item that matches the search criteria. You must maintain cursor focus in the search text box when you press the **Enter** key. Otherwise, the default command button will be activated.

**Regular Expressions**

A regular expression is a search string used for pattern matching in the Tivoli 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:

<table>
<thead>
<tr>
<th>Character</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>^</td>
<td>Matches lines that begin with the expression</td>
</tr>
<tr>
<td>$</td>
<td>Matches lines that end with the expression</td>
</tr>
<tr>
<td>.</td>
<td>Matches a single character</td>
</tr>
<tr>
<td>*</td>
<td>Matches zero or more characters</td>
</tr>
<tr>
<td>[Rr]</td>
<td>Matches any one character in brackets</td>
</tr>
<tr>
<td>[c–z]</td>
<td>Matches any character in the sequence</td>
</tr>
<tr>
<td>[^c–z]</td>
<td>Matches characters not in the sequence</td>
</tr>
</tbody>
</table>
Windows and Dialogs

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

<table>
<thead>
<tr>
<th>Character</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>\</td>
<td>Matches any character by disabling special meaning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Character</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>balder</td>
<td>blue</td>
</tr>
<tr>
<td>gate–1</td>
<td>green</td>
</tr>
<tr>
<td>odin</td>
<td>orange</td>
</tr>
<tr>
<td>red</td>
<td>thor</td>
</tr>
<tr>
<td>yellow</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Regular Expression</th>
<th>Search Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>^b</td>
<td>Returns system names beginning with the letter b: balder and blue</td>
</tr>
<tr>
<td>e$</td>
<td>Returns system names ending with the letter e: blue and orange</td>
</tr>
<tr>
<td>.n</td>
<td>Matches any character preceding the letter n: green, odin, orange, and rainbow</td>
</tr>
<tr>
<td>[dk]</td>
<td>Returns system names containing the letter d or k: balder, loki, odin, and red</td>
</tr>
<tr>
<td>[o–s]</td>
<td>Returns system names containing the letters o through s: balder, frey, green, loki, odin, orange, rainbow, red, thor, violet, and yellow</td>
</tr>
</tbody>
</table>
Some scrolling lists enable you to open the Browser dialog, which is indicated by the presence of the Browser button:

A Browser dialog displays a scrolling list that contains the same items as the browser’s associated scrolling list. However, with a browser list you can resize the dialog so that you can view more of the items without scrolling. Doing so makes it easier to select an item from a large number of entries.

To access a Browser dialog, such as the following example, click the Browser button at the bottom of the scrolling list:

You can also search for items in a Browser dialog by specifying a regular expression in the text box and pressing the Enter key. Any matching items will be selected. Click the Search All and Search Next buttons to iterate through the list of items to find either all matches or the next match, respectively.

When you select items in a Browser dialog, the items selected in the associated scrolling list are also updated. After you close the Browser
The Desktop

dialog, you are returned to the scrolling list. The items you selected in the Browser dialog are highlighted in the scrolling list.
To close a Browser dialog and return to the associated scrolling list, click the Ok button.

Status Lines

A status line is displayed at the bottom of some windows and dialogs to provide a short description of what action will be initiated if a button is clicked or a menu item selected. For example, when you move the mouse over entries in a pull-down or pop-up menu, the status area at the bottom of the dialog or window provides a description of the action associated with each entry.

Status Messages

Similarly, when an operation has been invoked that may take more than a few seconds, status messages are sent to the Operation Status area on the main desktop to indicate the progress of the operation.

File Browser Dialog

On some dialogs, you must specify a file to be used for a particular operation. For example, during installation you might need to change the directory path to access the installation media. When a path to a
directory or file is required, Tivoli Management Framework displays the **File Browser** dialog.

When appropriate, the dialog contains a **Hosts** scrolling list from which you can specify the system on which the file is located. Following are two examples of the **File Browser** dialog:

The **File Browser** dialog enables you to identify or specify the path to a file. If you already know the path to the file you want, perform the following steps:

1. Enter the full path and file name in the **Path Name** text box.
2. Click **Set Path** to change to the specified directory.
3. Click **Set Media & Close** to save the path and close the **File Browser** dialog.

If you do not know the exact path to the file you want, perform the following steps:

1. From the **Host** scrolling list, select the host on which the file is located. Choosing a host updates the **Directories** scrolling list to show the directories of the host you chose.
2. From the **Directories** scrolling list, select the directory containing the file. Choosing a directory updates the **Files** scrolling list to show the files contained in the directory you chose.
   a. If desired, enter a regular expression in the **File Name Filter** text box to limit the number of file names in the **Files** scrolling list.
list. See “Regular Expressions” on page 1-14 for information about regular expressions.

b. Click Filter to update the Files scrolling list with only those files matching the regular expression. You can then select the correct file.

3. Select a file from the Files scrolling list.

4. Click Set File & Close to save the path and close the File Browser dialog.

**Tivoli Desktop Menus**

The Tivoli desktop contains four pull-down menus: Desktop, Edit, View, and Create. The following sections describe each of these menus and their associated menu options.

**Desktop Menu**

The Desktop menu provides access to operations for the Tivoli management region. Many of these operations require the highest Tivoli authorization roles.

**Navigator**

Opens the Desktop Navigator. The Desktop Navigator allows you to view all of the resources in a Tivoli management region. You can open the Desktop Navigator regardless of your authorization roles. You cannot, however, perform operations on the resources in the Desktop Navigator unless you have the appropriate authorization role for the selected resource. See “Desktop Navigator” on page 1-21 for more information.

**Backup**

Opens the Backup Tivoli Management Region dialog from which you can back up one or more managed nodes. You must have the backup role or super role in the Tivoli management region to perform a Tivoli backup.
Tivoli Desktop Menus

TMR Connections
Enables you to create, maintain, list, and delete Tivoli management region connections between the local region and other regions. From this menu, you can also view all top-level policy regions that are available in your Tivoli management region. These policy regions might be local to your Tivoli management region or exchanged from a region connected to your region. You must have the super role to connect or disconnect regions.

Install
Enables you to install other Tivoli products or patches. You must have the install-product role or the super role in the Tivoli management region to perform these installations.

Maintenance
Opens the TMR Maintenance Mode dialog, which allows you to put your local Tivoli management region into maintenance mode. You can also transmit maintenance messages to Tivoli administrators.

About
Opens the About Tivoli dialog. From this dialog, you can view the products and patches currently installed and send e-mail to your Tivoli support provider.

Quit
Closes the Tivoli desktop.

Edit Menu
The Edit menu contains the following options:

Select All
Highlights all icons on the desktop.

Deselect All
Removes the highlighting from all icons on the desktop.

Remove
Removes an icon from the desktop. However, the Tivoli object associated with the icon is not deleted from the database. If you use this option in a collection, the object is removed from the collection but not from the desktop.
To return the icon to the desktop, you can either drag it from another desktop or use the `wln` command. See the `wln` command in the *Tivoli Management Framework Reference Manual* for additional instructions.

### Delete
Deletes an icon from desktops and collections, and also deletes the associated object from the database.

### View Menu
The View menu allows you to change the look of the resources on the desktop. You can choose to view the resources by icon or by name. From this menu you can also refresh the desktop.

### Create Menu
The Create menu allows you to create additional desktop resources such as policy regions or collections. (For more information about collections, see “Collections” on page 1-23.) The contents of this menu change depending on which Tivoli products are installed.

### Desktop Navigator
The Desktop Navigator 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 local Tivoli management region’s name registry. When you double-click the task library name, the correct task library window opens.
The following diagram shows the Desktop Navigator dialog:

The Navigate To scrolling list shows the resource types you can access through the navigator. The contents of this list vary depending on the resources you have created and the applications you have installed. When you select a resource type from the Navigate To list, the Resources scrolling list is refreshed with the names of each instance of the resource type you selected.

You can limit the contents of the Resources scrolling list by using the Filter text box. To filter the contents of the list, enter a regular expression in the Filter text box and click the Filter button. See “Regular Expressions” on page 1-14 for more information.
Collections

After you become familiar with the desktop, you may want to define shortcuts to frequently accessed resources. For example, for authorization or policy reasons, there may 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 Tivoli collection.

A collection is a container that you create and place on the 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. You can create collections from the desktop only.

To create a collection, perform the following steps:

1. From the Create menu, select the Collection option.

The Create Collection dialog is displayed.
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 **Create Collection** dialog.

To populate the collection, open one or more windows and use drag-and-drop 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. Remember, the icons in a collection are a *link* to the original resource, not a duplicate of the resource.

---

**Tivoli Icons**

Following are icons you might see while using the Tivoli desktop:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Tivoli Policy Region" /></td>
<td>The <strong>Tivoli Policy Region</strong> icon. One icon is displayed for each policy region you create. Double-click this icon to open a policy window, or use the right mouse button to open the icon’s pop-up menu.</td>
</tr>
<tr>
<td><img src="image" alt="Notification Bulletin Board" /></td>
<td>The <strong>Notification Bulletin Board</strong> icon with no messages. This icon indicates no messages are waiting to be read.</td>
</tr>
<tr>
<td><img src="image" alt="Notification Bulletin Board" /></td>
<td>The <strong>Notification Bulletin Board</strong> icon with messages. Double-click this icon to read your messages.</td>
</tr>
<tr>
<td><img src="image" alt="Scheduler" /></td>
<td>The <strong>Scheduler</strong> icon. Double-click this icon to schedule a job, or drag and drop a job icon onto the <strong>Scheduler</strong> icon.</td>
</tr>
<tr>
<td>Icon</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td><img src="image" alt="Administrator Collection" /></td>
<td>The <strong>Administrator Collection</strong> icon. An administrator collection contains icons for all administrators in a Tivoli installation. Double-click this icon to open the <strong>Administrator</strong> window, or use the right mouse button to open the icon’s pop-up menu.</td>
</tr>
<tr>
<td><img src="image" alt="Endpoint Manager" /></td>
<td>The <strong>Endpoint Manager</strong> icon. Double-click this icon to see a list of endpoints in the Tivoli management region.</td>
</tr>
<tr>
<td><img src="image" alt="Administrator" /></td>
<td>The <strong>Administrator</strong> icon. One icon is displayed for each administrator in the policy region. Use the right mouse button to open the icon’s pop-up menu.</td>
</tr>
<tr>
<td><img src="image" alt="Collection" /></td>
<td>The <strong>Collection</strong> icon. Double-click this icon to see the contents of the collection.</td>
</tr>
<tr>
<td><img src="image" alt="Task Library" /></td>
<td>The <strong>Task Library</strong> icon. One icon is displayed for each task library in the policy region. Double-click this icon to see the jobs and tasks contained in a task library.</td>
</tr>
<tr>
<td><img src="image" alt="Task" /></td>
<td>The <strong>Task</strong> 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.</td>
</tr>
<tr>
<td><img src="image" alt="Job" /></td>
<td>The <strong>Job</strong> icon. One icon is displayed for each job in a task library. Double-click this icon to run the job. You can also drag and drop this icon onto the <strong>Scheduler</strong> icon to schedule the job to run later.</td>
</tr>
<tr>
<td><img src="image" alt="Database Profile Manager" /></td>
<td>The <strong>Database Profile Manager</strong> 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 see the profiles contained in the profile manager.</td>
</tr>
</tbody>
</table>
## Tivoli Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Tivoli Icons" /></td>
<td>The <strong>Dataless Profile Manager</strong> icon. One icon is displayed for each dataless profile manager in the policy region. A dataless profile manager can distribute to any Tivoli client—managed nodes and endpoints—but not to other profile managers. Double-click this icon to see the profiles contained in the profile manager.</td>
</tr>
<tr>
<td><img src="image" alt="Tivoli Icons" /></td>
<td>The <strong>Tivoli Managed Node</strong> icon. One icon is displayed for each client on which Tivoli Management Framework is installed.</td>
</tr>
<tr>
<td><img src="image" alt="Tivoli Icons" /></td>
<td>The <strong>Tivoli Endpoint Client</strong> icon. One icon is displayed for each endpoint client. Unlike for managed nodes, you cannot toggle this icon to a server icon.</td>
</tr>
<tr>
<td><img src="image" alt="Tivoli Icons" /></td>
<td>The <strong>Connect TMRs</strong> icon. This icon appears on dialogs for connecting or maintaining Tivoli management regions.</td>
</tr>
<tr>
<td><img src="image" alt="Tivoli Icons" /></td>
<td>The <strong>Install Client</strong> icon. This icon appears on client installation dialogs.</td>
</tr>
<tr>
<td><img src="image" alt="Tivoli Icons" /></td>
<td>The <strong>Install Tivoli Server</strong> icon. This icon appears on server installation dialogs.</td>
</tr>
<tr>
<td><img src="image" alt="Tivoli Icons" /></td>
<td>The <strong>Patch Install</strong> icon. This icon appears on patch installation dialogs.</td>
</tr>
<tr>
<td><img src="image" alt="Tivoli Icons" /></td>
<td>The <strong>TMR Backup</strong> icon. This icon appears on Tivoli management region backup dialogs.</td>
</tr>
<tr>
<td><img src="image" alt="Tivoli Icons" /></td>
<td>The <strong>Tivoli Desktop</strong> icon. This icon appears when you iconify the main Tivoli desktop.</td>
</tr>
</tbody>
</table>
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 management regions is down or unavailable.
The Tivoli environment can include the following two 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 management region server (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 Tivoli management region server database. A managed node can also be a proxy system for a gateway. For more information about gateways, see the Tivoli Management Framework Planning for Deployment Guide.

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 tasks. 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. For more information about endpoints, see the Tivoli Management Framework Planning for Deployment Guide.

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

about the Desktop for Windows, see the Tivoli Enterprise Installation Guide.

Each Tivoli client is a managed resource and represents a single machine in the Tivoli management region. One icon is displayed in a Policy Region dialog for each managed node in the Tivoli management region. By default, endpoint icons are not added to a policy region. You can add 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. You can also use the after_install_policy script to add endpoints to policy regions after the endpoint is installed. See the Tivoli Management Framework Reference Manual for more information about the wmv command and the after_install_policy script.

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 dialog 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.

Icons

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 dialog unless you add them to the policy region using the wmv command or the after_install_policy script, as stated previously. Regardless of whether the endpoint icon is displayed in the policy region, you will see the endpoint icons in the subscriber section of the Profile Manager dialog. The following is the icon for a managed node:
Managed node icons have two states, server and client, which you can toggle depending on the machine’s role in your organization. The icons have identical functionality, and changing the icon state has no affect on Tivoli Management Framework operations. (The endpoint icon cannot be changed to a server icon.)

Following are examples of the managed node server icon:

```
[Icons]
```

Following are examples of the managed node client icon:

```
[Icons]
```

**Managed Nodes**

Managed node icons represent machines running a supported version of UNIX or Windows.

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

```
Open... Properties... Run xterm Toggle icon... Synchronize...
```

- **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.
### Moving a Client

**Run xterm**  
Opens an Xterminal session on the machine. This option is not valid on Windows; if you select this option, an error message is displayed.

**Toggle Icon**  
Toggles the managed node icon from a client to a server and back.

**Synchronize**  
Allows you to synchronize the information stored in one or more profiles with the corresponding data in system files. See Chapter 6, “Configuration Management” for more information about synchronizing profiles.

### Endpoints

An endpoint is a Tivoli resource that can be created on UNIX or PC platforms, including NetWare and OS/2. Endpoints communicate with endpoint gateways, but rarely with the Tivoli management region server.

The endpoint icon does not have a pop-up menu. To review the properties of an endpoint, you must go through the endpoint manager. See “Endpoint Properties” on page 2-15 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 region. However, any subscriptions that the managed node has remain intact and fall under the default and validation rules of their respective policy regions. See Chapter 6, “Configuration Management” for more information about subscriptions.

Because the move operation cuts the client from one policy region and pastes it in another, you must have appropriate authorization in both policy regions. In addition, you must have the Tivoli role of senior. For example, if you have permission to cut from the original policy region but do not have permission to paste 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 tasks:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cutting a client from a policy region</td>
<td>Policy region</td>
<td>senior</td>
</tr>
<tr>
<td>Pasting a client in a policy region</td>
<td>Policy region</td>
<td>senior</td>
</tr>
</tbody>
</table>

**Note:** You also need the Tivoli role of senior to complete this activity.

You can move a client from one region to another using either drag and drop 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 a managed node from one policy region to another, see the `wmv` command in the *Tivoli Management Framework Reference Manual.*
Client Properties

Each Tivoli client has a set of associated properties, which you can view from the Managed Node dialog. The information included on this dialog varies by machine type and client type. Generally, this information includes machine name, operating system, and IP addresses.

Managed Nodes

Selecting Properties from the pop-up menu of a managed node icon allows you to display properties about the machine associated with that icon.

Following is an example of the Managed Node dialog:

![Managed Node dialog example]

The Properties list in this dialog displays information about the managed node, including the system name and ID, memory size, and operating system version. You cannot edit these fields.
Client Properties

Note: To view managed node properties from the command line, see the **whostid**, **wmanode**, **wmensize**, and **wuname** commands in the *Tivoli Management Framework Reference Manual*.

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**. 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 dialog. 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. See the *Tivoli Management Framework Reference Manual* for more information.

In the preceding example, the system name and primary IP interface name are the same, **vernon**. On your system, the names may be different.

**Adding a Managed Node IP Interface**

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

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.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding an entry to the IP interface list</td>
<td>Managed node</td>
<td><strong>admin</strong></td>
</tr>
</tbody>
</table>
To add an IP interface for the managed node, perform these steps:

1. From the pop-up menu of the managed node icon, select **Properties** to display the **Managed Node** dialog:

![Managed Node dialog]

2. Click **Add Interface** to display the **Add IP Interface** dialog:

![Add IP Interface dialog]
3. In the **Interface Device Name** text box, type the device name.

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 address.

5. In the **Name** text box, enter the name of the IP interface.

6. Select the **Make interface available to Tivoli daemon** check box if you want to notify the Tivoli software of the existence of the new IP address as a communication channel.

7. Click **Continue** to add the IP interface and return to the **Managed Node** dialog.

8. Click **Update & Close** to execute the changes you have made and close the dialog.

**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 a Managed Node IP Interface**

When you edit an IP interface, you can change the IP address or the IP name. If the Tivoli User Administration application is installed, this operation also updates the information associated with the appropriate managed node.

**Note:** If the machine has already had the IP interface changed 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.
The following table provides the context and authorization role required for this task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing an entry in the IP interface list; options include changing the IP address or IP name</td>
<td>Managed node</td>
<td>admin</td>
</tr>
</tbody>
</table>

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

**Desktop**

To edit an entry in the IP interface list of a managed node, perform the following steps:

1. From the pop-up menu of the managed node icon, select **Properties** to display the **Managed Node** dialog:
Note: You cannot edit the entry for the primary interface or the loopback interface from the Managed Node dialog. Use the wifconfig command to change the IP address for the local system. For more information, see the Tivoli Management Framework Reference Manual.

2. Select an entry in the IP Interfaces scrolling list and click the Edit Interface button. The Edit IP Interface dialog is displayed:

![Edit IP Interface Dialog](image)

This dialog allows you to change the IP address or the name of a managed node.

3. To change the IP address, enter 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 address.

4. To change the entry’s IP interface name, enter 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 dialog.

7. Click Update & Close to execute the changes you have made and close the dialog.
Command Line

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

Removing a Managed Node IP Interface

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

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

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removing an entry from the IP interface list</td>
<td>Managed node</td>
<td>admin</td>
</tr>
</tbody>
</table>

Desktop

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

1. From the pop-up menu of the managed node icon, select **Properties** to display the **Managed Node** dialog:
You cannot remove the primary IP address or loop interface. If you attempt to remove this address, you receive an error message.

2. From the list of interfaces in the **IP Interfaces** scrolling list, choose one or more entries.

3. Click **Remove Interface**.

4. Click **Update & Close** to execute the changes you have made and close the list.

**Command Line**

For information about using the `wifconfig` command to remove an IP interface from a managed node, see the *Tivoli Management Framework Reference Manual*. 
Opening an xterm Session on a UNIX Managed Node

You can open an Xterminal (xterm) session on a managed node from the pop-up menu of the UNIX managed node icon. This terminal 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 the Tivoli desktop from a PC, you must be running X Window System software to display the xterm.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opening a remote xterm</td>
<td>Managed node</td>
<td>user</td>
</tr>
</tbody>
</table>

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

**Desktop**

To open an xterm on the managed node:

1. From the pop-up menu of the managed node icon, select `Run xterm` to open an xterm window with your login name as the user.
   
   **Note:** If you do not have an account on the selected managed node, you will not be able to open an xterm window.

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 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 using the `wxterm` command to open an xterm on a managed node, see the Tivoli Management Framework Reference Manual.

Endpoint Properties

The Endpoint Properties dialog provides information about an endpoint. You cannot edit this information directly from this dialog. However, you can change the endpoint’s port number by restarting the endpoint with the `lcfd -P` or `lcfd.sh -P` command.

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 command `lcfd -xIPX -gIPXaddress+port` where `IPXaddress` 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 command `lcfd -xTCPIP -gIPaddress+port` where `IPaddress` is the TCP/IP address for the gateway of your previous connection.

Viewing from the Endpoint Manager

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

1. Double-click the endpoint manager icon to open the Gateway List dialog:
2. Double-click the gateway to which the endpoint is assigned to open the **Endpoint List** dialog:
3. Double-click the appropriate endpoint to open the **Endpoint Properties** dialog:

![Screenshot of Endpoint Properties dialog]

**Viewing from Web Browser**

You can also view endpoint properties from a Web browser. In fact, 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 in the **Location** text box:

```
http://hostname:port_number
```

where:

- `hostname` Specifies the name of the endpoint
- `port_number` Specifies the port number the endpoint is using
Entering an endpoint URL displays the following page:

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

**Version**  Shows the endpoint software version number.

**Interp**  Shows the interpreter type of this endpoint.

**Hostname**  Shows the name of the endpoint machine.

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

**Status**  Shows the current status of the endpoint. Following are possible entries:
Client Properties

**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 lcfd.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 restarted.

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

**Show Logfile** Displays the contents of the lcfd.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 spawner checked the cache for a method and found the method.
- **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 have been 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 lcfd.cfg file.

Show Trace Log
Displays code tracing message. The trace log is for debugging purposes only.

Network Addresses Configuration
Displays configuration information for the endpoint’s assigned gateway. Following is an example of the Location Configuration page:
At the bottom of the Location Configuration page is the Additional configuration options text box. Using this text box, you can enter lcfd command options, which modify the endpoint’s startup files. Although many lcfd command options require a manual restart of the endpoint daemon, you can reset the amount and type of debug messages written to the lcfd.log file (using the lcfd –d 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, enter the IP address or IP address and port number of the new gateway.

   ![Additional configuration options](image1)

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

   ![Username and Password Required](image2)

3. Enter the user name and password assigned to the endpoint. The user ID and password of an endpoint are randomly generated when the endpoint logs in to its gateway. Use the **wep** command to retrieve the ID and password for an endpoint. For more information about endpoint **http** passwords, see the *Tivoli Management Framework Planning for Deployment Guide*. 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 interfaces are added to the list used by **lcfd** to search for a gateway.

For gateways that support IPX, gateway information can be viewed from the Tivoli Management Gateway Web browser. To view this gateway information, enter the following URL in the **Location** text box:

**http://hostname:port_number**
From this browser, you can accomplish a variety of tasks that include the following:

- Viewing endpoints
- Choosing an endpoint’s protocol
- Searching for an endpoint
- Viewing gateways

Starting or Stopping the Endpoint Daemon

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

NetWare

To start an endpoint from the NetWare console, enter `lcf` command. To stop an endpoint from the NetWare console, enter the `lcfstop` command.

Windows NT or Windows 2000

You can start and stop an endpoint from the Windows desktop or from the command line.

**Desktop**

Select Control Panel→Services, and then start or stop the Tivoli Endpoint service.
Command Line

Use the `net start lcfd` or `net stop lcfd` command to start or stop Windows NT or Windows 2000 endpoints.

Windows 95 or Windows 98

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

Use the `lcfd -r` command to stop the endpoint.

UNIX Endpoints

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

OS/2 Endpoints

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

Starting and Stopping AS/400 Endpoints

This section contains information about starting and stopping the AS/400 endpoint.

Starting AS/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 `$BINDIR/./lcf_bundle/generic/lcfd.sh` script, which is available for other platforms.

The `STRTMEEPT` command starts the QLCD job on the AS/400 with the appropriate configuration information. To enter endpoint configuration parameter 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:

<table>
<thead>
<tr>
<th>Keyword and Description</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>LGNINTRFC</td>
<td>Login interface</td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>Hostname</td>
</tr>
<tr>
<td></td>
<td>Port</td>
<td>Port number</td>
</tr>
<tr>
<td>GATEWAY</td>
<td>Gateway</td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td>Name</td>
<td>Hostname</td>
</tr>
<tr>
<td></td>
<td>Port</td>
<td>Port number</td>
</tr>
<tr>
<td>BCASTDSBL</td>
<td>Broadcast disable</td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*YES or 1 to disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*NO or 0 to enable</td>
</tr>
</tbody>
</table>
## Client Properties

<table>
<thead>
<tr>
<th>Keyword and Description</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>EPTNAME</strong></td>
<td>Endpoint name</td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*HOSTNAME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the host name as the name for this</td>
</tr>
<tr>
<td></td>
<td></td>
<td>endpoint.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*HOSTNAME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the host name as the name for this</td>
</tr>
<tr>
<td></td>
<td></td>
<td>endpoint.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*HOSTNAME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use a valid AS/400 endpoint name</td>
</tr>
<tr>
<td><strong>PORT</strong></td>
<td>Local TCP/IP port</td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*HOSTNAME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the host name as the name for this</td>
</tr>
<tr>
<td></td>
<td></td>
<td>endpoint.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*HOSTNAME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use a valid AS/400 endpoint name</td>
</tr>
<tr>
<td><strong>MACHINEID</strong></td>
<td>Machine unique ID</td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*HOSTNAME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use a string that contains a unique</td>
</tr>
<tr>
<td></td>
<td></td>
<td>identifier</td>
</tr>
<tr>
<td><strong>THRESHOLD</strong></td>
<td>Log threshold</td>
<td>The following are valid entries:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0   No message logging</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1   Minimal logging (default)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2   Tracing and moderate output</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3   Data buffers and tight loops</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4   Data</td>
</tr>
<tr>
<td><strong>LOGSIZE</strong></td>
<td>Log size</td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*HOSTNAME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use a value between 10240 and 10240000.</td>
</tr>
<tr>
<td><strong>LOGQSIZE</strong></td>
<td>Log queue size</td>
<td>*NONE</td>
</tr>
<tr>
<td></td>
<td></td>
<td>*HOSTNAME</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use a value between 10240 and 10240000.</td>
</tr>
</tbody>
</table>
### Client Properties

#### LOGFILE
- **Specifies the name of the log file to be used for logging messages.**
- **Path name**
- Where path name is the name of the integrated file system (IFS) file used for the log.

#### CACHE SIZE
- **Specifies the maximum size of the method cache.**
- **Cache size**
- *NONE
  - size and integer

#### UDP INTERVAL
- **The number of seconds between endpoint broadcast calls.**
- **UDP interval**
- *NONE
  - seconds

#### UDP ATTEMPT
- **The number of times an endpoint will transmit a broadcast call.**
- **UDP attempts**
- *NONE
  - number of times where number is an integer value

#### START MEOUT
- **The amount of time in seconds before a communications timeout occurs during login.**
- **Start timeout**
- *NONE
  - seconds

#### RUN MEOUT
- **The amount of time in seconds before a communications timeout occurs following a successful login.**
- **Run timeout**
- *NONE
  - seconds

#### CFG FILE
- **The name of the configuration file to be used to start the endpoint.**
- **Configuration file name**
- *NONE
  - config_file_name
Stopping AS/400 Endpoints

The ENDTMEEPT command stops the endpoint daemon process for an endpoint. The job may be on a job queue, it may be active within a system, or it may have already completed running. Spoooled 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 DELAY (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.

---

<table>
<thead>
<tr>
<th>Keyword and Description</th>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RUNDIR</strong></td>
<td>Running directory</td>
<td>*NONE directory_name</td>
</tr>
<tr>
<td>*NONE</td>
<td>directory_name</td>
<td></td>
</tr>
</tbody>
</table>
Toggling a Managed Node Icon

You can toggle the icon associated with a managed node from client to server or from server to client.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toggling the icon for a managed node</td>
<td>Policy region</td>
<td>admin</td>
</tr>
</tbody>
</table>

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

1. From the pop-up menu of the managed node icon, select **Toggle Icon** to display the **Client/Server Icon Toggle** dialog:

2. Select the appropriate check box to indicate the icon type you want to associate with the managed node.

3. Click **Set & Close** to execute your change and return to the desktop. The icon in the policy region window is updated.
A *Tivoli administrator* is a person with a user account on a computer system with Tivoli Management Framework installed who is assigned to manage one or more policy regions in the Tivoli environment. Tivoli administrators can perform system management tasks and manage policy regions in one or more networks.

### Administrators Collection Icon

The Tivoli Administrators Collection icon contains an icon for each administrator defined for the local Tivoli management region and any connected regions. The pop-up menu for the initial **Administrators** icon (contained on the **root** administrator’s desktop) identifies the resource and includes the following options:

- **Open**
  - Opens the **Administrators** window and shows any Tivoli administrators defined in either the local Tivoli management region or any connected region.

- **Create Administrator**
  - Displays the dialog that allows you to create additional Tivoli administrators.
Administrator Logins

When you create an administrator, you must provide two login names. One is the user login name on the Create Administrator dialog, which is shown in step 1 on page 3-7. The second is the administrator login name on the Set Login Names dialog, which is shown in step 6 on page 3-10.

The user login name that you enter on the Create Administrator dialog is the user name under which some Tivoli operations will run. Generally, on UNIX systems, Tivoli operations are performed as the user nobody. If the nobody user does not exist, the Tivoli user account tmersrvd is added. On Windows and NetWare, most operations are performed as tmersrvd, which is created during installation. However, some methods utilize a Tivoli Management Framework feature that runs operations with the user name that maps to the administrator who is running the method.

The user login name that you enter on the Create Administrator dialog must match a valid UNIX or Windows user account name. An administrator must have a user account on every system that he or she is going to manage. Operations that require the user login name will not be started if the administrator does not have a user account on the managed node. Following are examples of activities that require the user login name:

- Saving task output to a file. The user must have write access to the appropriate directory and file.
- Running an xterm session from a managed node.
- Performing backups.

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

- username
- NTdomain\username

The second login name you provide while creating a Tivoli administrator is on the Set Login Name dialog. To start a desktop as a Tivoli administrator, a user must have a valid system login name. When you create an administrator, you specify the user login name that will access the administrator desktop that you are creating. You can also limit the managed nodes from which the administrator can open the
Managing Multiple Logins

desktop by specifying a managed node name with the user login name. The administrator login name should be in one of the following formats:

- `username`
- `username@ManagedNode`
- `NTdomain\username`
- `NTdomain\username@ManagedNode`
- `kerberos-name:realm`

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

If you enter an unqualified login name (that is, `username`, `NTdomain\username`, or `kerberos-name:realm`), the administrator can bring up the desktop from any machine in the local Tivoli management region. If you enter a qualified login name (`username@ManagedNode` or `NTdomain\username@ManagedNode`), the administrator can bring up the desktop only from the specified managed node.

For example, Mario cannot start his Tivoli desktop on managed node `thor` unless the login `mario` or `mario@thor` is specified on the Set Login Name dialog. If he has only the login `mario@loki`, mario can bring up a desktop only on `loki`.

See “Creating a Tivoli Administrator” on page 3-7 for information about creating an administrator.

Managing Multiple Logins

In a heterogeneous environment, an administrator might have different user names on different operating systems. Administrator Chris might have the user name `chriss` on Solaris accounts but have the user name `chris_sanders` in a Windows domain.

To allow administrators to log in to Tivoli Management Framework or perform some Tivoli operations with a single login name, regardless of the system they are currently using, Tivoli Management Framework provides user login maps. A user login map enables Tivoli Management Framework with associate a single user login name to the correct user account on a specified operating system.
A user login map consists of the map name, an interpreter type, and the user name on that interpreter type. The following is an example of three user login maps, each with multiple entries:

root_user   default    root
root_user   w32-ix86   Administrator
root_group  default    root
root_group  w32-ix86   Administrator
root_group  solaris2   wheel
chris       solaris2   chriss
chris       w32-ix86   chris_sanders

You can enter the map name into Tivoli dialogs as $map_name. For example, you can enter $chris in the Execution Privileges text boxes (User Name or Group Name) of the Create Task dialog. If the task is then executed on a Solaris system, Tivoli Management Framework resolves the map name to user name chriss. If the job runs on a Windows system, Tivoli Management Framework resolves the map name to user name chris_sanders. You can also enter a map name in the User Login Name and Group Name text boxes of the Create Administrator dialog.

To create, edit, or remove a user login map, use the widmap command. See the Tivoli Management Framework Reference Manual for complete details on using this command.

**Viewing Tivoli Administrators**

You can view the administrators in a Tivoli management region by opening the Administrator collection.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing Tivoli...</td>
<td>Tivoli desktop</td>
<td>user</td>
</tr>
</tbody>
</table>

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

To view all administrators, perform the following steps:

1. Double-click the Administrators icon to display the Administrators window.

- Each icon represents a Tivoli administrator. The icon label is the administrator’s name. Depending on the size of your organization, you may have only a few or many Tivoli administrators. Each icon has a pop-up menu that allows you to edit the administrator properties, such as the administrator’s Tivoli management region roles, resource roles, logins, and notice groups. To make changes to any of the Tivoli administrators, you must have the super or senior role over the Administrators resource, as well as be the root administrator as defined by wauthadmin.

- The pop-up menu on each administrator’s icon identifies the resource (for example, the name of the specific Tivoli administrator) and includes the following options:
### Viewing Tivoli Administrators

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Open</strong></td>
<td>Displays the desktop for the administrator you selected</td>
</tr>
<tr>
<td><strong>Edit Properties</strong></td>
<td>Allows you to change the name, user login name, and group name associated with an administrator</td>
</tr>
<tr>
<td><strong>Edit TMR Roles</strong></td>
<td>Allows you to change the roles an administrator has in the local Tivoli management region and any connected region</td>
</tr>
<tr>
<td><strong>Edit Resource Roles</strong></td>
<td>Allows you to change the roles an administrator has over specific resources in the local Tivoli management region or any connected region (for example, policy regions or the Administrator collection)</td>
</tr>
<tr>
<td><strong>Edit Logins</strong></td>
<td>Allows you to change the login names mapped to an administrator</td>
</tr>
<tr>
<td><strong>Edit Notice Group Subscriptions</strong></td>
<td>Allows you to change the notice groups to which an administrator is subscribed</td>
</tr>
</tbody>
</table>

2. To view the contents and resources on a particular administrator’s desktop, double-click the appropriate icon, which opens the window.

### Command Line

You can use either 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.
Creating a Tivoli Administrator

The `wlookup` command shows the Administrator resources, including administrator name and login names.

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

```
wgetadmin name
```

where `name` is the administrator. The `wgetadmin` command without options shows the current administrator’s name, logins, roles, and notification groups.

See the *Tivoli Management Framework Reference Manual* for complete details on using these commands.

Creating a Tivoli Administrator

You must create a Tivoli administrator for every system administrator who will manage network resources using Tivoli.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a Tivoli administrator</td>
<td>Administrator resource</td>
<td>senior</td>
</tr>
</tbody>
</table>

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

Desktop

To create a new administrator, perform the following steps:

1. From the `Administrator` icon’s pop-up menu, select Create Administrator to display the Create Administrator dialog.
Creating a Tivoli Administrator

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

   The name of a Tivoli resource, such as an administrator, 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 (" ").

3. In the **User Login Name** text box, enter the administrator’s 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 name in the form of $\text{map_name}$.

   **Note:** The value entered here is important, because it is used to determine the user ID under which many operations are performed. For example, various dialogs contain options to save output to a file on a particular machine. Such file operations are performed with a user ID calculated from the login name specified here. An operation that runs on a managed node, such as **Run Xterm**, fails if the Tivoli administrator’s user login name specified here cannot be resolved to a user ID on that machine.
4. In the Group Name text box, enter the administrator’s group name (not a numeric group ID). The group name can be a user login map name in the form of $map_name. This text box is used only for operations performed on UNIX managed nodes.

**Note:** The value entered here is important, because it is used to determine the group ID under which which operations are performed. For example, various dialogs contain options to save output to a file. Such file operations are performed with a group ID calculated from the group name specified here.

5. Click **Set TMR Roles** to set the Tivoli management region roles for the new administrator and display the **Set TMR Roles** dialog:

![Set TMR Roles dialog](image)

a. Add or remove Tivoli management region roles.

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

You can also double-click an entry in the **Available Roles** scrolling list to move it automatically to the **Current Roles** scrolling list.
Notes:

- In general, you should not need to assign an administrator a role for the Tivoli management region, but rather assign only resource roles. Tivoli management region roles are required only for specific region-wide operations, such as connecting and disconnecting regions.

- You must have the super role in the local Tivoli management region to assign an administrator the super role. In general, you cannot give someone a role that you do not have yourself.

To remove Tivoli management region roles from the administrator, select one or more roles in the Current Roles scrolling list and click the right-arrow button. The selected roles are moved from the Current Roles scrolling list to the Available Roles scrolling list.

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

You can also double-click an entry in the Current Roles scrolling list to move it automatically to the Available Roles scrolling list.

b. Click Set & Close to accept your changes and return to the Create Administrator dialog.

6. Click Set Logins to set the login names under which the new administrator will be able to start a Tivoli desktop.
The **Set Login Names** dialog is displayed:

![Set Login Names dialog](image)

a. Add or remove a login name.

   To add a login name, type the administrator’s login name in the **Add Login Name** text box and press **Enter**. The login name should be in one of the following formats:

   - `username`
   - `username@ManagedNode`
   - `NTdomain\username`
   - `NTdomain\username@ManagedNode`
   - `kerberos-name:realm`

   The new login name is added to the **Current Login Names** scrolling list. To add more than one login name, repeat this step for each login name that you want to add.

   **Note:** Tivoli recommends that all login names be qualified for a specific machine. This helps ensure the security and integrity of your distributed system by limiting the locations from which a desktop or command line interface (CLI) command may be initiated.
Creating a Tivoli Administrator

To remove a login name or Kerberos principal from the list, select the login names and principals you want to remove from the **Current Login Names** scrolling list and click **Remove**. The selected login names and principals are removed from the **Current Login Names** scrolling list.

b. Click **Set & Close** to accept your changes and return to the **Create Administrator** dialog.

7. Click **Set Resource Roles** to specify the roles the new administrator is to have over system resources.

The **Set Resource Roles** dialog is displayed:

```
<table>
<thead>
<tr>
<th>Resources:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HR</td>
<td></td>
</tr>
<tr>
<td>Marketing</td>
<td></td>
</tr>
<tr>
<td>Novellidis</td>
<td></td>
</tr>
<tr>
<td>Prod</td>
<td></td>
</tr>
<tr>
<td>Desearch</td>
<td></td>
</tr>
<tr>
<td>Scheduler</td>
<td></td>
</tr>
<tr>
<td>Software Distribution</td>
<td></td>
</tr>
<tr>
<td>Support</td>
<td></td>
</tr>
<tr>
<td>System Monitors</td>
<td></td>
</tr>
<tr>
<td>Test</td>
<td></td>
</tr>
</tbody>
</table>
```

a. Select a resource for which you want to set the administrator’s role from the **Resources** scrolling list.

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

You can also double-click an entry in the **Available Roles** scrolling list to move it automatically to the **Current Roles** scrolling list.

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

You can also double-click an entry in the **Current Roles** scrolling list to move it automatically to the **Available Roles** scrolling list.

**Notes:**

- If you want to enable an administrator to create other Tivoli administrators or schedule operations, that administrators must have one or more roles over the Administrators collection or Scheduler resource. In addition, you must drag and drop the **Administrator** icon and **Scheduler** icon onto that administrator’s desktop. See “Adding Resources to an Administrator’s Desktop” on page 3-15 for details.

- The list of roles may include others not mentioned here, depending on the particular applications installed.

c. If you want to set other resource roles, click the **Set** button. Make sure that you click the **Set** button between each resource you set.

d. Click the **Set & Close** button to accept your changes and return to the Create Administrator dialog.

8. Click the **Set Notice Groups** button to set the notice groups for the new administrator.
Creating a Tivoli Administrator

The Set Notice Groups dialog is displayed:

![Set Notice Groups dialog]

a. Subscribe as administrator to or unsubscribe an administrator from one or more notice groups.

To subscribe an administrator to one or more notice groups, select the notice groups to be added from the Available Notice Groups scrolling list and click the left-arrow button. The selected notice groups are moved from the Available Notice Groups scrolling list to the Current Notice Groups scrolling list.

You can also double-click an entry in the Available Notice Groups scrolling list to move it automatically to the Current Notice Groups scrolling list.

To unsubscribe an administrator from one or more notice groups, select the notice groups to be removed from the Current Notice Groups scrolling list and click the right-arrow button. The selected groups are moved from the Current Notice Groups scrolling list to the Available Notice Groups scrolling list.

You can also double-click an entry in the Current Notice Groups scrolling list to move it automatically to the Available Notice Groups scrolling list.
Adding Resources to an Administrator’s Desktop

Note: The set of notice groups may include others not shown here, depending on the particular applications installed. When notice groups are added by installing new applications, you must assign the new notice groups to your administrators.

b. Click Set & Close to accept your changes and return to the Create Administrator dialog.

9. Click Create & Close to create the new administrator and return to the Administrators window. The new administrator’s icon is displayed in the Administrators window.

Command Line

For information about using the command line to create a new administrator, see the wcrtadmin command in the Tivoli Management Framework Reference Manual.

Adding Resources to an Administrator’s Desktop

When you have created a Tivoli administrator with a set of roles authorizing him or her to perform management operations over a set of resources, you need to allow the administrator to access those resources from his or her desktop. In Tivoli Management Framework, providing access to a set of resources from the desktop is accomplished through drag and drop.

You can copy icons representing policy regions, task libraries, individual tasks and jobs, the scheduler, or the Administrators collection. To keep the desktop ordered, you can also create a collection and then drag and drop into it icons representing several resources.
Adding Resources to an Administrator’s Desktop

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dragging and dropping a resource onto an administrator’s desktop</td>
<td>TMR</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can add resources to an administrator’s desktop from either the desktop or the command line.

**Desktop**

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

1. Open the Administrators collection to see the icons representing the defined Tivoli administrators.

   ![Administrators collection](image)

2. Select one or more resource icons from your desktop and copy them (using drag and drop) onto an administrator’s icon. The Tivoli administrator’s desktop now contains a reference to this resource that appears on his desktop the next time it is started. If the desktop is already active, the new icon appears immediately.
Note: The Tivoli administrator on whose desktop you dropped the managed resource icon must have a role over that resource to perform management operations. If you have not yet set a role for the resource, see “Setting Resource Roles” on page 3-21 for details.

**Command Line**

For information about using the command line to set or change the resources on an administrator’s desktop, see the `wln` command in the *Tivoli Management Framework Reference Manual*.

**Setting Administrator Properties**

An administrator’s properties (name, user login name, and group name) may be changed to adjust to new and changing requirements.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting or changing a Tivoli administrator’s properties</td>
<td>Administrators collection</td>
<td>senior</td>
</tr>
</tbody>
</table>

You can change an administrator’s properties from the desktop only.

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

1. Open the Administrators collection to see the icons representing the defined Tivoli administrators.
2. From one of the existing administrators, select **Edit Properties** from the administrator icon’s pop-up menu to display the **Administrator Properties** dialog.
Setting Administrator Properties

3. Edit the name of the administrator in the Administrator Name/Icon Label text box.

4. Edit the administrator’s user login name in the User Login Name text box. The user login name must be a valid login name on all machines managed by this administrator.

   **Note:** The value entered here is important, because it is used to determine the user ID under which many operations are performed. For example, various dialogs contain options to save output to a file. Such file operations are performed with a user ID calculated from the name specified here.

5. Edit the administrator’s group name in the Group Name text box. (This text box is used only for operations performed on UNIX managed nodes.)

   **Note:** The value entered here is important, because it is used to determine the group ID under which many operations are performed. For example, various dialogs contain options to save output to a file. Such file operations are performed with a group ID calculated from the name specified here.

6. Click Change & Close to change the properties of the administrator as specified. An informational dialog is displayed:

   ![Informational Dialog]

   The changes you have just made to the administrator named [Name] will not take effect for operations related to a currently running desktop. In order for the administrator to see the effects of these changes, they will need to restart their desktop.
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.

Click **Dismiss** to return to the **Administrators** window.

### Setting Tivoli Management Region Roles

After an administrator has been defined, you might find it necessary to change the administrator’s Tivoli management region roles due to 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 administrator’s roles are mapped across all Tivoli management regions to which the administrator’s Tivoli management region is two-way connected 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 Tivoli management region, these roles map across connected regions as the **user** role. The default mapping for roles can be changed by using the **odadmin** command with the region option. See the **Tivoli Management Framework Reference Manual** for more information.

Administrators with these roles can perform tasks that require these roles only within the Tivoli management region in which 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 management region. However, creating separate administrators still does not allow tasks requiring these roles to complete across Tivoli management regions.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting or changing Tivoli management region authorization roles for a Tivoli administrator</td>
<td>TMR</td>
<td>senior</td>
</tr>
</tbody>
</table>
You can edit an administrator’s Tivoli management region authorization role from either the desktop or command line.

**Desktop**

To change an administrator’s Tivoli management region authorization roles, perform the following steps:

1. Open the Administrators collection to see the icons representing the defined Tivoli administrators.
2. From one of the existing administrators, select **Edit TMR Roles** from the administrator icon’s pop-up menu to display the **Set TMR Roles** dialog:

![Set TMR Roles dialog](image)

3. Add or remove roles in the local Tivoli management region.

To add roles in the local Tivoli management region, select one or more roles from those listed in the **Available Roles** scrolling list and click the left-arrow button. The selected roles are moved from the **Available Roles** scrolling list to the **Current Roles** scrolling list.

You can also double-click an entry in the **Available Roles** scrolling list to move it automatically to the **Current Roles** scrolling list.
Setting Resource Roles

Note: You must have the super role in the local Tivoli management region to assign an administrator the super role.

To remove roles in the local Tivoli management region, select the roles to be removed in the Current Roles scrolling list and click the right-arrow button. The selected roles are moved from the Current Roles scrolling list to the Available Roles scrolling list.

You can also double-click an entry in the Current Roles scrolling list to move it automatically to the Available Roles scrolling list.

Note: The list of roles can include others not mentioned here, depending on the particular applications installed. Tivoli management region roles are not actually added or removed until you click Change & Close or Change; they are only moved to the Current Roles or Available Roles scrolling lists.

4. Click Change & Close to add or remove the selected Tivoli management 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 an administrator’s Tivoli management region authorization roles, see the wsetadmin command in the Tivoli Management Framework Reference Manual.

Setting Resource Roles

You may need to modify resource roles for an administrator due to changing responsibilities or new resources in your environment.
Setting Resource Roles

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting or changing resource</td>
<td>Administrators</td>
<td>senior</td>
</tr>
<tr>
<td>authorization roles for a Tivoli</td>
<td>collection</td>
<td></td>
</tr>
<tr>
<td>administrator</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can set an administrator’s resource role from either the desktop or command line.

**Desktop**

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

1. Open the Administrators collection to see the icons representing the defined Tivoli administrators.
2. From one of the existing administrators, select **Edit Resource Roles** from the administrator icon’s pop-up menu to display the **Set Resource Roles** dialog:
3. From the **Resources** scrolling list, select a resource for which you want to set the administrator’s role.

4. Add or remove roles for the selected resources.

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

   You can also double-click an entry in the **Available Roles** scrolling list to move it automatically to the **Current Roles** scrolling list.

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

   You can also double-click an entry in the **Current Roles** scrolling list to move it automatically to the **Available Roles** scrolling list.
Note: The list of roles may include others not mentioned here, depending on the particular applications installed. Roles are not actually added or removed until you click the Change & Close or Change button; they are only moved to the Current Roles or Available Roles scrolling lists.

5. If you are adding more than one role, click the Change button to add or remove the selected resource roles for the administrator as specified. The Set Resource Roles dialog remains displayed.

Note: You must click the Change button for each resource to which you assign roles. For example, using the example dialog in step 2, if you want to set roles for both the NoonTide and the Scheduler resources, you must select NoonTide, select the roles, and then click the Change button. You can then select the Scheduler resource, select the roles for that resource, and click the Change button again.

6. Repeat steps 3 through 5 for each resource to which you want to assign roles.

7. Click the Change & Close button to add or remove the selected resource 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 an administrator’s resource authorization roles, see the wsetadmin command in the Tivoli Management Framework Reference Manual.

Setting Logins

Tivoli sets the logins, Kerberos principal names, and managed nodes that are valid for an administrator. Administrators can have different logins for different managed nodes. For example, administrator 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 his or her desktop from a
specific machine), the administrator must have a login name or a valid Kerberos principal on the managed node. For example, Juan cannot run as administrator `juan` on managed node `cook` unless the login `juan` or `juan@cook` is established. 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting or changing a Tivoli administrator’s logins</td>
<td>Administrators collection</td>
<td>senior</td>
</tr>
</tbody>
</table>

You can set an administrator’s logins from either the desktop or command line.

**Desktop**

To set or change an administrator’s logins, perform the following steps:

1. Open the Administrators collection to see the icons representing the defined Tivoli administrators.
2. From one of the existing administrators, select the **Edit Logins** option from the administrator icon’s pop-up menu to display the **Set Login Names** dialog:

![Set Login Names dialog](image)

3. Add or remove a login name.

To add a login name, enter the administrator’s login name in the **Add Login Name** text box and press **Enter**. The login name can be in one of the following formats:

- `username`
- `username@ManagedNode`
- `NTdomain\username`
- `NTdomain\username@ManagedNode`
- `kerberos-name:realm`

The new login name is added to the **Current Login Names** scrolling list. If you want to add more than one login, repeat this step for each login that you want to add.

**Note:** Tivoli recommends that all login names be qualified for a specific machine. This helps ensure the security and integrity of your distributed system by limiting the locations from which a desktop may be initiated.
Removing an Administrator Icon from the Desktop

To remove a login name or Kerberos principal from the list, select the login names and principals you want to remove from the Current Login Names scrolling list and click the Remove button. The selected login names and principals are removed from the Current Login Names scrolling list.

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

Command Line

For information about using the command line to set or change an administrator’s logins, see the wsetadmin command in the Tivoli Management Framework Reference Manual.

Removing an Administrator Icon from the Desktop

Tivoli Management Framework creates a database object for each administrator you add. Tivoli also creates a desktop icon for each administrator. The Administrators collection provides a menu choice for removing an administrator. Removing an administrator erases the icon from the desktop. The data object for the account, however, remains in the database. See “Deleting an Administrator” on page 3-28 for information about erasing the data 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 desktop. This tactic prevents administrators with less authority or experience from mismanaging the accounts.

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

To remove a Tivoli administrator, select **Edit**→**Remove** in the collection menu bar. The command line alternative is as follows:

```
wrn /administrators/admin_name
```

Viewing Removed Administrators

Removed administrators no longer appear on the desktop, but the account remains as an object in the database. To view a list of all administrators, including those you have removed, enter the following command: command.

```
wls /Library/Administrator
```

Restoring a Removed Administrator

Removing an administrator erases the icon from the desktop. To restore the icon, perform the following steps:

1. From the command line, enter the following command:

```
wln /Library/Administrator/admin_name /Administrators
```
   
   where `admin_name` is the label (name) you gave to the administrator icon. This command restores the icon to the Administrators collection, but the icon is not visible until you complete the next step.

2. Select **View**→**Refresh** in the collection menu bar.

   The icon is displayed on the desktop.

Deleting an Administrator

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

**Note:** Tivoli Management Framework prevents you, with a pop-up dialog, from deleting the **root** administrator. The software also prevents you from deleting the last administrator with the **admin** role. These failsafe features ensure that you retain necessary accounts.
Setting Notice Group Subscriptions

Each Tivoli administrator account displays a desktop. The desktop can contain collections specific to the account. Before deleting an administrator, delete any collections in the desktop container.

To delete a Tivoli administrator, perform the following steps:

1. Delete any collections in the administrator’s desktop.
2. Select Edit→Delete in the collection menu bar. A confirmation dialog pops up.
3. Select Yes in the confirmation dialog.

The command line alternative is as follows:

```
wdel /Library/Administrator/admin_label
```

**Setting Notice Group Subscriptions**

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

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setting or changing a Tivoli administrator’s notice group subscriptions</td>
<td>Administrators collection</td>
<td>senior</td>
</tr>
</tbody>
</table>

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

**Desktop**

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

1. Open the Administrators collection to see the icons representing the defined Tivoli administrators.
Setting Notice Group Subscriptions

2. From one of the existing administrators, select the **Edit Notice Group Subscriptions** button from the administrator icon’s pop-up menu to display the **Set Notice Groups** dialog:

3. Subscribe or unsubscribe as administrator to one or more notice groups.

To subscribe an administrator to one or more notice groups, select the notice groups from the **Available Notice Groups** scrolling list and click the left-arrow button. The selected notice groups are moved from the **Available Notice Groups** scrolling list to the **Current Notice Groups** scrolling list.

You can also double-click an entry in the **Available Notice Groups** scrolling list to move it automatically to the **Current Notice Groups** scrolling list.

To unsubscribe an administrator from one or more notice groups, select the notice groups from the **Current Notice Groups** list and click the right-arrow button. The selected groups are moved from the **Current Notice Groups** scrolling list to the **Available Notice Groups** scrolling list.

You can also double-click an entry in the **Current Notice Groups** scrolling list to move it automatically to the **Available Notice Groups** scrolling list.
Note: The set of notice groups may include others not shown here, depending on the particular applications installed. Subscriptions are not actually added or removed until you click the Change & Close or Change button.

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

Command Line

For information about using the command line to set or change a new or existing administrator’s notice group subscriptions, see the wsetadmin command in the Tivoli Management Framework Reference Manual.
A Tivoli management region consists of a Tivoli server and the set of clients that it serves. Depending on the size and operational requirements of your organization, you may have more than one Tivoli management region. See the Tivoli Management Framework Planning for Deployment Guide for deployment recommendations.

In most situations, standalone Tivoli management 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 management regions to be managed in a consistent fashion. In either case, the regions need to be connected.

After you connect Tivoli management regions, schedule periodic exchanges of resource information between them. An initial exchange occurs automatically when the regions are connected.

**Note:** You can use the scheduler service to schedule an information exchange for a later time or to update information about a regular basis. Two-way interconnected regions should update information at different times. See Chapter 10, “Tivoli Scheduler” for more information.

This chapter explains the tasks and procedures for the following topics:

- Tivoli management region connections
- Resource updates
Making a Secure Tivoli Management Region Connection

- Tivoli management region disconnection

  When Tivoli management 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 management region is complete.

Making a Secure Tivoli Management Region Connection

You can make a secure Tivoli management region connection and specify the connection properties from the Tivoli desktop. The procedure for making a secure connection must be performed locally on each of the regions that you are connecting.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Making a secure Tivoli management region connection</td>
<td>TMR</td>
<td>super</td>
</tr>
</tbody>
</table>

You can make a secure Tivoli management region connection from either the 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** dialog: 
2. Enter the name of the server you want to connect to in the **Connect to Remote Tivoli Server** text box.

3. Enter 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. See the *Tivoli Management Framework Reference Manual* for more information about the `odadmin` command.

4. Identify the encryption level from the **Remote Inter-Region Encryption** drop-down list. The possible choices are **None**, **Simple**, and **DES**. Simple encryption is recommended. DES provides the highest level of security for network traffic.

   **Note:** This option does not allow you to select a new encryption level, but rather identifies the interregion encryption level specified when you installed the remote Tivoli management region.

5. If you specified an encryption level of **DES** or **Simple** in step 4, enter the password in the **Password** text box.

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

\texttt{odadmin region set\_region\_pw}

6. Click either the \textbf{One-way} radio button to specify a one-way connection or the \textbf{Two-way} radio button to specify a two-way connection. If you specify a two-way connection, skip to step 8.

7. Click either \textbf{Make this server the manager} to make your local server the managing server, or \textbf{Make other server the manager} to make your local server the managed server.

8. Click \textbf{Connect \& Close} to initiate the secure connection on the local side. (If you are performing the connection on the managed server, skip to step 9.) The \textbf{Confirm Connect} dialog is displayed.

\begin{figure}
\centering
\includegraphics[width=\textwidth]{confirm.png}
\caption{Confirm Connect dialog}
\end{figure}

\textbf{a. Select \textit{Update all resources immediately} if you want to exchange the resource information between the Tivoli management 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.
Making a Remote Tivoli Management Region Connection

b. Click **Continue with Connection** to connect the two Tivoli management regions.

9. An informational dialog reminding you that you must complete the secure connection operation on the other server is displayed.

![Secure Connection Completed](image)

10. Click **Continue** to acknowledge the message, close the dialog, and return to the desktop.

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

When you exchange resource information between the Tivoli management regions, you can use the **Top Level Policy Regions** window on the **TMR Connections** submenu to access the icons for the top-level policy regions in the Tivoli management region to which you connected. From this window, you can drag and drop remote resources onto the appropriate local or remote administrator’s desktop. See “Tivoli Administrators and Remote Tivoli Management Region Resources” on page 4-11 for complete details.

**Command Line**

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

**Making a Remote Tivoli Management Region Connection**

You can make a remote Tivoli management 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 enter
Making a Remote Tivoli Management Region Connection

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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Making a remote Tivoli management region connection</td>
<td>TMR</td>
<td>super</td>
</tr>
</tbody>
</table>

You can make a remote Tivoli management region connection from either the 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** dialog:
2. Enter 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, specify a remote encryption level from the Encryption Level drop-down list. The possible choices are None, Simple, and DES. Simple encryption is recommended. DES provides the highest level of security for network traffic.

   **Notes:**
   - This option does not allow you to select a new encryption level, but rather identifies the interregion encryption level specified when you installed the remote Tivoli management region.
   - For a interregion encryption level other than None, you must set the region's interregion encryption password to connect successfully. To set the interregion encryption password, enter the following command:

     ```
     odadmin region set_region_pw
     ```

4. If you specified a remote encryption level of DES or Simple in step 3, enter the remote encryption password in the Password text box.
Making a Remote Tivoli Management Region Connection

**Note:** If you specified a remote encryption level of None in step 3, no remote encryption password is necessary and the Password text box is not active.

5. In the Local Inter-region Encryption group box, specify a local encryption level from the Encryption Level drop-down list. The possible choices are None, Simple, and DES. Simple encryption is recommended. DES provides the highest level of security for network traffic.

**Note:** This option does not allow you to select a new encryption level, but rather identifies the interregion encryption level specified when you installed the local Tivoli management region.

6. If you specified a local encryption level of DES or Simple in step 5, enter the local encryption password in the Password text box.

**Note:** If you selected a local encryption level of None in step 5, no local encryption password is necessary and the Password text box is not active.

7. Click either One-way to specify a one-way connection or Two-way to specify a two-way connection.

**Note:** When a remote one-way connection is made, the server making the connection is the managing server.

8. Select either Shell Service or Trusted Host Facility. Click Shell Service to set the remote access mechanism to be a shell service, and then perform the following steps:
   a. Enter a login name in the Login text box. The identified user must have the super role in the remote Tivoli management region.
   b. Enter the password in the Password text box.

Click Trusted Host Facility to set the remote access mechanism to be a trusted host.

9. Click Connect & Close to initiate the remote connection. The Confirm Connect dialog is displayed.
Making a Remote Tivoli Management Region Connection

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

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

  **Note:** If the remote Tivoli server refuses access, a dialog 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.

When you exchange resource information between the Tivoli management regions, you can use the **Top Level Policy Regions** window on the **TMR Connections** submenu to access the icons for the top-level policy regions in the Tivoli management region to which you connected. From this window, you can drag and drop remote resources onto the appropriate local or remote administrator’s desktop. See “Tivoli Administrators and Remote Tivoli Management Region Resources” on page 4-11 for complete details.
Determining the Status of Tivoli Management Region Connections

Command Line

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

Determining the Status of Tivoli Management Region Connections

You can determine the current status of a Tivoli management 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Determining the status of Tivoli management region connections</td>
<td>TMR</td>
<td>senior</td>
</tr>
</tbody>
</table>

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

Desktop

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

1. Select **TMR Connections → List Connections** from the **Desktop** menu to display the **TMR Connection Status** dialog. The local server’s name and local region are displayed at the top of the dialog.
Note: This dialog 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 the Cancel button to close this dialog and return to the Tivoli desktop.

Command Line

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

Tivoli Administrators and Remote Tivoli Management Region Resources

When two or more Tivoli management 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 management region to the desktop of a remotely defined administrator or from the 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 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 tasks:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dragging and dropping local resources onto a remote administrator’s desktop</td>
<td>TMR</td>
<td>user</td>
</tr>
<tr>
<td>Dragging and dropping remote resources onto a local administrator’s desktop</td>
<td>TMR</td>
<td>user</td>
</tr>
</tbody>
</table>

You can update the resources on either a local or remote administrator’s desktop from the 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 management regions to which you want an administrator to have access.

3. Follow the procedure described in “Adding Resources to an Administrator’s Desktop” on page 3-15 to place the selected top-level policy regions on the administrator’s desktop.

4. Ensure that the administrator has been given one or more resource roles for the top-level policy regions added to his desktop. See the procedure described in “Creating a Tivoli Administrator” on page 3-7 for details.

Exchanging or Updating Resource Information

After connecting two or more Tivoli management regions, Tivoli recommends that you 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, updating all resources more frequently than once every couple of hours is not recommended. 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.

See the appropriate Tivoli application guide for listings of which resources should be exchanged for each application.

You can update resources from either the Update Resources from Multiple TMRs dialog or the TMR Connection Status dialog. However, you can schedule updates from the Update Resources from Multiple TMRs dialog only.
Exchanging or Updating Resource Information

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchanging or updating Tivoli management region information</td>
<td>TMR</td>
<td>senior</td>
</tr>
</tbody>
</table>

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

Desktop, Update Resources from Multiple TMRs Dialog

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

1. Select TMR Connections→Update Resources from the Desktop menu to display the Update Resources from Multiple TMRs dialog.
2. Select one or more remote Tivoli management 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 from the Available Resources scrolling list to the Resources to Update scrolling list.

You can also double-click an entry in the Available Resources scrolling list 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. See Chapter 10, “Tivoli Scheduler” for details about scheduling jobs.
Exchanging or Updating Resource Information

5. To update the resource information immediately, click the Update & Close button to update the resource information for the specified resource types in the selected Tivoli management regions and return to the desktop.

Desktop, TMR Connection Status Dialog

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

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

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** dialog.

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 from the **Remote Resources** scrolling list to the **Updated Resources** scrolling list.

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

5. Click **Update & Close** to update the resource information and close the **Remote Resources** dialog.

---

**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 management 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. See 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 management 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. See the *Tivoli Management Framework Reference Manual* for usage and examples of the `wupdate` command.

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

### Command Line

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

### Disconnecting Tivoli Management Regions

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

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnecting TMRs</td>
<td>TMR</td>
<td>super</td>
</tr>
</tbody>
</table>

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

**Desktop**

To disconnect two Tivoli servers, perform the following steps:

1. Select TMR Connections→Disconnect from the Desktop menu to display the Disconnect from remote TMRs dialog.

2. Select the current connection you want to disconnect in the Current Connections scrolling list.

3. Click Disconnect & Close. A confirmation dialog is displayed.
Disconnecting Tivoli Management Regions

4. Click **Yes** if you want to continue with the disconnection of the local Tivoli management region from the selected region. The Disconnect TMRs? dialog is closed.

5. Run the `wchkdb –ux` command on ensure database consistency and repair any object references across region boundaries.

**Command Line**

For information about using the command line to disconnect two Tivoli servers, see the `wdisconn` command in the *Tivoli Management Framework Reference Manual*.
Policy 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 performed by administrators. For example, you can implement a policy that determines on which hosts a particular task or job may run or where users’ home directories are located. 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.

Tivoli Policy Region Icon

The set of managed resources accessible from the local Tivoli management 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 managed resources that are members of the policy region
Region Properties
Displays the dialog that allows you to change the name of the policy region

Managed Resources
Allows you to specify the set of valid resource types for the policy region

Managed Resource Policies
Allows you to 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 administrator’s desktop. A window similar to the following one, with an icon for each managed resource, is displayed.

The following sections describe the procedures for creating, modifying, and checking policy regions in Tivoli Management Framework.
Default Policy

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, “Configuration Management” for information about profile policies. For an example of creating and editing a default policy that is not profile-based, see the *Tivoli Management Framework Reference Manual*.

Validation Policy

A validation policy ensures that all resources in a policy region comply with the region’s established policy. 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 an example of creating and editing a validation policy, see the *Tivoli Management Framework Reference Manual*.

Creating a Top-level Policy Region

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

When the top-level policy regions are defined, subregions under them can be created to further categorize and define administrative authority and policy. 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.
Creating a Top-level Policy Region

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a top-level policy region</td>
<td>TMR</td>
<td>senior and policy</td>
</tr>
</tbody>
</table>

Note: Both the senior and policy roles are required when performing this operation from the command line if you specify the –m option. See the documentation for the wcrtpr command in the Tivoli Management Framework Reference Manual.

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

Desktop

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

1. Select Region from the Create menu on the desktop to display the Create Policy Region dialog:

   ![Create Policy Region Dialog](image)

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 management region.

   The name of a Tivoli resource, such as a top-level policy region, can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.
Creating a Policy Subregion

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

**Command Line**

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

**Creating a Policy Subregion**

After you have created one or more top-level policy regions, you can create a policy region within a policy region. A policy subregion can be used to define a different set of default policies and validation policies within a policy region. It can also be used to further categorize and scope administrative authority and responsibility.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a policy subregion</td>
<td>Policy region</td>
<td>senior and policy</td>
</tr>
</tbody>
</table>

**Note:** Both the senior and policy roles are required when performing this operation from the command line if you specify the `-m` option. See the documentation for the `wcrtp` command in the *Tivoli Management Framework Reference Manual*.

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

**Desktop**

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

1. From the policy region’s **Create** menu, select the **Subregion** option to display the **Create Policy Region** dialog:
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 Tivoli resource, such as 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 the *Tivoli Management Framework Reference Manual*.

**Changing the Name of a Policy Region**

Each policy region has a name that uniquely identifies it in the local Tivoli management region. You can change this name at any time. The following table provides the context and authorization role required for this task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Changing the name of a policy region</td>
<td>Policy region</td>
<td>senior</td>
</tr>
</tbody>
</table>

You can change the name of a policy region from the desktop only.
To change the name of a policy region, perform the following steps:

1. In the policy region, select **Policy Region** from the **Properties** menu to display the **Policy Region Properties** dialog.

2. In the **Name** text box, type a new name for the policy region.

3. Click **Set & Close** to change the name of the policy region and close the dialog.

### Changing Managed Resource Types

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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding or removing a managed resource type for a policy region</td>
<td>Policy region</td>
<td>senior and policy</td>
</tr>
</tbody>
</table>

You can add or remove managed resource types to or from a policy region from either the desktop or the command line.
Changing Managed Resource Types

Desktop

To add or remove a managed resource type to or from the policy region managed resource type list, perform the following steps:

1. In the policy region, select the Managed Resources option from the Properties menu to display the Set Managed Resources dialog.

   The Current Resources scrolling list displays the policy region’s 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 from the Available Resources scrolling list to the Current Resources scrolling list.

   You can also double-click an entry in the Available Resources scrolling list to move it automatically 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 from the Current Resources scrolling list to the Available Resources scrolling list.
You can also double-click an entry in the **Current Resources** scrolling list to move it automatically to the **Available Resources** scrolling list.

**Note:** The selected managed resource types are not actually added to or removed from the policy region until you click **Set & Close**; they are only moved to the **Available Resources** or **Current Resources** scrolling list.

3. Click **Set & Close** to add or remove the selected managed resource types from the policy region and to return to the desktop.

When you add a managed resource type to a policy region, Tivoli Management Framework assigns the policy region’s basic default policy to the managed resource type. Tivoli Management Framework also adds the managed resource type 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 the *Tivoli Management Framework Reference Manual*.

**Assigning Policy to Resources Types**

Tivoli Management Framework assigns a default policy to each resource type on the managed resource type list when you first add the resource type to the 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.
Assigning Policy to Resources Types

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assigning policy for a managed resource type</td>
<td>Policy region</td>
<td>senior and policy</td>
</tr>
</tbody>
</table>

You can assign policy to a resource in a policy region from either the 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, select Managed Resources Policies from the Properties menu to display the Managed Resources Policies dialog:

   ![Managed Resources Policies dialog](image)

   The Managed Resources scrolling list displays the policy region’s managed resources.
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 option to change the resource’s default policy.

   **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 option to change the resource’s validation policy.

5. Select Validation Enabled to enable or disable 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 dialog.

   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.

**Command Line**

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

**Checking Policy in a Policy Region**

You can identify any policy region resources that do not conform to the region’s current policies.

If 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
Checking Policy in a Policy Region

validate resource properties automatically when a resource is moved to a different policy region. Therefore, the properties of a resource that has been moved to another policy region may not conform to the new region’s policies.

Also, if the validation policies of a policy region have been changed since a resource was created or last modified, the resource may not conform to the region’s current policies.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Checking policy in a policy region</td>
<td>Policy region</td>
<td>admin</td>
</tr>
</tbody>
</table>

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

**Desktop**

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

1. In the policy region, select **Check Policy** from the **Region** menu to display the **Check Policy** dialog:
2. Check policy on specific or all resource types.

   To check policy on a specific resource type in the policy region, make a selection from the Managed Resources scrolling list.

   To check policy on all policy region resource types in the policy region, select the All Members of the Policy Region option from the Source drop-down list.

3. Select where the results of the check policy operation are to be placed by using the Place Results in drop-down list. Valid options are Status Window, Collection, and Text File.

   **Status Window**
   
   Displays policy check results in a dialog.

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

   When you select Collection, the text box labeled Name is made sensitive. Enter the name of the collection into which the resource icons should be placed. If the collection does not already exist on the desktop, a new one is created.
Text File  
Writes the name of any resource that fails the policy validation to a file on a Tivoli client of your choosing.

When you select Text File, the Host and Name text boxes as well as the Browse button become active. Type the name of the managed node on which the file is to be created in the Host text box. Type the full path name for the file in the Name text box. 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, “Tivoli Scheduler” 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 policy region’s current policies, see the wchkpol command in the Tivoli Management Framework Reference Manual.
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

Tivoli Management Framework provides a centralized management point to control data distribution to groups of systems. You can develop prototypes, known as profiles, distribute these profiles across a network, and apply them to a diverse set of machines. In the Tivoli environment, a profile provides a container for application-specific information about a particular type of resource.

The profile feature is also scalable. Information stored in a central location is distributed to numerous locations. You can affect many machines and several system configurations with a minimal amount of time and effort.
Profile Item Locking

You can lock individual items in a profile database to control which configuration elements can be modified by subscribers at lower levels. Locked profile items are read-only when distributed to lower levels in the hierarchy. In addition, when locked items are distributed, they override any local profile modifications. You cannot lock individual properties within a profile item.

For example, if the profile item for user Hunter is locked, subscribers at lower levels in the hierarchy can view Hunter’s user properties but cannot change them.

You can perform profile item locking either when a profile is initially created and populated or at a later time. Each profile item in a database contains, in addition to its value, the Locked option, which is used by the profile manager during profile distribution. If this option is set, the profile item cannot be modified by any subscriber. In addition, when locked items are distributed, they always override any locally defined modifications.

Profile Policy Support

Each profile contains a set of default policies and validation policies. Default policies define default values used when creating new profile items. Validation policies define permissible values for profile items. Establishing or modifying policies requires the senior role.

Profile policies can be constant values or scripts. Profile policies are stored in the profile database and share the following features with other profile configuration information:

- Policies are propagated from a profile to its subscribers.
- Policies can be resolved or executed at the subscriber level.
- Local modifications to policies can be made at the subscriber level if you have the necessary authorization role.

Default and validation policies can be locked in the same manner as profile items. This enables you to define a profile policy so that the policy cannot be modified by a subscriber. As a result, a validation or default policy can be enforced throughout an installation.
If you have the required authorization role, you can modify a local profile policy and establish local rules for managing the systems you administer.

You can also disable policy validation on a profile. When validation is disabled, the validation policies are unchanged and remain stored in the profile database. However, the profile manager enforces these policies only if policy validation is enabled.

**Profile Default Policies**

The profile default record specifies the default values used when a new profile item is added. The default values are profile-specific. Refer to the appropriate Tivoli application guide for information about profile default values for specific Tivoli applications.

To edit profile default policies, you must have the *super* or *senior* role. You can define a default policy type for each profile item property. The defined policy can be one of the following types:

- **None**: No default value
- **Constant**: Default set as a constant
- **Script**: Default set by a script

**Profile Validation Policies**

Profiles can be validated to ensure that profile items comply with the current policy rules you have established. This ensures that lower levels in the hierarchy adhere to current policies.

The profile validation record specifies the validation policies used when a new profile item is added or an existing profile item is modified. To edit profile validation policies, you must have the *super* or *senior* role.

The defined validation policy can be one of the following types:

- **None**: No validation value
- **Constant**: Validation set as a constant
- **Script**: Validation set by a script

You can also set validation policies on individual properties of a particular profile item. These validation policies can be defined as a constant or as a script.
Profiles

For example, you can set a validation policy for the Accounting user profile. This validation policy might specify that all subscribers of this profile (for example, users in the Accounting department) have a home directory called /usr/home/user_name and that UNIX user IDs are between 4000 and 5000.

Profile Population

When you create a profile, it is only a definition of the information that each profile item includes. The profile items must then be populated with the actual data that defines the particular system configuration. You can populate a profile with the appropriate information from the current system configurations at the profile endpoints. For example, to populate a user profile, you can populate the profile items with users from one or more profile endpoints.

You specify which endpoints to retrieve the information from and whether this information should overwrite existing profile information or be appended to the profile.

The ability to populate profiles enables you to model existing configurations in the network when a profile-based application is first installed. Typically, you might choose one or more profile endpoints that most closely represent the desired configuration and then use these endpoints to populate the profiles. When the profiles have been populated from the current configurations, you can make any necessary modifications to the profiles to bring them closer to the desired configuration. These profiles can then be subscribed to by endpoints and distributed to subscribers.

For example, suppose your network serves three departments (Research, Grants, and Administration) and that each department has eight systems (R1 through R8, G1 through G8, and A1 through A8). You select the system from each department that most closely approximates the desired system configuration for that department (for example, R3, G7, and A2) and use those systems to populate the profiles for their respective departments. You then modify the resulting profiles to provide the desired system configuration for each department. Finally, you subscribe each system to the appropriate profiles and distribute the profiles to their endpoints.
If an environment contains a profile endpoint with thousands of resources (for example, a Network Information Services (NIS) user map with several thousand users), you should not create a single profile and populate it with thousands of items. Rather, you should determine a logical method for dividing the large number of resources into a subscription hierarchy. The advantage of creating such a hierarchy is that you can divide a large set of managed resources into smaller, more easily managed resource groups.

For example, if a system has several thousand users, you might divide them into groups based on department responsibilities. You can then create separate profiles for users in the Research department, the Grants department, the Administration department, and so on.

If you need to populate several profiles from a single large profile endpoint database, validation policies can be helpful. If validation is enabled on a profile that is being populated, the populate operation filters out any endpoint information that does not conform to the current validation policies. Tivoli notifies you of any endpoint information that does not conform to the current validation policies.

For example, if you want to include only users with user IDs between 300 and 800, you can specify this requirement in a validation policy and then enable validation. The profile population process incorporates only users with user IDs that meet the specified criteria. A list of any users that fail the validation process is displayed.

**Modifications to a Profile**

You can add items to a profile, modify the properties of existing profile items, and delete items from a profile.

Tivoli applications use profiles to specify application-specific templates. Each template includes information about the resources that can be managed by a Tivoli application. For example, the following Tivoli applications use profiles to manage specific resources:

- Tivoli Distributed Monitoring: a set of monitors
- Tivoli Software Distribution: a file package
- Tivoli User Administration: a user or group profile
Tivoli applications provide a profile-specific dialog that prompts you for the appropriate information. These dialogs differ for each profile type, but do contain elements common to all profile types.

When an add dialog is first displayed, only fields for which you are required to supply data are enabled. The application determines which fields you must supply data for, based on the current profile default policies. Any field with a default value is initially disabled.

You can enter the required data and then add the profile item immediately. The profile default policies are used to generate values for all fields having default values.

You can also access and modify fields that have default values after you have entered the required data for fields that do not have default values. The application uses the profile default policies to generate default values, displays the default values, and enables these previously disabled fields. You can accept the default values or modify them. You can then add the new profile item.

The modification of profile item properties and the deletion of profile items is also profile-specific. For information about adding profile items, modifying the properties of existing profile items, and deleting profile items from a profile, see the appropriate Tivoli application guide.

**Synchronizing Profiles and System Files**

If the system files and databases of a profile endpoint are changed directly without using Tivoli Management Framework, the profiles that the endpoint subscribes to may no longer accurately reflect the endpoint’s current configuration.

For example, suppose that the managed node **Galileo** subscribes to the user profile **Pisa**. You add new users **Juliet**, **Leonardo**, and **Louisa** to **Galileo**’s system configuration files, rather than adding them to the user profile. As a result, the user profile **Pisa** no longer accurately reflects the configuration of **Galileo**.

You can synchronize profiles so that they accurately reflect the current configurations of the profile endpoints that subscribe to the profiles. When you perform a synchronization, you specify the type of profile to be synchronized. All profiles of the specified type are synchronized to
their respective profile endpoints. You cannot synchronize an individual profile.

When you synchronize profiles, a list of differences between the profiles and the files and databases of their respective profile endpoints is displayed. Following are the types of differences:

- Profile items that exist in a profile database, but not in the profile endpoint’s files and databases
- Items that exist in a profile endpoint’s files and databases, but not in the profile database
- Items that differ between a profile endpoint’s files and databases and the profile database itself

After the list of differences is displayed, you can confirm the synchronization. Items in a profile database that do not exist in a profile endpoint’s files and databases are deleted from the profile database. For items that differ between a profile endpoint’s files and databases and the profile database itself, the profile database is modified to match the profile endpoint’s files and databases. For items that exist in a profile endpoint’s files and databases, but not in a profile database, you must choose which profile to add the items to. After the synchronization is completed, you can confirm any changes by viewing the profile items in the affected profiles. See “Synchronizing Profiles with a Profile Endpoint” on page 6-30 for information about how to synchronize profiles with profile endpoints.

### Sorting Profile Items

You can change the display sort order for profile items by specified criteria. Profile items are initially sorted by a profile-specific default key. Profile items can also be sorted by an arbitrary set of profile-specific keys that represent profile fields. The profile items are sorted in the order of the keys and may be sorted in ascending or descending order for each key.

For example, suppose the default sort key for user profiles is login name, sorted in ascending order. Instead of using the default sort key, you might sort the profile items by primary group ID and then alphabetically.
Profiles

by login name. In this case the sort key would be as follows:

1. Primary group ID, in ascending order
2. Login name, in ascending (alphabetical) order

As a result, the profile items would be sorted first by primary group ID, and then each resulting group would be sorted alphabetically by login name.

Note: Specifying the sort order for a profile affects only the order in which items are displayed. The items in a profile will always be written in application-specific order. Refer to the appropriate Tivoli application guide for details.

Common Profile Elements and Functions

Although profile content and functions are specific to a particular profile type, such as a user profile or a group profile, certain profile elements are common to all profile types. This section explains these common elements. For information about profile elements for a specific profile type, see the appropriate application guide.

All profiles contain the following information:

■ Profile type
■ Profile name
■ Profile records
■ Default policies
■ Validation policies
Profiles

Profile type Identifies the type of information the profile contains. For example, a user profile contains user default policies, user validation policies, and specific user information.

Profile name Specifies the profile icon label and is also displayed in profile-related dialogs.

Profile records Provide a managed node or other profile endpoint with profile-specific information, such as a list of users or groups. For example, a user profile contains information about specific users, which is used to configure managed nodes with users. You can then use this information to configure other managed nodes with the same set of users.

Default policies A set of values applied to a new profile item. For example, when a new user is created in a user profile, the default policies can be used to supply the user data.
Validation policies
Ensure that the profile records conform to the policies established in the policy region that contains the profile.

Profile View
You can view copies of profiles at all levels of the profile manager hierarchy. Lower-level profiles can contain records that have been locked at a higher level in the hierarchy. These profile records are read-only and cannot be edited.

The subscription hierarchy is displayed as a hierarchical view of the profile manager and all its subscribers. Each level of the hierarchy is indicated by an indentation. The greater the indentation of an item, the lower in the hierarchy the item is located.

- Profile Manager for General Admin
  - Profile Manager Office
    + Profile Manager Reception
    + NIS Domain Supply
  + Profile Manager Marketing
    Managed Node Finance

The first item displayed is the profile manager containing the original instance of the selected profile. In the preceding example, this is Profile Manager for General Admin. As you traverse the hierarchy, you can view profiles residing at different levels, as indicated by the indentation. Profile Manager for General Admin has three subscribers: Profile Manager Office, Profile Manager Marketing, and Managed Node Finance. In addition, Profile Manager Office has two subscribers: Profile Manager Reception and NIS Domain Supply.

You can navigate the hierarchy tree by expanding and collapsing the branches. A minus sign (-) in front of an item indicates that the item is expanded. For example, Profile Manager Office is expanded, and displays the next level of subscribers. A plus sign (+) indicates that the item is collapsed. Profile Manager Reception, NIS Domain Supply, and Profile Manager Marketing all have subscribers, but the view is collapsed, so their subscribers are not shown. An item with no symbol in front of it has no subscribers; for example, Managed Node Finance.
Profiles

Profile Properties Window

Every profile has a profile properties window that displays data associated with a specific profile, including default policy types and policy validation. You can view a profile at a specific subscription level and make and save changes to profile items.

Following is an example of a profile properties window. Depending on the applications you have installed, the window you see may look slightly different.

All profile properties windows contain the following areas:

- Profile properties menu bar
- Identification area
- Table area
- Status area

Profile Properties Menu Bar

The profile properties menu bar is a pull-down menu, located at the top of the profile dialog, that contains menu items for general profile operations, editing and viewing profiles, and help.
Identification Area

The identification area contains a profile name text box, a subscription path text box, and the name of the profile manager in which the profile resides.

The profile name text box displays the name of the profile; the profile name is also the profile icon label. You must have the super or senior role to enter new information or edit current profile names. The profile name can be changed in an original profile but not in subscription copies of a profile.

The subscription path text displays the subscription path of the profile copy you are viewing.

The identification area contains a button that enables you to view or edit a profile. You can select the original profile or any profile subordinate to it in the hierarchy. You must have the required authorization role to edit a profile. Without the required authorization role, you can only view the profile.

Table Area

The table area displays the data contained in each profile item. You can view, add, edit, or remove profile items in this area. The table area is similar for all profile types, but the actual information it contains is profile-specific.

If a local change to a profile has been made in the table area, a change bar is displayed to indicate the change. Changes do not affect actual system configuration files and databases until the profiles are distributed to profile endpoints.

If profile items are locked at a higher level in the hierarchy, a lock icon is displayed to indicate that changes cannot be made at the viewed level.

The buttons displayed at the bottom of the table area perform functions common to most profiles. These functions can also be accessed using the profile properties menu bar.

Status Area

The status area, at the bottom of the window, displays messages concerning the status of a selected operation. Abbreviated help text for menu items is also displayed in this area.
Profile Managers

Several profiles are required to describe the entire configuration of a managed node or other profile endpoint. Tivoli Management Framework provides profile managers to organize groups of profiles. Profile managers control the distribution of profiles to subscribers across an entire network or across a specified portion of a network.

You determine the mode in which a profile manager operates when you create the profile manager. You can change the mode by using the `wsetpm` command. See the Tivoli Management Framework Reference Manual for additional information.

Default Policies

Tivoli Management Framework uses both default and validation policies to control the operations of a profile manager. You can modify these policies to reflect your operational requirements. See the `wlspol`, `wgetpolm`, and `wputpolm` commands in the Tivoli Management Framework Reference Manual for procedures to modify policy. The following default policies are provided:

`pm_def_subscribers`

Provides a list of potential subscribers to a profile manager. The list provided by this policy is displayed in the Subscribers dialog. See “Subscribing to a Profile Manager” on page 6-19 for an example of this dialog.

`pm_def_profile_managers`

Provides a list of profile managers to which a profile can subscribe. See “Cloning Profiles from a Profile Manager” on page 6-34.
Profile Managers

Validation Policies

The following validation policies provided by Tivoli Management Framework govern profile manager subscription:

**pm_val_subscribers**

Used by a profile manager to validate potential subscribers

**pm_val_subscription**

Used by a profile manager or profile endpoint to validate potential subscribers

**pm_val_remove_subscribers**

Used by a profile manager to validate the removal of a subscriber

**pm_val_remove_subscription**

Used by a profile manager or profile endpoint to validate the removal of a subscription

For a successful subscription to a profile manager, both the profile manager being subscribed to and the subscribing profile manager or profile endpoint must conform to the required subscription validation policies (**pm_val_subscribers** and **pm_val_subscription**, respectively). For removal of a subscription, both the profile manager that is subscribed to and the subscribing profile manager or profile endpoint must conform to the subscription removal validation policies (**pm_val_remove_subscribers** and **pm_val_remove_subscription**, respectively).

For example, if you want to subscribe managed node Ed to profile manager Wilbur, managed node Ed must conform to the **pm_val_subscribers** validation policies of profile manager Wilbur, and profile manager Wilbur must conform to the **pm_val_subscription** validation policies of managed node Ed.

For information about the profile manager policies, see **pm_val_subscribers**, **pm_val_subscription**, **pm_val_remove_subscribers**, and **pm_val_remove_subscription** in the *Tivoli Management Framework Reference Manual*. 
Data Preservation During Distribution

You can specify whether a distribution will replace or preserve local data. The following two selections can be accessed on the Distribute Profiles dialog:

- **Preserve Modifications**: Any local modifications made to subscribers are retained.
- **Make Exact Copy**: Subscriber profile records are completely replaced by the source profile records, creating a subscriber database identical to the source.

**Note**: Exercise caution when using **Make Exact Copy**. Important information may be lost in lower levels of the hierarchy.

Distribution Levels

You can specify one of two distribution levels, which can be accessed on the Distribute Profiles dialog:

- **Next Level of Subscribers**: Copies of the profiles are distributed only to immediate subscribers (that is, subscribers that are one level lower in the hierarchy).
- **All Levels of Subscribers**: Copies of the profiles are distributed recursively down the hierarchy to all profile endpoints.

Profile managers and profile endpoints can reside at multiple levels in the distribution hierarchy. If you select **Next Level of Subscribers**, the distribution process affects only the next lower level in the hierarchy. You must perform the distribution process from profile managers residing at more than one level to reach all the profile endpoints. Also, if you perform a distribution from a profile manager to a profile endpoint using **Next Level of Subscribers**, only the profile endpoint database is updated; the actual system files are not updated. You can then make any necessary local modifications in the profile endpoint. You must perform a distribution from the profile endpoint to affect the actual system files and databases.

In the following example, profile manager A has two subscribers, managed node Tom and profile manager B, and profile manager B has one subscriber, managed node Ming.
If you select **All Levels of Subscribers**, profile manager A distributes profile copies to managed node Tom, profile manager B, and managed node Ming.

If you select **Next Level of Subscribers**, profile manager A distributes profile copies only to profile manager B and managed node Tom. Managed node Ming, residing one level below profile manager B, does not receive the profile copies. For managed node Ming to receive the profile copies, the distribution must also be performed from profile manager B.

**Recipient-based Profile Distribution**

Getting a new copy of a profile is similar to distributing a profile except that the recipient, not the sender, requests the distribution. When you get a new copy of a profile, a copy is distributed from the appropriate profile manager located one level higher in the hierarchy.
For example, profile manager C subscribes to profile manager A and profile manager B. Profile manager A distributes profiles P1, P2, and P3 to profile manager C, and profile manager B distributes profiles P4, P5, and P6 to profile manager C. If profile manager C performs a get new copy operation for profile P1, profile P1 is distributed from profile manager A. If profile manager C performs a get new copy operation for profile P4, profile P4 is distributed from profile manager B.

Creating a Profile Manager

You can create a profile manager within a policy region. After a set of profile managers is defined, you can delegate system management tasks to administrators with roles of super, senior, and admin.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a profile manager</td>
<td>Policy region</td>
<td>senior</td>
</tr>
</tbody>
</table>

You can create a profile manager from either the desktop or the command line.
Creating a Profile Manager

Desktop

To create a profile manager from a policy region view, perform the following steps:

1. From the Create menu, select Profile Manager to display the Create Profile Manager dialog.

   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 “Changing Managed Resource Types” on page 5-7 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 will distribute to Tivoli endpoints. If Dataless Endpoint Mode is selected, the profile manager can distribute to Tivoli 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 Tivoli endpoints.

4. Click Create & Close to create the profile manager and return to the policy region window. The new profile manager’s icon is displayed in the policy region view.
Subscribing to a Profile Manager

Command Line

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

Subscribing to a Profile Manager

Subscribing profile managers or endpoints 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 tasks, while delegating other tasks 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 profile manager or profile endpoint must conform to the necessary subscription validation policies.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscribing to a profile manager</td>
<td>Profile manager</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can add subscribers to a profile manager using drag and drop, from the desktop or from the command line.
Subscribing to a Profile Manager

**Desktop, Drag and Drop**

To subscribe a profile manager or profile endpoint to a profile manager, perform the following steps:

1. Select the icon of the profile manager or profile endpoint that you want to subscribe to a profile manager. These icons can be found on the desktop.
2. Drag the selected icon to the icon or profile manager subscriber area of the profile manager you want to subscribe to.
3. Drop the icon. The selected profile manager or profile endpoint is subscribed to the profile manager.

**Desktop**

To subscribe a profile manager or profile endpoint to a profile manager, perform the following steps:

1. Select **Subscribers** from the pop-up menu of the icon for the profile manager to which you want to subscribe. The **Subscribers** dialog is displayed:
Subscribing to a Profile Manager

A list of all profile managers and profile endpoints that can subscribe to the current profile manager is displayed in the **Available to become Subscribers** scrolling list.

You can add or remove available subscribers by modifying the **pm_def_subscribers** default policy. See the *Tivoli Management Framework Reference Manual* for instructions on how to edit policies.

2. Select one or more profile managers or profile endpoints in the **Available to become Subscribers** scrolling list, and click the left-arrow button. The selected profile managers and profile endpoints are moved from the **Available to become Subscribers** scrolling list to the **Current Subscribers** scrolling list.

You can also double-click an entry in the **Available to become Subscribers** scrolling list to move it automatically to the **Current Subscribers** scrolling list.

![Subscribers screenshot]

**Note:** The selected subscribers are moved to the **Current Subscribers** scrolling list but are not actually added to the profile manager subscription list until you click the **Set Subscriptions** button.

3. Click **Set Subscriptions & Close** to update the subscribers to the profile manager and return to the policy region window.
Removing a Subscriber from a Profile Manager

**Note:** You can subscribe and unsubscribe one or more profile managers and profile endpoints in a single operation by moving entries to or from the appropriate scrolling list before clicking **Set Subscriptions & Close**. See “Removing a Subscriber from a Profile Manager” on page 6-22 for information about how to remove a profile manager subscription.

**Command Line**

For information about using the command line to subscribe a profile manager or profile endpoint to a profile manager, see the `wsub` command in the *Tivoli Management Framework Reference Manual*.

**Removing a Subscriber from a Profile Manager**

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 profile manager or profile endpoint 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removing a subscription to a profile manager</td>
<td>Profile manager</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can remove a subscriber from either the desktop or the command line.
Desktop

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

1. Select Subscribers from the pop-up menu of the profile manager icon from which you want to remove subscribers. The Subscribers dialog is displayed:

   ![Subscribers dialog](image)

   The Current Subscribers scrolling list displays a list of all profile managers and profile endpoints that subscribe to the current profile manager.

   You can add or remove available subscribers by modifying the pm_def_subscribers default policy. See the Tivoli Management Framework Planning for Deployment Guide for instructions on how to edit default policies.

2. Select one or more profile managers or profile endpoints in the Current Subscribers scrolling list, and click the right-arrow button. The selected profile managers and profile endpoints are moved from the Current Subscribers scrolling list to the Available to become Subscribers scrolling list.

   You can also double-click an entry in the Current Subscribers scrolling list to move it automatically to the Available to become Subscribers scrolling list.
Removing a Subscriber from a Profile Manager

Note: The selected subscribers are moved to the Available to become Subscribers scrolling list, but they are not actually removed from the profile manager subscription list until you click Set Subscriptions & Close.

3. Click Set Subscriptions & Close to initiate the removal of the selected subscribers from the profile manager. The Unsubscribe Subscribers dialog is displayed:

![Unsubscribe Subscribers dialog](image)

   a. Keep or delete profile copies.

      Select Keep all profile copies if you do not want to delete 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 any trace 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 endpoint.

   b. Click Unsubscribe to remove the subscribers and return to the Subscribers dialog.

Command Line

For information about using the command line to remove a subscription to a profile manager, see the wunsub command in the 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing a profile manager</td>
<td>Policy region</td>
<td>senior</td>
</tr>
</tbody>
</table>

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

Desktop

To edit a profile manager from a policy region, perform the following steps:

1. Double-click the profile manager icon to open the Profile Manager window.
2. From the Edit menu, select Profile Manager to display the Edit Profile Manager dialog:
Deleting a Profile Manager

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 Tivoli 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 Tivoli 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 the 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 “Removing a Subscriber from a Profile Manager” on page 6-22 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.

Desktop

To delete a profile manager, perform the following steps:

1. From a policy region, select the profile manager you want to delete.

2. From the Edit menu, select the Delete option.
Creating Profiles

You can create a profile from a profile manager.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating profiles from a profile manager</td>
<td>Profile manager</td>
<td>senior</td>
</tr>
</tbody>
</table>

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

Desktop

To create a profile from a profile manager window, perform the following steps:

1. Double-click the profile manager icon to open the Profile Manager window.
2. From the Create menu, select the Profile option to display the Create Profile dialog:
Creating Profiles

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 to be created.

   **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 “Changing Managed Resource Types” on page 5-7 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 the *Tivoli Management Framework Reference Manual*. 
Distributing Profiles from a Profile Manager

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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributing profiles</td>
<td>Profile manager</td>
<td>admin</td>
</tr>
<tr>
<td>from a profile manager</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

**Desktop, Drag and Drop**

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

1. Select the icon of the profile that you want to distribute.
2. Drag the icon to the profile manager or profile endpoint to which you want to distribute the profile. The profile manager or profile endpoint must already be subscribed to the profile.
3. Drop the icon. The selected profile is distributed to the profile manager or profile endpoint using the default distribution parameters.

**Desktop**

To distribute profiles from a profile manager window using default distribution parameters, perform the following steps:

1. Double-click the profile manager icon to open the Profile Manager window.
2. Select one or more profile icons.
3. Select one or more subscriber icons.
4. From the Profile Manager menu, select Distribute to display the Distribute Profiles dialog:

![Distribute Profiles dialog]

5. Distribute or schedule the distribution of profiles.
   Click Distribute Now to distribute the profiles to the selected subscribers immediately.
   Click Schedule to schedule a distribution of the profiles for a later time. For information about how to schedule a job, see Chapter 10, “Tivoli Scheduler.”

**Command Line**

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

**Synchronizing Profiles with a Profile Endpoint**

A profile may not always match the current system files and databases on a particular managed node or other profile endpoint. 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 profile endpoint so that the profiles accurately reflect the profile endpoint’s current configuration.
Synchronizing Profiles with a Profile Endpoint

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synchronizing profiles with a profile endpoint</td>
<td>Policy region</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can synchronize profiles with the profile endpoint from either the desktop or the command line.

**Desktop**

To synchronize profiles with a profile endpoint’s current system files and databases, perform the following steps:

1. In the policy region, select the Synchronize option from the Managed Node menu to display the Synchronize Profiles dialog:

2. Select the type of profile you want to synchronize from the Available Profile Types scrolling list. The contents of this list will be different depending on the applications you have installed in the Tivoli management region. You can only synchronize one type of profile at a time.
3. Click **Synchronize**. The **Profile/System Discrepancies** dialog is displayed. This dialog and its contents will be different depending on the profile type selected in the previous step.

The **Profile/System Discrepancies** dialog displays three types of differences between profiles and profile endpoint files and databases:

- Profile items that exist in a profile database, but not in the profile endpoint’s files and database
- Items that exist in the profile endpoint’s files and databases, but not in a profile database
- Items that differ between the profile endpoint’s files and databases and the profile database itself

4. Click **Commit Changes** to synchronize the profile databases with the profile endpoint’s files and databases. Items in a profile database that do not exist in the profile endpoint’s files and databases are deleted from the profile database. For items that differ between the profile endpoint’s files and databases and the profile database itself, the profile database is modified to match the profile endpoint’s files and databases. For items that exist in the profile endpoint’s files and databases but not in a profile database, you must choose the profile to which to add the items.

5. Click the **Cancel** button to close the **Synchronize Profiles** dialog.
Copying Profiles from a Profile Manager

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

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copying profiles from a profile manager</td>
<td>Profile manager</td>
<td>senior</td>
</tr>
</tbody>
</table>

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

Desktop, 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. You should change this name to something meaningful by using the profile properties window.
Cloning Profiles from a 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 desktop only.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloning profiles from a profile manager</td>
<td>Profile manager</td>
<td>admin</td>
</tr>
</tbody>
</table>

Desktop

To clone profiles from a profile manager, perform the following steps:

1. Double-click the profile manager icon to open the Profile Manager window.
2. Select a profile icon.
3. Select Profiles → Clone from the Edit menu to display the Clone Profile dialog:
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’s icon is displayed in the Profile Manager window.

### Moving Profiles from a Profile Manager

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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Moving profiles from a profile manager</td>
<td>Profile manager</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can move profiles from the 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).
Deleting Profiles from a 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 databases at the profile endpoints.

Exercise caution when deleting profiles. Deleting a profile can cause problems throughout the distribution hierarchy. For example, if you delete a user profile from profile manager A, any subsequent distributions from profile manager A will not contain the deleted user profile. Thus, you will no longer be able to use the deleted user profile to update user information from profile manager A.

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 a profile endpoint’s files or databases, 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 that correspond to current information in a profile endpoint’s files or databases.
Deleting Profiles from a Profile Manager

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleting profiles from a profile manager</td>
<td>Profile manager</td>
<td>admin</td>
</tr>
</tbody>
</table>

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

**Desktop**

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

1. Double-click the profile manager icon to open the **Profile Manager** window.
2. Select one or more profile icons.
3. From the **Edit** menu, select **Profiles → Delete** to display the **Delete Profiles** dialog:

   ![Delete Profiles dialog](image)

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 the **Tivoli Management Framework Reference Manual**.

Tivoli Management Framework User's Guide 6–37
Query Facility

The Tivoli Management Framework *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). Some of the Tivoli applications that store information in a RIM repository are Tivoli Enterprise Console®, Tivoli Inventory, and Tivoli Software Distribution. The database in which the Tivoli Enterprise Console product stores its events is called the *event repository*, and the database in which Tivoli Inventory and Tivoli Software Distribution store information is called the *configuration repository*. See the appropriate application guide for more information about each repository.

The query feature consists of query libraries and queries. *Query libraries* reside in policy regions and are created to contain queries. *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 Tivoli 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...
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. 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 Tivoli Software Distribution file packages. Each query and query library in the Tivoli management region must have a unique name.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a query library</td>
<td>Policy region</td>
<td>senior or super</td>
</tr>
</tbody>
</table>

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

Desktop

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

1. Select the policy region in which you want to create the query library, and add the Query Library resource to the policy region’s list of managed resources.

   For instructions on adding resource types to a policy region, see “Changing Managed Resource Types” on page 5-7.
2. From the policy region, select QueryLibrary from the Create menu. The Create Query Library dialog is displayed:

3. In the Name/Icon Label text box, type a unique name for the query library in the Name/Icon Label text box.

4. Click Create & Close. Tivoli Management Framework creates the query library and returns to the Policy Region window. The policy region now contains an icon for the new query library:
Creating a Query

**Command Line**

To use the command line to create a query library, enter the following command:

```
wcrtqlib "Software Distribution" FilePack_Subscribers
```

where:

- **“Software Distribution”**
  - Specifies **Software Distribution** as the policy region where the query library will reside

- **FilePack_Subscribers**
  - Specifies **FilePack_Subscribers** as the name of the new query library

For information about **wcrtqlib**, 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 and is populated by Tivoli Inventory and Tivoli Software Distribution. For more information about the data stored in each repository, see the appropriate Tivoli application manual.

The **Create Query** dialog 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 management 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, that determines which columns you can 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 which information the query will return.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a query</td>
<td>Query library</td>
<td>senior or super</td>
</tr>
</tbody>
</table>

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

**Desktop**

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

1. From the policy region, double-click the icon of the query library in which the query will reside. The query library window is displayed.
2. From the Create menu, select Query. The Create Query dialog is displayed:
3. In the **Query Name** text box, type a unique name for the query. 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 text box is optional.
5. From the **Repository** drop-down list, which lists the names of the RIM objects in the local Tivoli management region, select a RIM repository against which the query will run. A RIM object is installed with each Tivoli application that uses a RIM repository. To access the configuration repository, select **inventory**.

6. Either type or select a table or view name.

Type the name of a table or view and click **Set** in the **Table/View Name** text box.

To select from a list of views in the repository, 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 text boxes on the dialog, including the **Chosen Columns**, **Where Clause**, and **Additional Clauses** scrolling lists.

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

7. In the **Available Columns** scrolling list, select the columns from which you want to retrieve information and click the left-arrow button to move them to the **Chosen Columns** scrolling list. Include the TIVOLI_OBJECT_ID item in the **Chosen Columns** scrolling list if you plan to use the query to select subscribers or targets.
Creating a Query

The available columns are determined by the table or view specified in the Table/View Name text box. Click the Table Description button to view the Table Description dialog:

![Table Description dialog]

Click Close to return to the Create Query dialog.

8. 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 either 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.

For example, you can make the names of software products in the query results all uppercase by changing the SOFTWARE_ID column to UPPER(SOFTWARE_ID).

9. Create a SQL search clause in the Where Clause scrolling 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. Complete the following steps:
   a. Either 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.
Creating a Query

To display the list of **Chosen Columns**, click the ellipses (…) button, and then 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. For example, the following where clause returns all rows in the repository that list AIX, Solaris, or HP_UX as values for `BOOTED_OS_NAME`.

  ```sql
  where BOOTED_OS_NAME IN ('AIX', 'Solaris', 'HP_UX')
  ```

- **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. For example, the following where clause returns information associated with configuration files that have the `.BAT` file extension.

  ```sql
  where CONFIG_FILE_NAME LIKE '*.BAT'
  ```

c. Either type or select the search criteria.

Type one or more values that complete the search criteria in the **Column Value** text box.
Creating a Query

To 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 %.

d. Click **Add** to add the criteria to the **Where Clause** scrolling list.

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

f. To build a compound query, select either **and** or **or** and repeat steps a–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, and 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**.

10. 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.

11. Click **Create & Close** to return to the query library window.

Command Line

Use **wcrquery** to create a query. Before you create a query, you must create a query library in which the query can reside. For more information, see “Creating a Query Library” on page 7-2.

To create the **Win–machines** query that finds processor information for all machines running Windows, enter the following command:

```
wcrtquery -d "Find processor info for Windows machines"
-r inventory -v PROCESSOR_TYPE -c PROCESSOR_ID
-w "(BOOTED OS_NAME LIKE 'Windows%')" NewQueries Win–machines
```
where:

–d “Find processor info for Windows machines”
  Specifies a description of the query

–r inventory
  Specifies the configuration repository as the RIM repository to query

–v PROCESSOR_TYPE
  Specifies PROCESSOR_TYPE as the view in the configuration repository from which to retrieve information

–c PROCESSOR_ID
  Specifies PROCESSOR_ID as the column in the view from which to retrieve information

–w “(BOOTED_OS_NAME LIKE ‘Windows%’)”
  Defines a search clause that returns PROCESSOR_ID for all machines in the PROCESSOR_TYPE view that include Windows in the BOOTED_OS_NAME column

NewQueries
  Specifies NewQueries as the name of the query library in which the query will reside

Win–machines
  Specifies Win–machines as the name of the new query

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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing a query</td>
<td>Policy region</td>
<td>senior, super, or Query_edit</td>
</tr>
</tbody>
</table>

You can edit a query from either the desktop or the command line.
**Desktop**

To edit a query from the desktop, perform the following steps:

1. Either right-click or double-click the query icon.

   Right-click the icon of the query you want to change in a query library, and then select **Edit Query** from the pop-up menu.

   Alternatively, double-click the query icon. The **Edit Query** dialog is displayed. This dialog is the same as the **Create Query** dialog.
2. Change the Repository, Table/View Name, Chosen Columns, Where Clause, Column Name, Column Value, or Additional Clauses field as necessary. (See “Creating a Query” on page 7-4 for an explanation of the fields on this dialog.)

3. Click Save & Close to save the changes.

Command Line

To modify an existing query, use wgetquery to list the properties of a query, and then use wsetquery to change the properties.

For example, to list information about the Available RAM query, enter the following command:

```
wgetquery -f "Available RAM"
```

where:

- **-f** Provides a full listing of the query information. If you do not specify this option, only the where clause is listed.

“Available RAM”

Specifies Available RAM as the query for which to list information.

This wgetquery command returns the following output:

```
Name: Available RAM
Description: Returns machines with 8MB of RAM
Repository: inventory
View: INVENTORYDATA
Columns:
   TIVOLI_OBJECT_ID
   TIVOLI_OBJECT_LABEL

Where Clause:
------------------------
(PHYSICAL_MEMORY_KB = '8000')
```

Use wsetquery to edit a query. To use wsetquery to change the view, columns, and where clause for the Available RAM query, enter the following command:

```
wsetquery -d "Returns machines with 16MB of RAM" 
-v MEMORY_VIEW -c HARDWARE_SYSTEM_ID 
-c PAGING_SPACE_RK 
-w "(PHYSICAL_MEMORY_KB = '16000')" "Available RAM"
```
Using Queries

where:

–d “Returns machines”
    Specifies a new description for the query

–v MEMORY_VIEW
    Specifies MEMORY_VIEW as the new view from which to retrieve information

–c HARDWARE_SYSTEM_ID
    Specifies HARDWARE_SYSTEM_ID and PAGING_SPACE_ID as the new columns from which to retrieve information

–w “(PHYSICAL_MEMORY_KB = ‘16000’)”
    Replaces the old where clause so that the query searches for machines with 16 MB of RAM instead of 8 MB

“Available RAM”
    Specifies Available RAM as the query to be modified

See the Tivoli Management Framework Reference Manual for more information about the wgetquery and wsetquery commands.

Using Queries

After you create or edit a query, you can run the query to access information in a repository. The query facility has three major functions.

The main function of the query facility is to access information in a RIM repository. You can run a query to access general information in a RIM repository and either display the query results or save the results in a file. For example, you might want to query the event repository for certain types of Tivoli Enterprise Console events and save the results in a file.

To run any query and display or save the results, perform one of the following actions:

■ Run wrunquery.
■ Click Run Query on the Edit Query dialog.
■ Click Run Query on the Create Query dialog.
Using Queries

- Right-click the icon of the query and select Run Query.

See “Running a Query” on page 7-15 for more information.

The second function of the query facility is to use the information in the configuration repository to select subscribers or targets for a Tivoli profile distribution. A query can determine which machines meet certain criteria and then add those machines to a list of distribution targets. To use the query facility to select subscribers, perform one of the following actions:

- Run `wruninvquery`.

- Click Query from one of the following dialogs:
  - Tivoli Management Framework Subscribers dialog
  - Tivoli Inventory Inventory Profile dialog
  - Tivoli Software Distribution Distribute File Package, Remove File Package, Distribute AutoPack, or Remove AutoPack dialog

If you run a query from one of these dialogs, the query must include the TIVOLI_OBJECT_ID and TIVOLI_OBJECT_LABEL columns in the Chosen Columns list.

See “Defining Subscribers and Targets” on page 7-18 for instructions about selecting subscribers with the query facility.

The third function of the query facility is to view Tivoli Inventory information about a particular machine in your Tivoli environment. When you run a query from the managed node’s icon menu, the query results for only that machine are displayed. To access a query library by right-clicking a managed node’s icon, you must first have the Query_execute and Query_edit authorization roles in the policy region where the query library resides. See the Tivoli Inventory User’s Guide for more information.

**Running a Query**

You can run a query and view the results or save them in a file.
Using Queries

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running a query</td>
<td>Policy region</td>
<td>senior, super, Query_edit, or Query_execute</td>
</tr>
</tbody>
</table>

You can run a query from either the desktop or the command line.

**Desktop**

To run a query from the desktop, perform the following steps:

1. Either right-click the icon or select **Run Query**.

   Right-click the icon of a query in a query library, and then select **Run Query** from the pop-up menu.

   Alternatively, select **Run Query** from either the **Create Query** or **Edit Query** dialog.

   The **Run Query** dialog is displayed, showing the results of the query in tabular form:
2. If you want to save the results of the query, you can do so from the 
Run Query dialog as follows:
   a. In the Run Query dialog, click the Export button. The 
      Export Query Results dialog is displayed:

   b. In the Host text box, type the name of the managed node on 
      which you would like to save the results file. If you do not 
      specify a managed node, the file will be saved on the local 
      machine.

   c. In the File text box, type the location and name of the query 
      results file.

      If you do not know the location and name of the query results 
      file, click the ellipses (…) button to browse the file system.

   d. Click one of the Delimiter radio buttons to 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 immediately to the right of it.

   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.
Using Queries

Command Line

You can use\texttt{wrunquery} to run a query and either display the results to standard output or save the results in a file. The \texttt{wrunquery} command can be used with any query. To use \texttt{wrunquery} to run the \texttt{Win-machines} query and save the results in a file, enter the following command:

\begin{verbatim}
wrunquery -n -h amon -f /tmp/query.txt -d ";" Win-machines
\end{verbatim}

where:

\begin{enumerate}
\item \texttt{-n} Omits headers from the results file
\item \texttt{-h amon} Specifies \texttt{amon} as the name of the managed node on which to store the file
\item \texttt{-f /tmp/query.txt} Specifies \texttt{/tmp/query.txt} as the location and name of the query results file
\item \texttt{-d ";"} Specifies a semicolon as the delimiter
\end{enumerate}

\texttt{Win-machines} Specifies the name of the query to be run

See the \textit{Tivoli Management Framework Reference Manual} for more information about \texttt{wrunquery}.

Defining Subscribers and Targets

You can query a repository to select subscribers or targets for a Tivoli profile distribution. When you run the query, it selects the list of the clients in the policy region that meet the query criteria. A query that you use to select subscribers and targets must include the TIVOLI OBJECT ID and TIVOLI OBJECT LABEL columns in the \textit{Chosen Columns} list. (See “Creating a Query” on page 7-4 for more information about the \textit{Chosen Columns} list.) Use the procedure in this section to run a query from any of the following dialogs:

\begin{itemize}
\item Tivoli Management Framework Subscribers — Select subscribers for a profile manager
\item Tivoli Inventory Profile — Select targets for a Tivoli Inventory profile distribution
\end{itemize}
Using Queries

- **Distribute File Package** and **Distribute AutoPack** — Select subscribers for a file package or an AutoPack distribution
- **Remove File Package** and **Remove AutoPack** — Select subscribers from which to remove a file package or an AutoPack profile

The following table provides the contexts and authorization roles required to perform these tasks:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adding subscribers to a profile manager</td>
<td>Profile manager</td>
<td>senior or super</td>
</tr>
<tr>
<td>Selecting targets for a Tivoli Inventory profile distribution</td>
<td>Inventory profile</td>
<td>senior or super</td>
</tr>
<tr>
<td>Selecting subscribers for distribution or removal of a file package</td>
<td>File package</td>
<td>admin, senior, or super</td>
</tr>
<tr>
<td>Selecting subscribers for distribution or removal of an AutoPack</td>
<td>AutoPack profile</td>
<td>admin, senior, or super</td>
</tr>
</tbody>
</table>

You can select subscribers from either the desktop or the command line.

**Desktop**

To run a query from the **Subscribers** dialog, perform the following steps:

1. From a **Profile Manager** window, select **Subscribers** from the **Profile Manager** menu. The **Subscribers** dialog is displayed:
2. Click the **Query** button to display the **Execute a Query** dialog:

3. In the **Query Libraries** scrolling list, double-click the query library that contains the query you want to run. The **Query Libraries** scrolling list displays all query libraries in the policy region. The query library you select populates the **Queries** scrolling list.

4. In the **Queries** scrolling list, select a query.
5. Click **Execute**. The query moves the subscribers in the policy region that meet the query criteria to the **Current Subscribers** scrolling list.

---

**Command Line**

The *wruninvquery* command runs a query and returns the results in an Interface Definition Language (IDL) format that you can use with scripts to populate subscription lists. A query that you run with this command must include both the TIVOLI_OBJECT_ID and TIVOLI_OBJECT_LABEL columns. In contrast, *wrunquery* can be used with any query, and the results are sent to standard output or to a file.

To run the **Win–machines** query, enter the following command:

```
wruninvquery -l Win–machines
```

where:

- `-l` Lists the names of the machines that match the query criteria, instead of their object IDs

**Win–machines** Specifies **Win–machines** as the query to run

See the *Tivoli Management Framework Reference Manual* for more information about the *wruninvquery* command.
Notification

You receive notices on your bulletin board by subscribing to a notice group. (See Chapter 3, “Tivoli Administrators” for instructions on subscribing to notice groups.) A bulletin board icon is displayed on each administrator’s desktop.

Initially, no notices are in the Tivoli system and the bulletin board is empty:

When new notices arrive, the bulletin board icon changes to indicate that the bulletin board now contains unread messages:

A notice is assigned the following attributes when posted:

- Unique ID
- Severity level
- Date and time stamp
- Administrator name
- Summary of the notice contents
When you view notices, you can sort or filter them by their severity or the name of the administrator who performed the management operation that caused the notice to be generated. Any sorting or filtering option you enable is disabled when you close the bulletin board; you must enable any desired sorting or filtering option each time you view your bulletin board.

Notices accumulate until you delete them or they expire. The default notice expiration is 168 hours (1 week); notices are automatically deleted 168 hours after they are posted, even if they have not been read. If you have the *senior* role, you can use `wexpnotif` to set notice expiration for a notice group; however, you cannot set notice expiration for an individual administrator.

### Reading Notices

You read a notice by choosing it from a table listing the 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.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reading notices</td>
<td>Tivoli desktop</td>
<td><code>user</code></td>
</tr>
</tbody>
</table>

You can read notices from either the desktop or the command line.

### Desktop

To read notices, perform the following steps:

1. Double-click the bulletin board icon to display the *Read Notices* dialog:
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 selecting another notice group after opening the first.
a. Double-click a notice header in the scrolling list to populate the **Notice Group Messages** window:

![Notice Group Messages window]

b. If multiple notices for the notice group are unread, you can select one or more notice headers and click **View Message** to read them.

c. After you have finished reading the notices, click **Close**. The **Notice Message Viewer** dialog is closed and the **Notice Group Messages** window is displayed.

3. Click **Close** to close the **Notice Group Messages** window, click **Update** to refresh the list of unread notices, or click **Catch Up** to mark all notices as read.
Saving Notices

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. Note that you must have an account on the machine on which the file is saved.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saving notices</td>
<td>Tivoli desktop</td>
<td>user</td>
</tr>
</tbody>
</table>

You can save a notice to a text file from either the desktop or the command line.

Desktop

To save notices to a text file, perform the following steps:

1. Double-click the bulletin board icon to display the Read Notices dialog:
2. Double-click a notice header in the scrolling list to display the **Notice Group Messages** window:

3. Select the notice you want to save from the notice headers scrolling list.
4. Click Save. The **File Browser** dialog is displayed:

![File Browser dialog](image)

a. Select the host on which the file is to be saved.
b. Use the **Directories** and **Files** scrolling lists to set the directory and file names.
c. Click **Set File & Close** to save the selected notices to the specified file and return to the **Notice Group Messages** window.

5. Click **Close** to close the **Notice Group Messages** window.

**Command Line**

Save notices to a text file by redirecting the output of `wlsnotif`. For more information about `wlsnotif`, see the *Tivoli Management Framework Reference Manual*. 
Forwarding Notices

You can forward a notice to one or more users with electronic mail. 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Forwarding notices</td>
<td>Tivoli desktop</td>
<td>user</td>
</tr>
</tbody>
</table>

You can forward a notice to an e-mail alias from either the desktop or the command line.

Desktop

To forward notices, perform the following steps:

1. Double-click the bulletin board icon to display the Read Notices dialog.
2. Double-click a notice group in the scrolling list to display the **Notice Group Messages** window.

3. Select the notice you want to forward from the notice headers scrolling list.
4. Click **Forward** to display the **Forward Notice** dialog:

   ![Forward Notice dialog](image)

   a. Specify the e-mail address of the message recipient in the **Send To** text box.

   b. Specify the subject of the e-mail message in the **Subject** text box.

   c. Optionally, edit the text displayed in the **Message** area.

   d. Click **Send** to send the mail message to the e-mail addresses listed and return to the **Notice Group Messages** window.

5. Click **Close** to close the **Notice Group Messages** window.

### Command Line

Forward notices by piping the output of `wlsnotif` to a mail utility, such as `Mail` or `mailx`. For more information about `wlsnotif`, see the *Tivoli Management Framework Reference Manual*. 
Marking Notices as Read and Unread

After you have finished with a notice, it is automatically marked as read on 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 read a notice or mark it as read, it does not appear 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marking notices as read or unread</td>
<td>Tivoli desktop</td>
<td>user</td>
</tr>
</tbody>
</table>

You can mark a notice as read or unread from the desktop only.

1. To mark a notice as read in a notice group, perform the following steps:
   a. Double-click the Bulletin Board icon to display the Read Notices dialog:
b. Double-click a notice group in the scrolling list to display the **Notice Group Messages** window:

![Notice Group Messages window]

<table>
<thead>
<tr>
<th>Notice Id</th>
<th>Severity</th>
<th>Administrator</th>
<th>DateTime</th>
<th>Subject</th>
</tr>
</thead>
</table>

- **Next Unread**
- **Next Read**
- **Mail Read**
- **Mail Unread**
- **Select All**
- **Send Print**
- **View Message**

Notices of 3
Date: Sun Apr 20 09:58:1995
Policy: Notice
Administrator: root@vermom

A successful TIME database backup was performed.
A snapshot of the databases for the following managed nodes has been
collected:
"node name"
"node name"
"node name"

If the archive media is a disk, it should be saved in safe storage
as part of a regularly scheduled backup procedure for the system.

c. Select the notice or notices you want to mark as read in the **Notice Group Messages** window.

d. Click **Mark Read** to mark the selected notices as read. The **Notice Group Messages** window remains open.

2. To mark a notice as unread in a notice group, perform the following steps:

a. Select the notice or notices you want to mark as unread in the **Notice Group Messages** window.

b. Click **Mark Unread** to mark the selected notices as unread. The **Notice Group Messages** window remains open.
3. 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.

4. Otherwise, click **Close** to close the **Notice Group Messages** window.

**Sorting Notices**

You can specify how the notices displayed in the **Notice Group Messages** dialog are sorted.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sorting notices</td>
<td>Tivoli desktop</td>
<td>user</td>
</tr>
</tbody>
</table>

You can sort notices from the desktop only.

To sort notices, perform the following steps:

1. Double-click the bulletin board icon to display the **Read Notices** dialog:
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 dialog:

![Sort Notices dialog]

- 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 from the Severities scrolling list and click the left-arrow button to move the property to the Sort By scrolling list.
- 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.
- 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 messages in the Notice Group Messages window by filtering the messages. For example, you may want to 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filtering notices</td>
<td>Tivoli desktop</td>
<td>user</td>
</tr>
</tbody>
</table>

You can filter notices from the desktop only.

To filter notices, perform the following steps:

1. Double-click the bulletin board icon to display the Read Notices dialog:
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 dialog:

![Filter Notices dialog](image)

Each administrator who has 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, select the administrator and click the right-arrow button to move the entry to the Available Administrators scrolling list.

b. Select one or more severity levels from the Severity list 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.

4. 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 messages relate to some specific operation and you want to group them as a single message in the notice headers scrolling list.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Combining notices</td>
<td>Tivoli desktop</td>
<td>user</td>
</tr>
</tbody>
</table>

You can combine notices from the desktop only.

To combine notices, perform the following steps:

1. Double-click the bulletin board icon to display the **Read Notices** dialog:
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 messages are combined in the **Notice Group Messages** window.

4. 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.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Displaying old notices</td>
<td>Tivoli desktop</td>
<td>user</td>
</tr>
</tbody>
</table>

You can display old notices from the desktop only.

To display notices, perform the following steps:

1. Double-click the bulletin board icon to display the Read Notices dialog:

   ![Read Notices dialog](image)

   **Note:** This step requires the presence of at least one unread notice.
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 messages that have not yet expired are displayed in the Notice
Group Messages window:

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.)
Notice Expiration

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Expiring notices</td>
<td>TMR</td>
<td>senior</td>
</tr>
</tbody>
</table>

You can expire one or more notices in a notice group from the command line using `wexpnotif`. For more information about `wexpnotif`, see the *Tivoli Management Framework Reference Manual*. 
A task library icon is displayed in a policy region for each library that you create:

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 the tasks and jobs defined therein
- **Create Task**: Displays a dialog that allows you to create a task
- **Create Job**: Displays a dialog that allows you to create a job
- **Execute Task**: Displays a dialog that allows you to specify the execution parameters for a task
- **Execute Job**: Displays a dialog that allows you to select and execute a job
Tasks

You can specify that a task be run with any user ID or group ID except root. By default, you cannot create a task that requires root access. To change this behavior, you must modify the `tl_val_set_uid` or `tl_val_set_gid` validation policy. See the Tivoli Management Framework Reference Manual for procedures on editing policy.

In some cases, a task requires more information before it can run. For example, suppose you create a task that uses the UNIX `rdump` command to dump your file systems to tape. For `rdump` to execute, you must specify which file systems should be dumped. The task, therefore, requires input from the administrator at the time the task is executed.

You can execute these tasks from the command line, which allows you to specify more information, or you can create another dialog through which you can enter the necessary information. Using the Task Library Language (TLL), you can define the additional arguments required by the task. When you execute tasks defined with the TLL, a dialog prompts you for the task arguments. These dialogs are displayed after the Execute Task dialog. At that time you can, for example, specify the file system to be dumped. See the Tivoli Task Library Language Developer’s Guide for information about using the TLL to create the additional dialogs as well as an explanation of other TLL capabilities.

An icon is displayed in a task library for each task created. A single task icon, however, may represent the definition of multiple implementations of an operation—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 a dialog that allows you to specify the execution parameters for a task

**Edit Task**    Displays a dialog that allows you to modify a task that you previously created
You can also execute a task by double-clicking the task icon or dragging and dropping the icon onto either a managed node or profile manager icon.

**Jobs**

You can create several jobs that run the same task. Each job can be set up to run on different managed nodes and to direct the task output to the desktop or a specified file.

**Note:** You must create a task before you can create a job.

A job icon is displayed in a task library for each job created. You can copy a single job icon onto an administrator’s desktop without copying the entire task library. The administrator can then run that job as necessary. Following is an example of a job icon:

![Job Icon Example]

The pop-up menu of a job icon identifies the name of the job and includes the following options:

- **Execute Job**  Executes the job and sends the output to the specified destination
- **Edit Job**  Displays a dialog that allows you to modify a job that you previously created

You can also execute a job by double-clicking the job icon or, if you have admin authority, by dragging and dropping the job icon onto a managed node or profile manager. When you drag and drop a job icon, the specified list of task endpoints on which the job will execute is overridden. The job is then executed on the managed node or subscribers of the profile manager on which you dropped the job icon.

**Task Information**

When you create a task, you specify the following information:

- Platforms on which the task will run
- Authorization roles required to execute the task
Task Information

- User ID or group ID under which the task will run
- Comments concerning the task

When you select the supported platforms, you must provide the path and file names of the executable files required to run the task on each platform. The executable files are then copied from the specified path to the Tivoli bin directory.

**Note:** The executable files are copied to the bin directory; they are not linked. If you need to modify the executable file, you must replace the copy in the bin directory. See “Editing a Task” on page 9-19 for instructions on how to replace an executable file.

The task executable files are then copied to the Tivoli bin directory on the Tivoli server, on all the file servers in a Tivoli management region, or on all file servers in all regions. The extent of this distribution is determined by the distribution mode specified in the tl_def_dist_mode default policy. See “Distribution of Task Executable Files” on page 9-7 for more information about distributing task binaries.

The authorization role you specify for a task is the role required to perform the task. The administrator that executes the task must have the specified role in the policy region of the task endpoint or region-wide roles of admin.

You also specify the user ID or group ID under which the task will run. The default setting for the user ID is an asterisk (*) in the User ID text box. The asterisk indicates that the task should run under the ID of the administrator executing the task. The default setting for the group ID is nogroup.

**Note:** By default, you cannot specify root in either the User ID or Group ID text box. If you want to allow one or more administrators to create tasks that run as root, you must modify the tl_val_set_uid or tl_val_set_gid validation policy. See the Tivoli Management Framework Reference Manual for procedures on editing policy.

When the task is executed, all of the task information, including the full executable file name, is passed to the task endpoint. To locate the executable file to be passed, Tivoli first looks for a platform-specific executable file. For example, if the task is executed 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 is passed to the task endpoint. Tivoli Management Framework then validates the user ID and authorization role and runs the task directly from the managed resource.

For example, the `fs_check` task uses the `/usr/sbin/df` executable file for Solaris machines, and the `/usr/bin/bdf` executable file for HP-UX machines. The task requires the `senior` role, and the user ID is set to the default value, an asterisk (*).

Chris has the `senior` role in policy region A, but only the `admin` role in policy region B. When Chris executes the `fs_check` task on managed node `rushmore` in policy region A, Tivoli Management Framework passes all the task information to `rushmore`. Tivoli Management Framework then determines the administrator’s user ID, determines that Chris is an administrator in policy region A, and determines Chris’s role in the policy region. Because Chris has the `senior` role in policy region A, the task is executed on managed node `rushmore`. If Chris tries to execute the task on a managed node in policy region B, the task will not execute because Chris does not have the proper authorization.

**Note:** Each time a task is executed, the task executable file is passed to the task endpoint. Passing 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 use Tivoli Software Distribution to distribute these executable files.) You can then create a task that passes only a small script to run the installed executable file.

### Execution Information

When you execute a task or create a job, you must specify the following detailed information to run the task or job:

- Execution mode
- Execution parameters
Execution Information

- Output format
- Output destination
- Execution targets

The execution mode can be parallel, serial, or staged. In parallel execution mode, a task runs on all endpoints at the same time. In serial execution mode, a task runs on one endpoint at a time. If you must run a task on a large number of endpoints, you might want to use the staged execution mode. The staged mode enables you to run a task on smaller groups of endpoints until the total number has been reached. For example, if the task must run on 100 endpoints, you can use the staged mode to execute the task on 20 endpoints at a time. You can also specify an amount of time Tivoli Management Framework should wait between each execution. This minimizes the impact of large operations on system resources.

The execution parameters include the staging count (number of resources on which to execute at one time), the staging interval (duration between executions), and the task timeout setting. The timeout setting specifies how long the task library waits for task results to be returned from the target resource. If the task library times out, it does not mean that the task itself has failed, only that the task library has stopped waiting for task results.

You can choose the format and destination of the task output. The types of output you can receive are task header information, a return code, standard error, or standard output. Output can be displayed on the Tivoli desktop or sent to a file.

**Note:** When you choose to display the output on the desktop, output is displayed when the task completes on all target resources. If you schedule a job that displays its output to the desktop, an output window is not displayed when the task executes. You should save the task output to file when you schedule a task.

The execution targets are the managed resources on which the task will run. You can select from a list of endpoints and a list of profile managers. The type of resources included in the endpoint list depends on the Tivoli applications you have installed.
Distribution of Task Executable Files

When you create a task, you must specify the executable files to be used when the task is run. The task executable files (which could be programs, scripts, or binaries) are then copied to the Tivoli bin directory on either the Tivoli server in the local Tivoli management region (the default), all file servers in the local region, or all file servers in all connected Tivoli management regions. The extent of this distribution is determined by the distribution mode specified in the `tl_def_dist_mode` default policy. See “Default Policies” on page 9-8 for more information about modifying the default distribution policy.

For daily use of the task library—creating tasks and jobs that are executed by the system administrator, as necessary—the default mode of distribution is sufficient. Tivoli Management Framework searches for the task executable file on the Tivoli server and passes that executable file to the endpoint. Additional distribution of the task executable files does not increase productivity or efficiency.

Distributing task binaries to file servers either in the local Tivoli management region or in connected regions is useful only when you have Tivoli-based applications that use executable files stored in the task library. In either case, the task library provides a storage service to the application. An application can store a collection of executable files in the task library, which can then be distributed throughout local or remote Tivoli management regions. This service is most beneficial to Tivoli-based applications that have components residing on individual managed nodes.

Some Tivoli applications (such as Tivoli Distributed Monitoring) include an application-specific task library containing executable files used by the application. These executable files are automatically 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 the Tivoli Management Framework Reference Manual.

**Note:** If you distribute task binaries to file servers shared by multiple Tivoli management regions, file creation or file editing conflicts cause the distribution to fail.
Distributing the executable files to all the file servers in a Tivoli management region gives the application faster access to the executable files. Having access to local tasks also makes an application more flexible and extensible in the actions it can perform. For example, the application may have access to a wider variety of tasks or may be able to perform multiple actions, where previously it could perform only one. Tivoli recommends that you do not distribute task binaries to file servers other than the Tivoli management region server (Tivoli server) until you begin using Tivoli-based applications capable of utilizing this functionality.

**Task Library Policy**

A task library uses default and validation policies to control the tasks and jobs within the library. Administrators with the senior role and the policy role can modify the policy to reflect the operational requirements of an organization. See the *Tivoli Management Framework Reference Manual* for procedures to edit policies.

**Default Policies**

The task library default policies define the list of entries displayed in the Available Task Endpoints and Available Profile Managers scrolling lists on the Execute Task dialog. 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 distribution modes:

- **ALI** — Copies task binaries to the Tivoli server only
- **LOCAL** — Copies task binaries to all file servers in the local Tivoli management region
Task Library Policy

GLOBAL
Copies task binaries to all file servers in all connected Tivoli management regions

tl_def_man_nodes
Provides the list of endpoints displayed on the Execute Task and Create Job dialogs. From this list, you select the endpoints on which the task or job will execute.

tl_def_prof_mgrs
Provides the list of profile managers displayed on the Execute Task and Create Job dialogs. From this list, you select the profile managers on which a task or job will execute.

tl_def_set_uid
Provides the default setting for the User Name text box of the Create Task dialog. The default is an asterisk (*).

tl_def_set_gid
Provides the default setting for the Group Name text box of the Create Task dialog. The default is empty.

Validation Policies

The task library validation policies 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 will be identical to the contents of the default policies.

tl_val_man_nodes
Validates the list of endpoints on which a task or job will execute

tl_val_prof_mgrs
Validates the profile managers on which a task or job will execute

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
Creating a Task Library

policies, the administrator can drag and drop the task or job onto the additional resource. The task or job then executes on that resource.

The following policies validate the user or group ID specified on the Create Task dialog. 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

Creating a Task Library

You can create a task library within a policy region. When a task library has been created, you create and store jobs and tasks in it.

**root** write permission is required in the task library subdirectory to create a task library.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a task library</td>
<td>Policy region</td>
<td>senior</td>
</tr>
</tbody>
</table>

You can create a task library from either the desktop or the command line.

**Desktop**

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

1. From the policy region’s **Create** menu, select **Task Library** to display the Create Task Library dialog.
Creating a Task

If there is no entry on the Create menu for creating a task library, you need to first add Task Library as a managed resource type for the policy region. See “Changing Managed Resource Types” on page 5-7 for more information about adding and removing managed resources.

2. Type the name of the task library in the Name/Icon Label text box. The name of a task library can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.

3. Click Create & Close to create the task library and return to the policy region window.

After creating a task library, you are ready to populate it with tasks and jobs.

Command Line

For information about using the command line to create a task library, see werttlib in the Tivoli Management Framework Reference Manual. For information about setting the policy to control tasks and jobs within a task library, see tl_def_dist_mode, tl_def_man_nodes, tl_def_prof_mgrs, tl_def_set_uid, tl_def_set_gid, tl_val_man_nodes, tl_val_prof_mgrs, tl_val_set_gid, and tl_val_set_uid in the Tivoli Management Framework Reference Manual.

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 operation associated with the task must exist.
Creating a Task

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a task</td>
<td>Task library</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can create a task in an existing task library from either the desktop or the command line.

**Desktop**

To create a task, perform the following steps:

1. Double-click the icon of the task library in which the task will reside to display the **Task Library** window:
2. From the Create menu, select Task to display the Create Task dialog:

![Create Task dialog]

3. Type the name of the task in the Task Name text box. The name of a task can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.

4. From the Platforms Supported list, select the first platform on which the task is to be run. If you have a generic executable file such as a shell script that will run on multiple platforms, select the Generic from the list of platforms. The Generic Executable for Task dialog is displayed:

![Generic Executable for Task dialog]
Running a Task

a. In the **On Host** text box, type the name of the managed node that contains the executable file for the selected platform.

b. In the **Path to File** text box, type the full path name of the executable file for the selected platform.

c. Click **Set & Close** to display the **Create Task** dialog. You can select multiple platforms on which the task is to be run.

   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. 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 executing the task.

7. 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**.

8. Optionally, you can type a description of what the task does in the **Comments** scrolling list.

9. Click **Create & Close** to create the task and return to the **Task Library** window.

**Command Line**

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

**Running a Task**

You can run a task after the task has been created in a task library.
Running a Task

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running a task</td>
<td>Task library</td>
<td>As specified when the task was created or edited</td>
</tr>
</tbody>
</table>

You can run a task in the task library using drag and drop, from the desktop, or from the command line.

**Desktop, Drag and Drop**

To run a task, drag the task icon and drop it on the desired managed resource icon or profile manager icon. The task runs in parallel execution mode if run on a profile manager, with all output sent to the desktop.

**Note:** If you drop the task on a managed resource icon, the task is run on the managed resource. If you drop the task on a profile manager, the task is run on all of the profile manager’s subscribers. The task is subject to the policy of the managed node or task library in the policy region in which its task library is located.
Running a Task

Desktop

To run a task, perform the following steps:

1. Double-click the task icon to display the **Execute Task** dialog:

2. Specify the execution mode. Select **Parallel** if the task should run on all targets at once. Select **Serial** if the task should run on all targets, one at a time. Select **Staged** if the task should run in staged mode on sets of machines. If you select **Staged**, you must also specify the number of endpoints to include in each staged set and how many seconds for the staging interval between each set’s startup time. When the execution mode is serial or staged, the job is executed on the endpoints in alphabetical order.
3. In the **Timeout** text box, type the timeout value (in seconds) for the task. This value specifies the amount of time that the task library waits for results to be returned from the task.

4. In the **Output Format** list, select the types of output you want the task to return. The output types are **Header**, **Return Code**, **Standard Error**, and **Standard Output**.

5. Select **Display on Desktop** if you want the task output to be displayed on the desktop.

6. Select **Save to File** to save the task output to a file and display the **Destination for Task Output** dialog. Skip to the next step if you do not want the task 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 Tivoli managed node.

   b. Enter the full path name of the file to which the output of the task is to be written in the **Output File** text box.

   c. Click **Set & Close** to return to the **Execute Task** dialog.

7. To run the task on specific endpoints, select the desired endpoints from the **Available Task Endpoints** scrolling list and then click the left-arrow button. The selected endpoints are moved to the **Selected Task Endpoints** scrolling list.

8. To run the task on all subscribers of the specified profile managers, select the profile managers from the **Available Profile Managers** scrolling list and then click the left-arrow button. The selected profile managers are moved to the **Selected Profile Managers** scrolling list.

9. Click **Execute & Dismiss** to run the task as specified and return to the **Task Library** window.
Saving Task Output to a File

Command Line

For information about using the command line to run a task, see `wruntask` in the *Tivoli Management Framework Reference Manual*.

Saving Task Output to a File

If you run a task that displays its output on the desktop, you can save the output to a file.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saving displayed task output to a file</td>
<td>Task</td>
<td>As specified when the task that the job is based on was created or edited</td>
</tr>
</tbody>
</table>

To save the task output to a file, perform the following steps:

1. After the task completes, click **Save to File** on the task output dialog:
The **Save Task Output** dialog is displayed:

![Save Task Output dialog]

a. In the **On Host** text box, type the name of the managed node on which to save the task output. The machine must be a Tivoli managed node.

b. In the **Output File** text box, type the full path name of the file to which the task output is to be written.

c. Click **Save & Close** to save the task output in the specified file and return to the task output dialog. The file is written with the user ID and group ID of the administrator who invoked the task.

**Note:** If the specified file already exists, the task output is appended to the file.

---

### Editing a Task

You can edit a previously created task in a task library. The following table provides the context and authorization role required for this task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing a task</td>
<td>Task library</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can edit an existing task from either the desktop or the command line.
To edit an existing task, perform the following steps:

1. Select **Edit Task** from the task icon’s pop-up menu to display the **Edit Task** dialog:
2. From the **Platforms Supported** list, select the first platform on which the task is to be run. The **Executable for Task** dialog is displayed:

![Executable for Task dialog](image)

a. In the **On Host** text box, type the name of the managed node that contains the executable file for the selected platform.

b. In the **Path to File** text box, enter the path name of the executable file for the selected platform.

c. Click **Set & Close** to save the executable file information and return to the **Edit Task** dialog.

You can select multiple platforms to run the task on. Repeat this step for each platform the task is to be run on.

3. From the **Roles Required to Execute Task** scrolling list, select the roles that are authorized to run the task.

4. If you want the task to run under a specific user ID rather than the user ID of the administrator who runs the task, type the user ID in the **User Name** text box.

5. If you want the task to run under a specific group ID rather than the group ID of the administrator who runs the task, type the group ID in the **Group Name** text box.

6. You can enter comments in the **New Comments** scrolling list if desired. The previous revisions are described in the **Task History and Comments** scrolling list.

7. Click **Change & Close** to save your edits to the task and return to the task library window.
Creating a Job

Command Line

For information about using the command line to edit a task, see `wsettask` in the *Tivoli Management Framework Reference Manual*.

Creating a Job

You can create a job in a task library. Before you create a job, the task for the job must already exist. Jobs are subject to the policy of the policy region in which the task library exists.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Creating a job</td>
<td>Task library</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can create a job in the task library from either the desktop or the command line.

Desktop

To create a job, perform the following steps:

1. 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** dialog:

![Create Job dialog](image)

3. In the **Job Name** text box, type the job name.
   
   The name of a job can include any alphanumeric character, an underscore (_), a hyphen (-), a period (.), or a space.

4. From the **Task Name** scrolling list, select the task that the job will execute.
5. Specify the execution mode. Select **Parallel** if the job should be run on all targets at once. Select **Serial** if the job should run on all targets, one at a time. Select **Staged** if the job should run in staged mode on sets of machines. If you select **Staged**, you must also specify the number of endpoints to include in each staged set and how many seconds for the staging interval between each set's startup time. When the execution mode is serial or staged, the job is executed on the endpoints in alphabetical order.

6. In the **Timeout** text box, type the timeout value (in seconds) for the job. If the job does not complete within the specified amount of time, any output from the job is lost.

7. Select the types of output you want the job to return in the **Output Format** list. The output types are **Header**, **Return Code**, **Standard Error**, and **Standard Output**.

8. Select **Display on Desktop** if you want the job output to be displayed on the desktop.

9. Select **Save to File** to save the job output to a file and display the **Destination for Task Output** dialog. Skip to the next step if you do not want the job output saved to a file.

   a. In the **On Host** text box, enter the name of the managed node on which to save the output. The machine must be a Tivoli managed node.

   b. In the **Output File** text box, type the full path name of the file to which the output of the job is to be written.

   c. Click **Set & Close** to return to the **Create Job** dialog.

10. To run the job on specific endpoints, select the desired endpoints from the **Available Task Endpoints** scrolling list and then click the left-arrow button. The selected endpoints are moved to the **Selected Task Endpoints** scrolling list.
11. To run the job on all subscribers of the specified profile managers, select the profile managers from the **Available Profile Managers** scrolling list and then click the left-arrow button. The selected profile managers are moved to the **Selected Profile Managers** scrolling list.

12. Click **Create & Close** to create the job and return to the task library window.

**Command Line**

For information about using the command line to create a job, see `wcrjobj` in the *Tivoli Management Framework Reference Manual*.

**Running a Job**

You can run a job after the job has been created in a task library. The following table provides the context and authorization role required for this task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running a job</td>
<td>Task library</td>
<td>As specified when the task that the job is based on was created or edited</td>
</tr>
</tbody>
</table>

You can run a task library job using drag and drop, from the desktop, or from the command line. Note that using drag and drop requires the `admin` role.

**Desktop, Drag and Drop**

To run a job using drag and drop, drag the job icon onto the icon of the managed resource or profile manager on which you want the job to run.
Saving Job Output to a File

Desktop

To run a job, double-click the icon of the job you want to run. The job is run and the output is displayed on the desktop or sent to the file designated in the job specification.

Command Line

For information about using the command line to run a job, see the wrunjob command in the Tivoli Management Framework Reference Manual.

Saving Job Output to a File

If you run a job and display the output to the desktop, you can save the output to a file.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saving displayed job output to a file</td>
<td>Job</td>
<td>As specified when the task that the job is based on was created or edited</td>
</tr>
</tbody>
</table>

You can save displayed job output to file from the desktop only.

To save the job output to a file, perform the following steps:

1. After the job completes, select Save to File on the job output dialog:
Saving Job Output to a File

The **Save Job Output** dialog is displayed:

![Save Job Output Dialog](image)

a. In the **On Host** text box, type the name of the managed node on which to save the job output. The machine must be a Tivoli managed node.

b. In the **Output File** text box, type the full path name of the file to which the job output is to be written.

c. Click **Close** to save the job output in the specified file and return to the job output dialog. The file is written with the user ID and group ID of the administrator who invoked the job.

2. Click **Dismiss** to return to the job output dialog.
You can edit a previously created job in a task library. The following table provides the context and authorization role required for this task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Editing a job</td>
<td>Task library</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can edit a job in the task library from either the desktop or the command line.

**Desktop**

To edit a previously created job, perform the following steps:

1. Select **Edit Job** from the job icon’s pop-up menu to display the **Edit Job** dialog:
2. In the **Task Name** scrolling list, change the name of the task that the job will execute.

3. Change the execution mode. Select **Parallel** if the job should run on all targets at once. Select **Serial** if the job should run on all targets, one at a time. Select **Staged** if the job should run in staged mode on sets of machines. If you select **Staged**, you must also specify the number of managed resources to include in each staged set and how many seconds for the staging interval between each set’s startup time. When the execution mode is serial or staged, the
job is executed on the managed resources in alphabetical order.

4. In the **Timeout** text box, change the timeout value (in seconds) for the job. If the job does not start within the specified amount of time, it is canceled.

5. In the **Output Format** list, change the types of output you want the job to return. The output types are **Header**, **Return Code**, **Standard Error**, and **Standard Output**.

6. Select **Display on Desktop** to display the job output on the desktop.

7. Select **Save to File** to save the job output to a file and display the **Destination for Task Output** dialog. Skip to the next step if you do not want the job output saved to a file.

   ![Destination for Task Output](image)

   a. In the **On Host** text box, enter the name of the managed node on which to save the output. The machine must be a Tivoli managed node.

   b. In the **Output File** text box, type the full path name of the file to which the output of the job is to be written.

   c. Click **Set & Close** to return to the **Edit Job** dialog.

8. To run the job on specific managed nodes, select the desired managed nodes from the **Available Task Endpoints** scrolling list and then click the left-arrow button. The selected managed nodes are moved to the **Selected Task Endpoints** scrolling list. The job is subject to the policies of the specified managed nodes.

9. To run the job on all subscribers of the specified profile managers, select the profile managers from the **Available Profile Managers** scrolling list and then click the left-arrow button. The selected profile managers are moved to the **Selected Profile Managers** scrolling list. The job is subject to the policies of the specified profile managers and their subscribers.
10. Click Change & Close to save your changes to the job and return to the task library window.

**Command Line**

For information about using the command line to edit a job, see `wsetjob` in the *Tivoli Management Framework Reference Manual*.

**Deleting a Task or Job**

You can delete a task or job from a task library.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deleting a task or job</td>
<td>Task library</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can delete a job or task from the task library from either the desktop or the command line.

**Desktop**

To delete a task or job from a task library, perform the following steps:

1. Select the icon of the task or job to be deleted.
2. From the Edit menu, select Delete. The selected task or job is deleted.

**Command Line**

For information about using the command line to delete a task or job, see `wdeltask` and `wdeljob` in the *Tivoli Management Framework Reference Manual*. 
Using the AS/400 Task Library for Common Tasks

Tivoli provides an AS/400 task library to automate tasks that are performed frequently by an AS/400 operator. These tasks are primarily designed to help automate Tivoli Enterprise Console actions or to aid in remotely managing an AS/400 system. As with all AS/400 commands or jobs, these commands must be executed under the explicit authority of an AS/400 user profile that is specified in the task dialog box. If no profile is specified in the dialog box, the user ID running the desktop is used.

Tasks for AS/400 can be batch jobs, REXX scripts, or compiled programs. The following tasks are provided:

- **Command** Enables you to enter any AS/400 control language command, valid in batch mode, for which all parameters are known. Prompting is not supported.
- **Send_Reply** Invokes the AS/400 command `SNDRPLY` to send a reply to a message on a specific message queue.
- **Run_Backup** Invokes the AS/400 command `RUNBKUP` to start saving information about your AS/400 system.
- **Start_cleanup** Invokes the AS/400 command `STRCLNUP` to start cleaning up information about your AS/400 system, such as spool files or temporary libraries.
- **Power_Down_System** Invokes the AS/400 command `PWRDWNSYS` to end all subsystems, power down the system, and optionally re-IPL a remote AS/400 system.
- **Vary_Configuration** Invokes the AS/400 command `VRYCFG` to reset lines, controllers, and devices attached to an AS/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, refer to the *IBM AS/400 Control Language Reference Manual.*
Like other components of Tivoli Management Framework, the scheduler is not so much an application or standalone resource as a service. For example, you make use of the scheduler when you have other components or applications installed. The scheduler is represented on your desktop by the following icon:

![Scheduler Icon]

**Job Scheduling**

You can schedule a job to run one time only, or you can specify that the job be repeated at specified intervals or for a specified number of times. You can also add restrictions to when a job runs. You might, for example, schedule a job to run daily, but only Monday through Friday. After a job runs, you are notified in the manner you selected. If the job does not have a repeating specification, the job is removed from the scheduler queue.

**Jobs Scheduled to Run Once**

To run a job once, you specify the following information:

- Job name
- Scheduled date and time for the job
Action that occurs when the job completes

For example, to schedule a job for August 15, 1996, at 5:00 p.m., perform the following steps:

1. From any window or dialog with a **Schedule** button, click the button to display the **Add Scheduled Job** dialog:

2. In the **Job Label** text box, specify the job label. If you do not provide a job label, the job name is used by default.

3. In the **Schedule Job For** text boxes, specify the date and time at which the job is to run.
4. Specify the action to occur when the job completes by selecting the Log to File check box and entering the appropriate information in the Host and File text boxes.

5. To schedule the job and return to the desktop, click Schedule Job & Close.

Jobs Scheduled to Run Frequently

A job can be scheduled to run repeatedly in two ways:

- Indefinitely at specified time intervals
- A specified number of times at specified time intervals

Jobs Scheduled to Run at Specified Intervals

You can schedule a job to begin at a specified time and then repeat indefinitely at specified intervals. You can specify the repeat frequency in minutes, hours, days, weeks, months, or years.

For example, if you want to schedule a job to run at 3:00 a.m. on April 25, 1996, and then repeat indefinitely at 5-day intervals, perform the following steps:

1. From any window or dialog with a Schedule button, click the button to display the Add Scheduled Job dialog:
2. In the **Job Label** text box, specify the job label. If you do not provide a job label, the job name is used by default.

3. In the **Schedule Job For** text boxes, specify the date and time for the initial job run.

4. Select **Repeat the job indefinitely**.

5. Enter **5** in the **The job should start every** text box.
6. Select **day** from the drop-down list displayed to the right of the **The job should start every** text box.

7. Specify the action to occur when the job completes by selecting the **Log to File** check box and entering the appropriate information in the **Host** and **File** text boxes.

8. Click **Schedule Job & Close** to schedule the job and return to the Tivoli desktop.

After the initial job runs, the next scheduled job runs 5 days later, on April 30, 1996, at 3:00 a.m. The job repeats at 5-day intervals until you remove it from the scheduler.

If the scheduler cannot run a job at the scheduled time or if the job times out before it can start, the job does not run. The job is then rescheduled for the next scheduled time.

**Jobs Scheduled to Run a Specified Number of Times**

You can also schedule a job to repeat a specified number of times at specified intervals. After a job runs the specified number of times, it is removed from the scheduler.

If the scheduler cannot run a job at the scheduled time or if the job times out before it can start, the job does not run. The job is then rescheduled to run for the specified number of times.

**Note:** This does not include jobs that fail and are being retried. See “Retry on Failed Jobs” on page 10-11 for information about retrying jobs.

For example, you schedule a job to run on January 28, 1998, at 11:30 p.m. and then repeat twice at 10-hour intervals. After the initial job run, the job repeats on January 29, 1998, at 9:30 a.m. and again on January 29, 1998, at 7:30 p.m. The job is then removed from the scheduler.

**Jobs Scheduled to Run Monthly**

The scheduler automatically adjusts for jobs scheduled to run at the same time each month. The scheduler adjusts the number of days so that the job runs on the same date each month. If there are not enough days in a particular month, the scheduler runs the job on the last day of the month. For example, if you schedule a job for January 31, 1998, and specify that it repeat monthly, the second run will occur on February 28,
1998. The scheduler maintains the original scheduling information so that the job always falls on the same date of the month, or else on the last day of the month if there are not enough days in a particular month. In this example, the third run would occur on March 31, 1998.

You can also schedule a job to run only on February 29 by specifying a date of February 29 and a yearly increment of four. If you want a job to run annually on the last day of February, you can specify a date of February 29 and a yearly increment of one. The job will run on February 29 in leap years and on February 28 in non-leap years.

**Jobs Scheduled for the Past**

If you schedule a job to run once and the scheduled run time is prior to the current time, a warning is displayed indicating that the scheduled time has already passed; you can either reenter the time or continue. If you choose to continue, the job is run immediately.

If you schedule a repeat job and one or more of the scheduled run times are prior to the current time, a warning is displayed indicating that the scheduled time for one or more job runs has already passed. If you choose to continue, these job runs are not performed; the number of scheduled job runs is decreased by the number of job runs that were not performed because their specified times have already passed. Only job runs scheduled to occur after the current time are added to the scheduler.

For example, assume the current time is 1:00 p.m. on January 9, 1998. You schedule a job to run on January 8, 1998, at 11:00 p.m., and specify that it repeat three times at 5-day intervals.

A warning is displayed indicating that the scheduled date for the first job run has already passed, and you choose to continue. The first job run is not scheduled. You are notified that the first job run did not occur because the scheduled date has already passed. The scheduler decreases the number of job runs by one and schedules the next job run. The scheduler runs the job on January 13, 1998, at 11:00 p.m. and again on January 18, 1998, at 11:00 p.m.

As another example, assume the current time is 3:00 p.m. on January 21, 1998. You schedule the same job as in the previous example. Because 11:00 p.m. on January 8, 1998, has already passed, you are notified that the first job was not run. The scheduler decreases the number of job runs...
by one and schedules the next job run for 11:00 p.m. on January 13, 1998. Because this date has already passed, you are notified that the second job was not run. The scheduler decreases the number of job runs by one and schedules the next job run for 11:00 p.m. on January 18, 1998. Because this date has also passed and the scheduler has attempted to schedule the job the specified number of times (three), the scheduler removes the job and posts a notification that all three scheduled runs were for dates that had already passed and that the job never ran.

Job Restrictions

The Tivoli scheduler lets you limit when a job can run. You can restrict a job to run during the day, at night, during the week, or on weekends. For example, you might create a job that runs every day at 10:00 p.m., and then restrict the job to run only Monday through Friday.

To add job restrictions, perform the following steps:

1. From any window or dialog with a Schedule button, click the button to display the Add Scheduled Job dialog:
2. Click **Set Retry/Cancel/Restriction Options** to display the **Set Retry/Cancel Options** dialog.
3. Select the appropriate check box in the Restrictions group box. Then use the associated drop-down lists to set restrictions for time of day and day of the week. For example, select During the day and use the drop-down lists to the right to set specific run times.

4. Click Set to save the restrictions and return to the Add Scheduled Job dialog.

The scheduler maintains the specified repetition cycle during the times that the job is restricted from running. Suppose, for example, you schedule a job to start running at 6:00 a.m. and repeat every 2 hours. You then restrict the job to run only from 9:00 a.m. to 1:00 p.m. This job runs at 10:00 a.m. and 12:00 p.m., but not at 9:00 a.m., 11:00 a.m., and 1:00 p.m. Because the job was started at 6:00 a.m. and repeated every 2 hours, it runs only at even-numbered hours.

**Jobs Starting within a Given Time**

A scheduled job may not be able to start at the specified time. For example, a large number of jobs may be scheduled to start simultaneously or the scheduler may be down. You can optionally specify a period of time, after the scheduled start time, within which it is
acceptable for the job to run. If the job does not start within this period of time, it does not run and you are notified. You can specify the allowable start-time period in minutes, hours, or days.

**Note:** If the scheduler is down for any reason, it maintains information about all scheduled jobs. When the scheduler is restarted, it automatically reschedules any jobs that were scheduled before it was stopped, as long as the allowable time period for starting a particular job has not passed.

For example, you schedule a job for January 25, 1998, at 3:00 a.m., and then click **Set Retry/Cancel/Restriction Options** (on the **Add Scheduled Job** dialog) to specify the allowable time period for starting the job.

In the **Set Retry/Cancel Options** dialog, you specify that the job should be canceled if it does not start within 5 minutes of its scheduled start time. The current time is 3:02 a.m., January 25, 1998. Because the scheduler has been busy, the job has not yet been run, but the scheduler is now available to run the job. The current time is within the allowable start-time period, so the job runs normally. If the scheduler remained
busy until 3:07 a.m., however, the job would not run and you would be notified.

**Retry on Failed Jobs**

If a scheduled job does not start due to a failure of some type (for example, the scheduler is down or the job times out before it can be started), you can specify that the scheduler retry the job. A job can be retried until it starts successfully, or it can be retried a specified number of times before it is removed from the scheduler. You can also specify the time interval (in minutes, hours, or days) at which the job should be retried. Note that after successfully starting a job, the scheduler continues to monitor a job’s progress. If the job does not complete successfully, the scheduler notifies you.

For example, you schedule a job to run at 12:00 p.m. on January 29, 1998, and specify that it be retried at 1-hour intervals until it is successful.

1. After entering the basic job information in the **Add Scheduled Job** dialog, click **Set Retry/Cancel/Restriction Options** to display the **Set Retry/Cancel Options** dialog:
Retry on Failed Jobs

2. Select **Retry the job until success**.

3. Enter **1** in the **The job should retry every** text box.

4. Select **hour** from the drop-down list to the right of **The job should retry every** text box.

5. Click **Set** to schedule the job and return to the desktop.

Ideally, the job begins at the scheduled start time and runs successfully. Suppose, however, the scheduler is busy at 12:00 p.m. but attempts to start the job at 12:03 p.m. The job does not run, and you are notified based on the notification method you selected when you created the job. The job is rescheduled to run at 1:00 p.m. The scheduler continues this process until the job runs successfully or until the allowable run time has passed.

**Note:** Only successful retries count as runs for repeat jobs. Failed retries do not decrease the number of scheduled repeat job runs unless the retries are for a finite number and they all fail.

Retries occur only within a job’s start-time period or run restrictions. In the preceding example, the job is canceled if it does not start within 3 hours. If the job fails on the first run attempt, the scheduler tries to run the job every hour in the 3-hour start period, or a maximum of two times.

If the job was scheduled to run only once, the scheduler cancels the job if it did not start during the start period. If the job is scheduled to repeat later and fails to run during the start time, the scheduler logs a message that the job failed and schedules the job for the next repeat time.

If a repeat job’s specified retry period overlaps the specified start time for a later repetition, the job is not scheduled and you are notified that the scheduled start and repeat times conflict. For example, if you specify a start-time period of 7 hours but schedule the job to repeat every 6 hours, the job is not scheduled and you are notified that the start and repeat times conflict.

If a job has restrictions specified for when it can run, the scheduler retries the job only during the allowable run time for the job. Suppose a job is scheduled to run at 10:00 p.m. on Monday through Friday, has no cancellation limit, and should retry every hour until successful. If Friday’s job fails, the scheduler retries the job at 11:00 p.m. on Friday. If that retry fails, the scheduler does not try to run the job again until Monday. At 12:00 a.m. Monday, the scheduler continues to retry.
Job Disabling

Friday’s failed job; Monday’s job is not scheduled until Friday’s job runs successfully.

Job Disabling

You can disable a job so that it remains in the scheduler, but does not run. You must have the admin authorization role to enable or disable a scheduled job. The procedure for disabling jobs differs for jobs that are scheduled to run at a specified time and jobs that are scheduled to repeat a specified number of times.

Jobs Set for a Specified Time

If you disable a job that is scheduled to run at a specified time, the job does not run but remains in the scheduler. If the scheduled time passes before you enable the job and the job does not specify an allowable time period for starting, the job runs as soon as you enable it. If you do not want the job to run immediately when you enable it, you should edit the job before enabling it.

Note: If a disabled job specifies an allowable time period for starting and the allowable start-time period has already passed when you enable the job, the job does not run.

Jobs Set to Repeat

If a job is scheduled to repeat for a specified number of times, scheduled runs that are skipped while the job is disabled count as job runs. If you disable a job that is scheduled to run at specified intervals, the job does not run but remains in the scheduler. If the scheduled time for the job passes while the job is disabled, the job is rescheduled for its next scheduled time. If it is still disabled at that time, it does not run. For example, suppose you schedule a job to run four times, but it is disabled when the time for the first scheduled run occurs. If you then enable the job (before the second scheduled run), the job runs a total of three times only.
Notification

The scheduler notifies you of all scheduler events. You can specify notification options in specific scheduler dialogs. All scheduler events are posted to the **Tivoli Scheduler** notice group by default; it is not necessary to explicitly specify that a scheduler event be posted to the **Tivoli Scheduler** notice group.

The scheduler can notify you in the following ways:

- Posting a Tivoli notice to a specified notice group
- Sending electronic mail
- Posting a status dialog to an administrator’s desktop
- Logging to a file on a managed node

Scheduler across Tivoli Management Regions

Each Tivoli management 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 management region in which the job was scheduled. For example, a job scheduled in region **Baltimore** is stored in region **Baltimore**’s scheduler.

Most scheduler actions, such as editing or removing a job, occur only within the scheduler’s Tivoli management region. However, you can run jobs across multiple regions.
Jobs Run in Multiple Tivoli Management Regions

A job that is run in a Tivoli management region can cross region boundaries.

For example, 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.

Start Times in Tivoli Management Regions

The start times for jobs residing in a Tivoli management region are specified in the region’s local time.

For example, you use Bulldog to schedule a job to be run on Bulldog. 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. Eastern Standard Time (EST).
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 Tivoli task library or from within an application. You cannot use the scheduler to create a job.

Note: There are several options for scheduling jobs. See “Job Scheduling” on page 10-1 for more information.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scheduling a job</td>
<td>Scheduler</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can schedule a job using drag and drop, from the desktop, or from the command line.

**Desktop, Drag and Drop**

To schedule a job using drag and drop, drag and drop the job’s icon onto the scheduler icon. The **Add Scheduled Job** dialog is displayed. See the next section for instructions on using this dialog.

**Desktop**

To schedule a job, perform the following steps:

1. From any window or dialog with a **Schedule** button, click the button to display the **Add Scheduled Job** dialog:
2. In the **Job Label** text box, type the job label. If you do not enter 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. In the **Schedule Job For** text boxes, Specify the scheduled date and time.

4. If necessary, specify the number of times the job is to repeat and the time interval for repetitions. If the job is to be run only once, it is not necessary to use the repeat options.
Scheduling a Job

Note: The Repeat the job indefinitely and Repeat the job n times check boxes are mutually exclusive.

5. Type the action that should occur when the job completes.

6. To set retry, cancel, or restriction options for the job, click Set Retry/Cancel/Restriction Options. The Set Retry/Cancel Options dialog is displayed. If you do not want to specify these options for the job, skip to step 7 on page 10-19.

In the Set Retry/Cancel Options dialog, you can do the following:

- Specify that a job should be canceled if it does not start within a specified time period after its scheduled start time.

- Specify that a job should be retried if it is unable to start at the scheduled time:
  - To specify a time limit for the start of a job, select Cancel job if it does not start within and enter the allowable time period (after the scheduled start time) for the job to start. Use the text box and drop-down list to the right of this check box to specify the allowable start-time period in minutes, hours, or days.
Changing or Viewing Scheduled Jobs

To retry a job until it is successful, select **Retry the job until success**. Then enter the time interval at which the scheduler should retry the job in the **The job should retry every** text box. Use the drop-down list to specify the retry-time interval in minutes, hours, or days.

To retry a job a specified number of times, select **Retry the job n times** and enter the number of times the job is to be retried. Then enter the time interval at which the scheduler should retry the job in the **The job should retry every** text box. Use the drop-down list to specify the retry-time interval in minutes, hours, or days.

Specify restrictions on when the job can run:

- To restrict a job, select **During the day**, **At night**, **During the week**, or **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 retry/cancel options and return to the **Add Scheduled Job** dialog.

7. Click **Schedule Job & Close** to schedule the job and return to the desktop.

**Command Line**

For information about using the command line to schedule a job, see `wschedjob` in the *Tivoli Management Framework Reference Manual*.

**Changing or Viewing Scheduled Jobs**

You can use the **Browse Scheduled Jobs** window to edit a previously scheduled job before it is run. You can edit the scheduling information but not the job itself. You can also use this window to disable, enable, delete, or browse scheduled jobs.

**Note:** See Chapter 9, “Task Library” if you want to edit a job.

When a scheduled job is edited, it is rescheduled based on the revised information. A rescheduled job is scheduled after all other jobs that have the same start time.
Changing or Viewing Scheduled Jobs

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viewing scheduled jobs</td>
<td>Scheduler</td>
<td>user</td>
</tr>
<tr>
<td>Disabling or enabling a job</td>
<td>Scheduler</td>
<td>admin</td>
</tr>
<tr>
<td>Deleting a job</td>
<td>Scheduler</td>
<td>admin</td>
</tr>
<tr>
<td>Editing a job</td>
<td>Scheduler</td>
<td>admin</td>
</tr>
</tbody>
</table>

You can perform these tasks from either the desktop or the command line.

**Desktop**

The following procedures can be performed from the **Browse Scheduled Jobs** window.

**Viewing Scheduled Jobs**

To view scheduled jobs, perform the following steps:

1. From the **Scheduler** icon’s pop-up menu, select **Browse/Edit** to display the **Browse Scheduled Jobs** window:
Changing or Viewing Scheduled Jobs

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 Display of Job Attributes” on page 10-24 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.

Disabling or Enabling Scheduled Jobs

To disable or enable a job, perform the following steps:

1. From the Scheduler icon’s pop-up menu, select Browse/Edit to display the Browse Scheduled Jobs window.

2. Select the job row. You can select more than one job by pressing the Shift key while selecting a job row.

3. Click Enable to enable the job, or click Disable to disable the job.
Deleting Scheduled Jobs

To delete a job, perform the following steps:

1. From the Scheduler icon’s pop-up menu, select Browse/Edit to display the Browse Scheduled Jobs window.
2. Select the job row. You can select more than one job by pressing the Shift key while selecting a row.
3. Click Delete.

Editing Scheduled Jobs

To edit a job, perform the following steps:

1. From the Scheduler icon’s pop-up menu, 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 existing job parameters are displayed in the Edit Scheduled Job dialog:
4. Specify the job changes.

5. Click Update & Close to accept the job changes and return to the Browse Scheduled Jobs window.

**Command Line**

For information about using the command line to edit scheduled jobs, see `wgetsched` and `wedsched` in the Tivoli Management Framework Reference Manual.
Controlling 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifying displayed job</td>
<td>Scheduler</td>
<td>user</td>
</tr>
<tr>
<td>information</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can specify job display information from the desktop only.

To set the information displayed about each job, perform the following steps:

1. From the Scheduler icon’s pop-up menu, select Browse/Edit to display the Browse Scheduled Jobs window:
2. From the View menu, select the Columns option to display the Browse Table Attributes dialog:

![Browse Table Attributes dialog](image)

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 from the Attributes Available scrolling list 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 from the Attributes Displayed scrolling list to the Attributes Available scrolling list.

4. Click Display & Close to accept your changes, update the scheduled jobs dialog, 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 or not that attribute is displayed in the Browse Scheduled Job window.
You can organize a sort in ascending order (for example, A, B, C or 1, 2, 3) or descending order (for example, Z, Y, X or 3, 2, 1). You can also choose multiple sort options and arrange them in the desired order. 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sorting job information</td>
<td>Scheduler</td>
<td>user</td>
</tr>
</tbody>
</table>

You can sort job information from the desktop only.

To sort job information, perform the following steps:

1. From the **Scheduler** icon’s pop-up menu, select **Browse/Edit** to display the **Browse Scheduled Jobs** window:
2. From the **View** menu, select the **Sort** option from the **View** menu to display the **Sort** dialog:

![Sort dialog](image)

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 or not the attribute is displayed in the **Browse Scheduled Jobs** window.
The following table provides the context and authorization role required for this task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Finding job information</td>
<td>Scheduler</td>
<td>user</td>
</tr>
</tbody>
</table>

You can find a job from the desktop only.

To find a specific job, perform the following steps:

1. From the **Scheduler** icon’s pop-up menu, select **Browse/Edit** to display the **Browse Scheduled Jobs** window:
2. From the View menu, select the Find option to display the Find dialog:

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.
11 Application Management

Application management is a significant part of the activities that make up network administration. Networks make commercial and custom applications available to users in multiple locations on various platforms. Network administrators rely on management software, such as Tivoli Management Framework and its tools, to distribute, install, and maintain applications from a central, integrated point of control.

Tivoli provides products that coordinate the application management features of Tivoli tools. Such products as the Tivoli Application Management modules and Tivoli Application Management Specification (AMS) modules automate the process of loading tools with management data and integrating the views that tools display for managed applications. The modules are add-on products, sold separately from Tivoli Management Framework. As an included feature, Tivoli Management Framework also provides the winstruct command. Like the modules, this command automates the process of loading Tivoli tools with management data. With winstruct, you can quickly set up the Tivoli environment to distribute, install, and maintain applications.

This chapter focuses on winstruct. For more information about the modules, refer to the product documentation for each one.
Description of Application Management

Application management is the work that network administrators do to provide programs to users. This entails distributing and installing an application on many computers, often in different geographical locations. The computers are typically of different platform types. The distribution must account for network traffic as well as the operational status of the computers—that is, whether they are up and running. The installation must account for the different system requirements of an array of operating systems.

When installed, an application requires maintenance. The network administrator monitors the application and the computers on which it runs, checking that resources (such as memory and disk space) remain at sufficient levels. If it becomes necessary to modify the operation of either the application or a computer, the administrator runs scripts or programs to make adjustments.

The full cycle of management tasks for an application consists of the following processes:

**Distributing** Transferring application source files and auxiliary management files to target computers

**Dependency checking** Determining, before installation, that the hardware and software configurations of targets satisfy the application’s requirements

**Installing** Executing installation programs and scripts

**Configuring** Setting configuration options related to the installed application

**Monitoring** Soliciting and receiving notices about the operation of the application, the operating system, and the computer

**Maintaining** Executing maintenance tasks, such as managing disk space or stopping and starting processes

**Updating** Distributing and installing new versions of the application

**Uninstalling** Removing an application from one, some, or all of the computers in the network
Application Management Data

Application management data provides information about an application. The information describes the application itself as well as support files, such as configuration scripts and programs that execute maintenance tasks.

Management data includes the following:

- Name and version of the application
- Types and versions of target platforms
- Requirements for different platform operating systems
- Hierarchical organization of the application as elemental components, and the relationships between those components
- Paths and names of source files that make up the application
- Paths of destination directories on targets
- Dependencies for distribution to targets
- Configuration scripts that run before or after the distribution
- Specification of events generated by the application and the systems on which it runs
- Methods for receiving and responding to events
- Maintenance scripts and programs that perform tasks for operational control

Applications for which data is defined are considered management ready.

Tivoli Management Framework and its tools require application management data in a format that complies with the AMS 2.0. The AMS is a Tivoli innovation based on the Management Information Format (MIF). The MIF is an open standard invented by the Desktop Management Task Force (DMTF), a consortium of such industry leaders as IBM, Microsoft Corporation, Hewlett-Packard, and Intel Corporation. The goal of the DMTF is to define standardized syntax for data that describes how to manage the hardware and software components of desktop computers.
Application Description Files

In accordance with the AMS, management data must be stored in a set of several application description files. Following is the set of description files for each application:

**Application Object File (.aof)**

Text file that lists and calls the other description files. One .aof is created for an application.

**Global Description File (.gdf)**

Text file that describes the application in general terms: application name, version, manufacturer or author, and description. One .gdf is created for an application.

**Component Description File (.cdf)**

AMS-compliant file that provides data necessary to manage some aspect of an application. One or more .cdf files are created for an application. A comparatively simple application might require only one .cdf that supplies all the management data. A more complex application might have several .cdf files for the server, client, and database components.

Tools for Developing Management Data

Application description files are ASCII text files. By adhering to the AMS guidelines for syntax, developers can write description files with any text editor. However, this method is slow and tedious. Instead, developers typically use an AMS-compliant development tool to create application management data. Examples are Tivoli Module Builder, Version 2.0 and Tivoli Module Designer, Version 2.0, which conform to the AMS 2.0 standards. These software development programs provide GUIs through which developers supply management data. With the values developers enter in the dialogs, the tools create all the description files necessary to make an application management ready.

In addition to the application description files, the Tivoli development tools produce an application management package (AMP). (Tivoli Module Builder also creates the image file with which you install a
How Tivoli Tools Use Management Data

Tivoli Application Management module or AMS module.) An AMP is a compressed file in the Java™ JAR format. An AMP contains all the description files for an application: one .aof, one .gdf, and one or more .cdf files. An AMP also includes support files, such as task scripts and executable programs used to conduct management activity in the Tivoli environment. Optionally, the AMP can include source files for the application. Developers who choose not to include application source files in the AMP can specify a different location for distribution.

For more information about Tivoli Module Builder and Tivoli Module Designer, refer to the appropriate application guide.

How Tivoli Tools Use Management Data

Management tools interpret the application data and apply it in the operations for which the tools are designed. A full installation of the Tivoli environment, for example, provides tools for distributing files and monitoring the environment. Tivoli tools also provide user administration and access management. Each tool uses only specific parts of the management data provided for an application.

For example, the Tivoli Software Distribution tool uses information about source files and their locations to create file packages. Tivoli Distributed Monitoring uses information about event parameters and thresholds to create monitors. Some tools use the same information to accomplish different tasks; for example, both Tivoli Inventory and Tivoli Software Distribution use data about the file structure of application components. Tivoli Inventory uses the data to keep records of installations, and Tivoli Software Distribution uses it to configure distributions.

The following Tivoli management tools support AMS 2.0:

- Tivoli Management Framework
- Tivoli Enterprise Console
- Tivoli Software Distribution
- Tivoli Inventory
- Tivoli Distributed Monitoring
- Tivoli Application Management modules
How Tivoli Tools Receive Data

Although you can supply each Tivoli tool individually with information about an application, winstruct provides automated delivery of all data to the entire Tivoli environment.

In previous releases of Tivoli, you informed the environment about an application by manually entering data in each tool. You created file packages in Tivoli Software Distribution; created monitors, tasks, and event responses in Tivoli Distributed Monitoring; and created software signatures in Tivoli Inventory. After providing the information to all the tools, you were finally prepared to manage the application in the Tivoli environment.

Now, winstruct automates the individual preparations required for each tool. Using the data stored in the application description files, which are contained in the AMP, winstruct makes management data available to each relevant Tivoli tool. The command writes the management data to the Tivoli database. When the command finishes processing, you are ready to manage the application.

Superseded AMS Commands

The winstruct command replaces the Tivoli import commands, wimprtcdftl, wimprtcdffp, and wimprtdfmon. These commands represent the AMS 1.1 import model. The winstruct command set represents the AMS 2.0 instruct model.

In the import model, you supplied the Tivoli Management Framework tools, one at a time, with information about a software product. The import commands parsed AMS 1.1 syntax and performed minimal setup procedures. These commands required you to perform several preliminary steps before performing the import. For each import, the information was limited to the purpose of the management tool for which the command was given.

In the current instruct model, you can prepare the entire environment in one step. By entering a single command, you can supply (or instruct) the entire Tivoli environment—the Tivoli Management Framework and all installed tools—with all the management information for a software product. With the environment properly instructed, you can readily find product information that is specific to the different management tools.
New Icons on the Tivoli Desktop

In addition to adding data objects to the Tivoli database, **winstruct** adds icons the Tivoli desktop.

The following diagram illustrates the hierarchy of the new icons:

When you issue the **winstruct** command for the first time, it creates the Applications policy region on the Tivoli desktop. The name of the icon is **Applications_Policy-Region**, where **Policy-Region** is the name of the Tivoli management region. Each region has only one Applications policy region. Subsequent uses of **winstruct** do not create additional Applications icons in a single Tivoli management region.

**Note:** If an AMP contains Management Tool Extension Group (MTEG) data, **winstruct** creates a Tivoli Application Management module icon in addition to the icon for the Applications policy region.
The Applications policy region contains a secondary policy region for the specific application you instructed. The name of this icon is **PR_AppName_tag_Policy-Region**, where **AppName** is the name of the application as stated in the global description file (**.gdf**). The **tag** variable is a unique version identifier (also called an administrator's tag).

With subsequent uses, **winstuct** creates new, uniquely named secondary policy regions for each new application you add. The command also creates new secondary policy regions for modified variations, called tagged versions, of original applications. You specify an administrator’s tag with the **–t** option on the **winstuct** command line. If you do not use **–t**, such as when instructing the original application, **winstuct** supplies **Default** for the tag string.

In each **AppName** policy region, **winstuct** creates task and dependency libraries, depending on whether the developer defined tasks and dependency checks in the component. For each component (represented by a **.cdf** file in the AMP), **winstuct** creates one task library and one dependency library, if defined. Also, for each component that specifies files or monitors, or both, **winstuct** creates a profile manager. The profile manager contains one file package or one monitor collection, or both. If a component has neither files nor monitors, the command does not create a profile manager for that component.

### Data Objects

The **winstuct** command creates the following Tivoli data objects:

- Notification groups
- Task library
- Dependency library
- Query library
- Policy regions
- Profile managers
- Profiles
- File packages
- Monitors
Using the winstruct Command

The command set creates profile managers, but not dataless profile managers. Because Tivoli endpoints require dataless profile managers, you must take extra steps following a winstruct session to provide them. See “Subscribing Endpoints” on page 11-18 for more information.

New Notification Groups

In addition to the desktop icons, winstruct creates new notification groups in the Notices viewer. With its first invocation, winstruct creates a general Applications Management notification group, plus another group for the specific application described in the AMP. The name of this second notification group reflects the name of the application. Each new use of winstruct creates another group for a new application. However, winstruct does not create new notification groups for multiple versions of the same application. For example, if you enter the winstruct command and specify the –t option for an alternate tagged version, winstruct does not create a new notification group. Instead, notices for all versions are contained in the single group created for the application.

Using the winstruct Command

The winstruct command is a set of command line interfaces (CLIs), consisting of a top-level command and several subcommands. The command is not available in the Tivoli desktop. The winstruct commands are so named because they instruct or “teach” the Tivoli environment how to work with management-ready applications. All AMS 2.0-compliant tools installed in the Tivoli environment can receive data from the management information stored in AMPs. Developers can design the AMP to provide data for some or all of the eligible tools.

winstruct Command Set

The winstruct command set consists of one main command and six subcommands:

winstruct Provides the Tivoli Enterprise environment with information necessary to install and manage an
Using the winstruct Command

application. This command is packaged with the Tivoli Management Framework product.

winstruct_task
Provides the Tivoli Enterprise environment with information necessary to create tasks and dependencies for installing and managing an application. This command is packaged with the Tivoli Management Framework product.

winstruct_file
Provides Tivoli Software Distribution with information necessary to create file packages for distributing an application. This command is packaged with the Tivoli Software Distribution product.

winstruct_monitor
Provides Tivoli Distributed Monitoring with information necessary to create monitors for maintaining an application. This command is packaged with the Tivoli Distributed Monitoring product.

winstruct_event
Provides the Tivoli Enterprise Console product with information necessary to receive events from monitors defined for an application. This command is packaged with the Tivoli Enterprise Console product.

winstruct_inventory
Provides Tivoli Inventory with information necessary to add signatures for an application to the database. This command is packaged with the Tivoli Inventory product.

winstruct_plus
Creates Tivoli Application Management modules from AMS 2.0-compliant files produced by the Tivoli Module Builder. This command is packaged with the Tivoli Management Framework product.

When invoked, winstruct calls the subcommands in the order they are listed here.
Sequence of winstruct Calls

The `winstruct` main command calls from one to six `winstruct` subcommands, depending on which Tivoli tools are installed. When invoked, `winstruct` first calls a function in the `libamsi` shared library. The function returns a list of installed tools. The `winstruct` command then calls appropriate subcommands.

The following diagram shows the sequence of `winstruct` calls:

```
Sequence of winstruct Calls
```

![Diagram showing the sequence of winstruct calls]

The `winstruct` command determines what needs to be done and delegates work to the subcommands, one for each management tool. Because `winstruct` and `winstruct_task` are a part of Tivoli Management Framework, `winstruct` always calls `winstruct_task` first. The remaining subcommands are called in the order shown in the diagram. The `winstruct_plus` subcommand is always the last called because it typically depends on data objects created by other subcommands.
Using the winstruct Command

The subcommands receive the options and values entered with the main command.

winstruct Command Options

The winstruct command and subcommands accept the following options, some of which are optional:

<table>
<thead>
<tr>
<th>option</th>
<th>Req'd</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>–a amp_file</td>
<td>Yes</td>
<td>Specifies the path and file name of an AMP.</td>
</tr>
<tr>
<td>–s staging_area</td>
<td>Yes</td>
<td>Specifies a directory into which the winstruct command extracts the contents of the AMP.</td>
</tr>
<tr>
<td>–t tag_name</td>
<td>No</td>
<td>Specifies an administrator tag. Unique administrator tags enable the instructing of multiple versions of an AMP. The default tag name is Default.</td>
</tr>
<tr>
<td>–D variable=value</td>
<td>No</td>
<td>Specifies an arbitrary variable and its value.</td>
</tr>
</tbody>
</table>

For the complete syntax, descriptions, and examples for the winstruct command set, see the Tivoli Management Framework Reference Manual.

–a Option

The –a option specifies the path and file name of an AMP. The AMP is a compressed file that contains application description files and management software for a single management-ready application. Developers create AMPs with AMS 2.0-compliant tools, such as Tivoli Module Builder and Tivoli Module Designer. The winstruct command set creates data objects in the Tivoli environment by using the management information in the AMP.

Management software can include scripts and executable files for installing the application, monitoring it, and executing tasks. In addition
to creating description files, the Tivoli Module Builder or Tivoli Module Designer creates the AMP file by compressing the files together with the management software.

An AMP can also contain the source files that make up the application. However, these files are not required parts of the package because you can specify an alternate source location on the `winstruct` command line. For example, a commercial application such as Lotus Notes typically does not have its installation image or program binaries in the AMP. The developer who creates the AMP uses the software distribution sections of the description files to refer to the Lotus Notes files. When you issue the `winstruct` command, you specify the location of the files as a command line option (see the “–D Option” on page 11-14 for more information). In contrast, the source files for an internally developed application (such as a payroll system) can be stored in the AMP. The –a option is required.

### –s Option

The –s option specifies a staging area directory. The `winstruct` command uncompresses the contents of the AMP into the staging area. The Tivoli management tools retrieve management information from files in the staging area. To prevent confusion about which file a management tool must use, the application object file (.aof) in each AMP maintains a list of files related to the AMP’s application. Management tools first consult the .aof before accessing other files in the staging area.

The –s option is required.

### –t Option

The –t option specifies a unique identifier that distinguishes multiple copies, or versions, of a management-ready application. The identifier is also referred to as an administrator’s tag. Multiple versions permit more than one instruction of the same application. For example, a developer can create different AMPs for versions of an application that runs on various platforms. The developer assigns different administrator tags to each AMP. You use the –t option to distinguish between the different versions.

The –t option is optional.
Using the winstruct Command

–D Option

The –D option specifies the name of an arbitrary variable and its value in the following format:

variable=value

where variable is any name for the variable and value is its value. Similar to modifying the PATH environment variable, this option provides Tivoli Management Framework with a persistent value for a variable.

For example, you can use the –D option to specify the location of the source files that make up a management-ready application:

–D src_loc=/cdrom

In this example, src_loc is the name of a variable that the developer created in the application description files. The /cdrom value is a mounted drive specification for your CD-ROM drive. The developer must give you the variable name upon delivering the AMP. However, the value, /cdrom, is arbitrary; you decide the location of the source files, such as a CD-ROM or a shared file system. As winstruct processes the AMP, the command creates files packages for Tivoli Software Distribution. The file packages indicate the mounted drive as the source location for the application files. When you distribute the files, the Microsoft Exchange CD-ROM must be in the mounted drive.

You can specify multiple variable and value pairs, but you must enter the –D option for each pair. Tivoli Management Framework and the management tools all receive the same variables passed with –D, but each tool uses only those variables that apply to the tool. The management tools ignore irrelevant variables. In the previous example, Tivoli Software Distribution uses the source location when distributing an application, but other tools with no need for the source files ignore this variable.

The –D option is optional.

Uses for winstruct

Although it is possible to invoke a single subcommand, the winstruct main command is designed to be the only command users execute to
Using the winstruct Command

instruct the Tivoli environment. You typically instruct the environment in the following situations:

■ Receipt of a management-ready application
■ Installation of a new Tivoli core application
■ Failure of a tool, which requires repeated instruction
■ Invocation of a single subcommand

Receipt of a Management-Ready Application

Typically, an AMP is supplied through one of the following methods:

■ Tivoli distribution channels
■ Value Added Resellers (VARs), system integrators, or other third-party developers
■ In-house developers

Upon receipt of a new management-ready application, you issue the winstruct command, specifying the application’s AMP as an option. See “Using an Example AMP” on page 11-19 for a description of the effect winstruct has on the Tivoli Management Framework and management tools.

Installation of a New Tivoli Management Tool

When the Tivoli environment receives a new management tool that supports AMS 2.0, you must issue the winstruct command. This step instructs the new management tool with the information contained in an AMP. You must repeat the process of instructing the new tool for each AMP in the environment.

The winstruct command and subcommands create Tivoli data objects, such as policy regions, profile managers, and profiles. These objects remain in the environment until you use a Tivoli tool to remove them. The winstruct commands do not overwrite the data in the object with each invocation. This design feature, referred to as iterative instruction, allows you to instruct the environment repeatedly without risk of losing previous instructions. For example, suppose you install Tivoli Inventory sometime after instructing the environment. Issue the winstruct command for each AMP in the environment. The main command calls
Using the winstruct Command

the subcommands, which add data specific to the Tivoli Inventory tool without overwriting objects already existing for the other Tivoli tools. See “Invocation of a Single Subcommand” on page 11-16 and “Iterative Instruction” on page 11-18 for more information.

Failure of a Tool Requiring Repeated Instruction

If a management tool experiences problems during an instruction, winstruct continues with the next tool. You must repair the tool error, and then repeat the instruction process, using the main winstruct command. The winstruct design accounts for this kind of iterative instruction by ignoring tools that have already been processed.

The winstruct command does not pop up messages in response to errors. You must confirm each winstruct session by checking notification groups in the Tivoli desktop; any errors reported in the groups. See “New Notification Groups” on page 11-9 for more information about how winstruct creates and manages notices.

Invocation of a Single Subcommand

Although the winstruct main command is designed as the only command you need for instructing the Tivoli environment, it is still possible to enter a single subcommand. For example, suppose you receive an updated AMP for an application that is already distributed. In addition to the original management information (such as file package data), the AMP contains new monitors. You want the monitors, but you do not want to create file packages again. In this case, you can issue the winstruct_monitor subcommand to instruct only the Tivoli Distributed Monitoring tool.

The ability to invoke a single subcommand is potentially useful, but Tivoli cautions against this method in general practice. The risk of missing information stored in an AMP is high. Using the previous example, you saved time by foregoing the file package information, but you might have missed subtle changes related to management tools other than the targeted Tivoli Distributed Monitoring tool. For example, you might miss new response tasks for the monitors because the tasks are defined by the winstruct_task subcommand.
Additional Steps after Using winstruct

The `winstruct` command might require additional procedures or accommodations, depending on the characteristics of your Tivoli installation. For example, if the Tivoli Enterprise Console product is installed, you must stop and start the Tivoli Enterprise Console server after the `winstruct` process completes. Also, to subscribe endpoints to an application’s profile manager, you must create dataless profile managers.

You might need to issue the `winstruct` command more than once for a single application. For example, if a Tivoli management tool fails during a session, you must issue `winstruct` again. Also, if you later add a tool, you must issue `winstruct` again to load the new tool with application data.

Stopping and Starting the Tivoli Enterprise Console Server

Following an instruction process, the Tivoli Enterprise Console server must be stopped and restarted for any Tivoli installation that includes the Tivoli Enterprise Console product. (If the Tivoli Enterprise Console product is not installed, `winstruct` skips the `winstruct_event` subcommand.) During an instruction, the `winstruct_event` subcommand adds new event classes to all existing rule bases in the Tivoli Enterprise Console environment. The Tivoli Enterprise Console product does not recognize these event classes until the server is stopped and restarted. During startup, the Tivoli Enterprise Console product receives the rule base changes.

Administrators can choose when to restart the Tivoli Enterprise Console server. For example, if the new event classes are not immediately required, and the Tivoli Enterprise Console product is busy handling events, an administrator might wait until activity lessens. The Tivoli Enterprise Console product’s `wstopesvr` and `wstartesvr` commands stop and start the server.
Subscribing Endpoints

In addition to other types of data objects, the \texttt{winstruct} commands create profiles managers. The commands do not, however, create dataless profile managers. Endpoints cannot be assigned (that is, subscribed) to a profile manager unless it is dataless. Because of this requirement, you must take the following extra steps after a \texttt{winstruct} session:

1. Create a dataless profile manager.
2. Subscribe endpoints to the dataless profile manager.
3. Subscribe the dataless profile manager to the profile manager created by \texttt{winstruct}.

See the \textit{Tivoli Management Framework Planning for Deployment Guide} for more information about endpoints. See “Data Objects” on page 11-8 for the list of Tivoli data objects that \texttt{winstruct} creates.

Iterative Instruction

The \texttt{winstruct} command must be invoked again to complete an instruction if either of the following events occur:

- A Tivoli management tool experiences problems during an \texttt{winstruct} session.
- A new management tool is installed.

Each successfully instructed management tool ignores repeated instructions about a given application component. The \texttt{winstruct} commands never overwrite data objects. This design feature permits a repeated \texttt{winstruct} session to continue for the remaining uninstructed tools without interfering with completed instructions. The term for this procedure is iterative instruction.

If data objects created during a previous instruction have been deleted or renamed, a subsequent \texttt{winstruct} call creates the objects again. For example, if a task library is created during an instruction, users can delete or rename the library, and then execute \texttt{winstruct} again. The command creates the original task library again.
Using an Example AMP

The following example illustrates how to use an AMP with the `winstruct` command, and the effect it has on Tivoli Management Framework. In this case, the AMP contains management data for the commercial Microsoft Exchange application. The example assumes a developer has created the AMP and delivered it to you, the system administrator. The developer has also directed you to use a specific variable with the `-D` option when invoking `winstruct`.

The first step is to invoke the `winstruct` command. After the process finishes creating data objects, the Tivoli management tools that received data are available for use in the management of the Exchange application. The following subsections describe how to invoke `winstruct`, subscribe notice groups, and distribute and monitor the application.

Invoking winstruct

Before starting the `winstruct` process, you must choose a directory to serve as the staging directory. This directory is the storage area that holds the contents of the AMP when `winstruct` uncompresses the file. Another preparatory step is determining the source location variable for the `-D` option.

Because the Exchange application is too large to include in the AMP, the developer must specify a source location variable for the Exchange CD when creating the application description files. In this example, the variable name specified by the developer is `src_loc`, and your CD-ROM drive is mounted on `/cdrom`.

Enter the `winstruct` command, specifying the path and file name of the AMP, the path of the staging directory, and the source location variable:

```
winstruct -a /data/amps/exchange.amp -s /apps/staging \ 
-D src_loc=/cdrom
```
The command processes the data, adds it to the Tivoli database, and represents the data objects with a series of icons on the Tivoli desktop, as shown in the following figure:

The `winstruct` command creates the `Applications_adrastea–region` policy region on the main desktop. In this example, `adrastea` is the name of the host. This policy region contains the `PR_Exchange_Default_adrastea–region` subpolicy region. The desktop contains only one Applications icon, but it can hold multiple subpolicy regions for each new AMP you add to Tivoli Management Framework. In this example, the Exchange policy region is the first and only application in the environment.

The Exchange policy region contains several icons representing the profile managers and task libraries related to the application components. In this example, the AMP does not include dependency libraries because the developer did not define dependency checks for any of the components.
Subscribing Notice Groups

In the following example, `winstruct` creates two notice groups: **Application Management** and **Exchange**. The first is the general group for all applications you instruct in the Tivoli environment. Subsequent `winstruct` sessions do not create additional **Application Management** notice groups. The second group, **Exchange**, is specific to the application. For each new application you instruct, `winstruct` creates a new notice group. These notice groups contain logging and error information related to the `winstruct` processing for each application.

You must subscribe the application notice groups to an administrator, such as the Tivoli root administrator. To do so, right-click the administrator’s icon and select **Edit Notice Group Subscriptions** from the menu. The **Set Notice Groups** window is displayed:

![Set Notice Groups Window]

Move the **Applications Management** and **Exchange** groups to the **Current Notice Groups** box; then click the **Change and Close** button.

Distributing the Application

Before distributing the application, you must also subscribe endpoints. See “Subscribing Endpoints” on page 11-18 for more information.
The Exchange AMP contains several profile managers, one for each component that specifies either file packages, monitor collections, or both. File packages are data objects related to Tivoli Software Distribution. Monitor collections are related to Tivoli Distributed Monitoring.

Distribute the application components by first opening the profile manager icon, and then opening the file package. For example, when you click the profile manager for the **Application Tools** component, the **Profile Manager** dialog is displayed with a file package listed:

When you click the **FP_Exchange_4.0_Default_Application Tools (NT)_1.0.0_adrastea-region** icon, the **File Package Properties** dialog is displayed:
This dialog is a part of the Tivoli Software Distribution management tool. The files in the **Source Directories & Files** scrolling list are specified in the Exchange AMP. The Software Distribution tool uses this data to distribute the **Application Tools** component. See the *Tivoli Software Distribution User’s Guide* for more information about file packages.

You must distribute all components in the application. In this case, the Exchange CD must be in your mounted drive, `/cdrom`. The AMP for the Exchange application consists of four components, three of which contain file packages. For each of the three components containing file packages, you should open the profile manager icon, and then the file package icon. Then use the Tivoli Software Distribution dialogs and windows to specify targets and install the application.

The fourth component contains a monitor collection. The monitors are used to maintain both the application and the systems where it is installed.
Monitoring the Application

The Exchange 4.0 component contains a monitor collection. When you click the PM_Exchange_4.0._Default_Exchange_4.0._adrastea–region profile manager, the Profile Manager dialog is displayed with a monitor collection listed:
Troubleshooting a winstruct Session

When you click the SN_Exchange_4.0_Default_Exchange_4.0_adrastea-region icon, the Tivoli Distributed Monitoring Profile Properties dialog is displayed:

This dialog is a part of the Tivoli Distributed Monitoring management tool. The listed monitors are specified in the Exchange AMP. In managing an application, you can review, change, remove, and distribute any of these monitors. See the Tivoli Distributed Monitoring User’s Guide for more information about working with monitors.

Troubleshooting a winstruct Session

A successful winstruct session requires the application’s management data to satisfy certain conditions. The developer who creates application description files must do the following:

■ Specify source locations with the proper syntax
■ Specify versions for operating systems
■ Use correct naming conventions for monitors and tasks

If you receive an AMP that does not meet these requirements, return it to the developer for corrections.
Troubleshooting a winstruct Session

Specifying Source Locations

Developers specify the source files that make up a managed application when creating the application description files. The specification includes the file name and the location where the files are stored—that is, the source location. If the application is compressed as part of the AMP, the source location is the staging directory. If the application is too large to add to the AMP, the source location can be another directory or drive. For example, a large commercial application, such as Microsoft Exchange, typically ships on a CD. The source location could be a CD-ROM drive or a shared directory that holds a copy of the CD.

When you invoke the winstruct command, you specify the type of source location by using either the –s or –D option, or both. If the AMP contains the application files, use the –s option to uncompress the files into the staging directory. If the AMP does not contain the application files, use the –D option with the specific variable supplied by the developer.

During the winstruct process, the command creates file packages for Tivoli Software Distribution. The file packages contain the specified files, provided the developer adequately identified the source location. The developer indicates the source location when defining data for application description files. If the developer defines the source location for a file as type Unknown (an AMS 2.0 option), winstruct does not add the file to the file package. Later, when you distribute and install the application, it will be missing any files not included in the file packages.

Problems with an incomplete distribution might not be apparent until you begin using the application. A likely symptom is an error message from the application indicating missing files. If your AMP requires the –D option, verify with the developer that you used the correct variable (or variables). Also, look for notices in the application’s notification group. If you suspect that the application description files contain an invalid specification for a source location, return the AMP to the developer for review.

Specifying Versions for Operating Systems

Developers can define tasks, monitors, and queries for an application component. The Tivoli management tools require details about the
operating systems on which the objects will run. The details include platform type and version, or range of versions. Developers must include version information about each operating system on which tasks, monitors, and queries will run.

**Naming Monitors and Tasks**

When developers define tasks and monitors, they name them. The names for monitors must consist of alphabetic characters only; no numbers, spaces, or special characters (punctuation marks, spaces, underscores, hyphens, and so on) are allowed. The names for tasks are less restrictive, but cannot contain spaces.
Distribution Management

Multiplexed distribution is the general distribution mechanism used by Tivoli Enterprise applications to distribute large amounts of data to multiple systems within a Tivoli management region and across region boundaries. Tivoli Management Framework provides two multiplexed distribution services, MDist and MDist 2.

For an in-depth discussion of multiplexed distribution services—how they work, how they differ, and how to design a repeater hierarchy, see the *Tivoli Management Framework Planning for Deployment Guide*. This chapter explains how to create and configure repeaters for optimal performance in your Tivoli environment. It also focuses on how to use graphical user interfaces (GUIs) available only to Tivoli applications using the MDist 2 service.

**Before Using Multiplexed Distribution**

Before you submit a distribution using either the MDist or MDist 2 service, it is important to complete the following tasks:

1. Design a repeater hierarchy that meets the networking needs of your Tivoli environment. For information about how to set up a repeater hierarchy for maximum network efficiency, see the *Tivoli Management Framework Planning for Deployment Guide*.

   **Note:** To determine which service your application uses, consult the information that came with your application.
Creating a Repeater

2. Create and configure repeaters in your repeater hierarchy. An application can use only one MDist service for each distribution; however, both MDist and MDist 2 services share the same repeater hierarchy and can be active at the same time. Therefore, if your applications use both services, you must configure a repeater for both MDist and MDist 2 services.

3. If your application uses the MDist 2 service, install the following components to take full advantage of its functionality:
   - A database to store distribution and target status. Without this database, your Tivoli application (not MDist 2) must track when distributions are completed.
   - The Tivoli Distribution Control console, which provides administrators with real-time reporting and control of software distribution.
   - The Tivoli Mobile Computing console, which provides end users on Windows systems with notification of pending distributions and enables them to control distributions sent to their computers.

Notes:
- For installation information about MDist and MDist 2, see the Tivoli Enterprise Installation Guide.
- For disk space requirements and configuration information for the MDist 2 database, see the Tivoli Management Framework Release Notes.

Creating a Repeater

Repeaters relay the distribution, collect status, and return status to the Tivoli management region server (Tivoli server), as well as offset the network load on other repeaters. The procedure for creating a repeater is the same whether your application uses MDist or MDist 2. Create a repeater when you set up your repeater hierarchy or service additional targets in your Tivoli management region. You can create a repeater in the following ways:
   - Use the wrpt command to create a repeater on a managed node.
Creating a Repeater

- Automatically create a repeater when you create a gateway. For information about creating a gateway, see the *Tivoli Enterprise Installation Guide*.

Repeaters on gateways and managed nodes differ as shown in the following table.

<table>
<thead>
<tr>
<th>Repeater on:</th>
<th>Function</th>
<th>Can send MDist distributions to:</th>
<th>Can send MDist 2 distributions to:</th>
<th>Log file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managed node</td>
<td>Exit if their queue is empty after 20 minutes.</td>
<td>Repeaters and managed nodes</td>
<td>Repeaters</td>
<td>$DBDIR/rptlog</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(only MDist 2)</td>
</tr>
<tr>
<td>Gateway</td>
<td>Always up and running as part of the gateway.</td>
<td>Repeaters, managed nodes, and endpoints</td>
<td>Repeaters and endpoints</td>
<td>$DBDIR/gatelog</td>
</tr>
</tbody>
</table>

**Notes:**

- If you create a gateway on a managed node that is currently configured as a repeater, the repeater inherits the gateway’s repeater configuration settings.
- A repeater depot and queue are automatically created when you create a repeater. These components, used by MDist 2, are discussed in the *Tivoli Management Framework Planning for Deployment Guide*.

The following table provides the context and authorization role required to create a repeater on a managed node:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a repeater</td>
<td>TMR</td>
<td>senior or super</td>
</tr>
</tbody>
</table>

To create a repeater on a managed node, follow these steps.
Creating a Repeater

Note: You also can use the wrpt command after a repeater has been created to change the existing range of a repeater on managed nodes and gateways. For information about wrpt, see the Tivoli Management Framework Reference Manual.

1. To create a repeater, enter the following command:

   \texttt{wrpt -n repeater\_name range=value}

   where \texttt{repeater\_name} is the name of the repeater and \texttt{value} specifies the dispatcher numbers in the distribution range for the new repeater.

   Notes:
   
   • To obtain a dispatcher number, enter the following command:
     \texttt{odadmin odlist}
   
   • Specify the range values in ascending order.
   
   • To specify multiple nonconsecutive dispatcher numbers, separate each number with a comma, such as \texttt{range=5,7,33}.
   
   • To specify multiple consecutive dispatcher numbers, enter a range of dispatcher numbers, such as \texttt{range=5–7,33,35–38}.

   Because the Tivoli management region server is a repeater by default, this server can distribute data to the new repeater. In turn, the repeater distributes the data to the targets specified in \texttt{range=value}.

2. To verify that the repeater was created successfully, enter the following command:

   \texttt{wrpt}

   The system displays the host numbers for all repeaters, gateways, and managed nodes in a region.

   Output similar to the following is displayed:

   \texttt{lazzaro [1] wd-- []}
where **lazzaro** is the repeater name, **1** is the dispatcher number, and **wd** indicates that the host is the default repeater in a wide area network (WAN).

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 management region, you must configure a repeater’s settings for both services.

### Configuring a Repeater

This section describes how to configure repeaters for MDist and MDist 2 services.

#### MDist Service

To configure a repeater for efficient MDist distributions, Tivoli Management Framework provides a number of 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a repeater for MDist</td>
<td>TMR</td>
<td>senior or super</td>
</tr>
</tbody>
</table>

To configure a repeater for MDist, use the following command syntax:

```
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 pid. To obtain pid (a
Configuring a Repeater

unique process number of an active distribution), enter
the following command:

\texttt{wrpt \ -L}

\textit{name}  Specifies the label, object ID, or managed node ID of
the repeater.

\textit{reinit}  Resets options to their default values.

\textit{–t}  When no other options are listed, returns the
configurations currently in use.

\textit{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. See the following
sections for descriptions of the keywords. You can
specify more than one keyword and value.

The following sections describe the keywords and values for the \texttt{wrpt}
command. For more information about the \texttt{wrpt} command, see the
\textit{Tivoli Management Framework Reference Manual}.

Setting Network Load

Use the \texttt{net_load} keyword to set the maximum amount of data (in
kilobytes per second [KBps]) that the repeater sends to the network for
each distribution. If you set \texttt{net_load} to 50, each distribution limits itself
to writing no more than 50 KB in 1 second. There is no connection
between independent distributions; therefore, if four distributions are
started by four different applications (at the same time), the total
network load could be four times the set value.

Notes:

- This keyword is dependent on your system’s performance. The
maximum \texttt{net_load} is 32 megabytes per second (MBps);
however, most systems cannot process data this fast.

- You can specify a negative value for \texttt{net_load} to enable the net
load for each target, rather than for the entire distribution. For
example, if you set \texttt{net_load} to –25, data transfers to each target
are limited to writing no more than 25 KBps.
Configuring a Repeater

Setting Network Spacing

Use the `net_spacing` keyword to specify a delay (in milliseconds) to insert between each write to the network. This is useful when you have slow network connections and you are concerned about flooding a single target. For most networks, this value is 0, indicating no delay. If network monitoring shows that MDist transfers are causing abnormally high collision rates, use this keyword to evenly space transfers when writes occur.

The `wrpt -t` command does not display a value for the `net_spacing` keyword unless you change the default configuration for a repeater.

Setting Timeout Values

Use the `stat_intv` keyword to specify the timeout value (in seconds) for repeaters on managed nodes after which a blocked connection is considered inactive. Some systems with unreliable networks experience network hangs that go undetected by the operating system Transmission Control Protocol/Internet Protocol (TCP/IP) stack. The high-level TCP timeout forces a timeout error on these connections so that the distribution can proceed.

**Note:** This keyword is only for repeaters on managed nodes. Use the `wgateway` command to set session timeout values for repeaters on gateways.

Setting Maximum Simultaneous Connections

Use the `max_conn` keyword to set the maximum number of simultaneous connections initiated by the repeater during a distribution. A repeater can distribute in parallel to any number of targets. This keyword sets a limit on the maximum number of connections; therefore, the repeater distributes in parallel to subsets of the targets in its range. This prevents the number of network connections from exhausting system limits. As soon as the distribution to a target is complete, the repeater opens a connection to the next target.

Setting Maximum Memory and Disk Space

Use the `mem_max` and `disk_max` keywords to specify values for maximum amounts of memory and disk-space system resources that can
be allotted to a repeater during a distribution. If targets accept data at the same rate that the repeater sends data, the repeater consumes very little memory. If the repeater has one slow target, the repeater attempts to keep the data flowing to the fastest targets.

To service both slow and fast targets, the repeater must temporarily save data for the slow targets. The repeater first uses memory up to the maximum amount specified in mem_max. When the maximum amount of memory has been used, the repeater starts paging data to disk. The repeater uses disk space up to the maximum amount specified in disk_max. When both the memory and disk limits are reached, the repeater stops receiving data. This stoppage appears as a slow target to its parent repeater and can its effect can ripple all the way up the distribution hierarchy to the source.

If the number of targets is greater than the number of maximum connections, the repeater must store all the data so that it can be sent to the remaining targets after the connection completes. The repeater stores the data in memory, up to the value specified in mem_max. If the data exceeds that value, the repeater stores the remainder of the data on disk, up to the value specified in disk_max. This means that if mem_max plus disk_max is not large enough to hold the largest possible distribution, you need to configure additional repeaters.

**Setting Paging Space, Disk Usage Rate, and Disk Delays**

Use the disk_dir, disk_hiwat, and disk_time keywords to specify temporary paging space, speed with which disk space is used, and time delays between disk allocations, respectively. When a repeater exhausts the maximum memory allocated and starts paging to disk, the distribution slows down when it reaches the maximum disk space. Above this threshold, the distribution uses pages of disk space only at a specified interval. The disk paging file is created in a specified directory.

**Setting the Final Timeout**

Use the –T [seconds] keyword 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
Configuring a Repeater

final timeout value of 0 indicates that there is no final timeout for the repeater, meaning that it will wait forever.

MDist 2 Service

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 repeater 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a repeater for MDist 2</td>
<td>TMR</td>
<td>senior or super</td>
</tr>
</tbody>
</table>

To configure a repeater for MDist 2, use the following command syntax:

```
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
Configuring a Repeater

Tivoli management region with one command. For example, you can set the cache size for all repeaters in your Tivoli management 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.

For more information about the wmdist command, see the Tivoli Management Framework Reference Manual.

Setting Network Load and Target Network Load

Use the net_load keyword to specify the maximum amount of network bandwidth that a repeater can allocate. This value is shared among all active connections. For example, if there are 10 open connections, with net_load=500 (default value), each connection receives 50 KBps. MDist 2 can use these 10 open connections for one or more distributions.

Use the target_netload keyword with net_load to specify the maximum amount of network bandwidth that a repeater can send to an individual target. For example, suppose net_load is 500 KBps and target_netload is 100 KBps (default value). If there is only one connection, the target_netload value takes effect and limits the connection to 100 KBps. However, if there are 10 connections, the net_load value takes precedence and limits each connection to 50 KBps. Because 50 KBps is less than the target_netload of 100 KBps, this value also satisfies the 100 KBps value for target_netload.

Both net_load and target_netload can be active at the same time. This is different from the MDist service’s negative net_load value, which offers no control on the total bandwidth.

Setting Timeout Values

Use the send_timeout keyword to specify the timeout between network writes. That is, a target has send_timeout seconds to receive a packet on the network. If a timeout occurs, the distribution remains in the repeater queue and attempts to resend the distribution as set by
Configuring a Repeater

**conn_retry_interval.** The default value is 300 seconds. This keyword replaces the gateway `session_timeout` keyword used by MDist.

Use the **execute_timeout** keyword to specify the timeout between when all the data is sent and the method returns. For example, applications might be running scripts after receiving data but before returning results to the repeater. The default value is 600 seconds. This keyword replaces the **final_timeout** keyword used by MDist.

### Setting Maximum Priority Connections

Use the **max_sessions_high**, **max_sessions_medium**, and **max_sessions_low** keywords to control the number of connections that the repeater can open for each priority (high, medium, or low). If no connections are available for a given priority, the repeater tries to borrow a connection from a lower priority. For example, if **max_session_high**=3 and all three high-priority connections are in use, the repeater tries to use a lower-priority connection that is available. The sum of high, medium, and low connections is the total number of available connections.

Repeater queues operate on a first in, first out (FIFO) basis. A repeater assigns a distribution to its queue based on which distribution arrives first, not when the distribution was submitted. For example, suppose that a medium priority distribution is using all the medium and low priority connections. If a high priority distribution arrives, and all high priority connections are in use, the repeater can use lower-priority connections for this distribution as soon as a medium or low priority connection becomes available. The original medium priority distribution is blocked until the high priority distribution has finished using the medium and low priority connections.

**Notes:**

- You must restart the repeater for any changes to take effect. These keywords replace the `wrpt max_conn` command used by MDist.
- For more information about repeater queues, see the *Tivoli Management Framework Planning for Deployment Guide*. 
Configuring a Repeater

Setting Maximum Memory and Disk Space

Use the `disk_max` and `mem_max` keywords to specify the amount of memory and disk space allocated to the repeater depot. These values are shared among distributions, unlike the MDist wrpt keywords, which are targeted per distribution. The default size for `disk_max` is 500 MB. This is the total size of the depot. The depot contains both permanent and temporary distributions. All simultaneous distributions must fit within the depot space.

If the `disk_max` value equals zero, no limit is enforced. The depot cannot exceed the size of the disk. Every distribution flowing through a repeater is stored at least temporarily in the depot. The depot must be large enough to hold the largest distribution that you expect to distribute.

The `mem_max` keyword specifies the amount of memory used to buffer data being sent to targets. This improves performance by reducing the number of disk accesses to the depot. The memory is shared among all active distributions. The default size for `mem_max` is 64 MB. This is a memory cache used for all active distributions.

**Note:** You must restart the repeater for any changes to take effect. These keywords replace the `wrpt mem_max` and `wrpt disk_max` commands used by MDist.

Setting the Status Notification Interval

Use the `notify_interval` keyword to specify the frequency (in minutes) a repeater reports status. As targets finish, their results are buffered by the repeater. When the length of time set by `notify_interval` has elapsed or all the targets of this distribution have finished, the results are sent to the application using MDist 2. In turn, the application notifies the distribution manager to update the database. The `notify_interval` keyword’s default value is 30, meaning that each repeater sends status every 30 minutes. Status information is sent to the database infrequently to cut down on network traffic and overhead on the Tivoli management region server.

Setting the Connection Retry Interval

The `conn_retry_interval` keyword specifies the frequency (in seconds) that a repeater retries unavailable or interrupted targets (default value is
900 seconds). Between a gateway and its endpoints, the retry mechanism is to retry the number of seconds set by `conn_retry_interval` up to the number of seconds set by `retry_ep_cutoff`. Between repeaters, the retry mechanism is to retry the number of seconds set by `conn_retry_interval` until the distribution’s deadline is reached. Because repeaters do not log in to each other, MDist 2 performs an explicit retry to know when an unreachable repeater becomes available.

### Setting the Retry Endpoint Cutoff Interval

Use the `retry_ep_cutoff` keyword to specify the length of time (in seconds) that you want the repeater to continue retrying an unavailable or interrupted endpoint. A repeater retries unavailable or interrupted targets until the distribution’s deadline is reached. For example, the repeater only knows if an endpoint is unavailable when it tries to contact the target (when a connection becomes available). This information is sent to the distribution manager only after the length of time set by `notify_interval`.

If an endpoint is down, the repeater skips the endpoint, leaves the information in its queue, and waits for the target to log in. The repeater also retries the target the number of seconds set by `conn_retry_interval` (default value is 900 seconds) up to the number of seconds set by `retry_ep_cutoff` (default value is 7200 seconds).

After the number of seconds set by `retry_ep_cutoff` is reached, the distribution remains in the queue until the distribution deadline, waiting for the endpoint to log in.

### Setting the Packet Size

Use the `packet_size` keyword to specify the number of bytes written to the network during each distribution. The packet size specifies how many bytes are written to the network before the repeater pauses to enforce bandwidth control. For very slow networks, it is useful to lower the packet size to prevent flooding the network for long periods of time.

For example, suppose that the default packet size is 16 KB. For a slow network line on a 9600 baud modem, it takes approximately 17 seconds for the 16 KB to transmit. This means that the line is busy for 17 seconds before the repeater pauses. This could be a lengthy time if you were
Configuring a Repeater

trying to perform other operations on the connection. However, for fast networks, you can increase the packet size to get better performance. This is mainly for networks that support larger packet sizes, such as asynchronous transfer mode.

Setting the Debug Level

Use the `debug_level` keyword to control the number of log messages written to the log files of the managed node repeater located at `$DBDIR/rpt2log`. The debug level ranges from 0 (least information) to 9 (most information); the default is 3.

Logging for a repeater on a gateway is controlled with the `debug_level` keyword set with the `wgateway` command. For information about the `wgateway` command, see the *Tivoli Management Framework Reference Manual*.

Setting a Repeater's Depot Directory

Use the `wmdist –s rpt_dir=pathname` command 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’s queue.

**Note:** You must restart the repeater for any changes to take effect.

The default directories for the depot and states directories are `rpt_dir/depot` and `rpt_dir/states` respectively.

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

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure a repeater depot</td>
<td>TMR</td>
<td>senior or super</td>
</tr>
</tbody>
</table>
Troubleshooting

Setting Permanent Storage

Use the `wmdist -s permanent_storage` command 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`, a distribution’s 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set permanent storage in a repeater depot</td>
<td>TMR</td>
<td>senior or super</td>
</tr>
</tbody>
</table>

The following examples depict typical scenarios:

- To set `permanent_storage` to `TRUE` for all repeaters on your Tivoli management region server, 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`

Troubleshooting

This section lists suggestions and tips to help you troubleshoot problems that might arise using multiplexed distributions services:

- Log files are available for debugging purposes. These files will continue to increase in size unless you delete unwanted data and maintain the amount of information that gets logged. Use the following log files to debug data distributed using multiplexed distribution services. Note that `debug_level` on `wmdist` specifies a value from 0 (least information) to 9 (most information).
MDist 2 Consoles

• A gateway repeater’s log file is located in \$DBDIR/gatelog. To specify the amount of information logged in this file, enter the following command:

\texttt{wgateway gateway\_name set\_debug\_level debug\_level}

• A standalone repeater’s log file is located in \$DBDIR/rpt2log (for MDist 2 distributions only). To specify the amount of information logged in this file, enter the following command:

\texttt{wmdist -s debug\_level=value}

• A distribution manager’s log file is located in \$DBDIR/distmgr.log on the Tivoli management region server. To specify the amount of information that is logged in this file, enter the following command:

\texttt{wmdist -D [debug\_level]}

- To optimize the visibility of the Tivoli Distribution Status console, increase the screen resolution of your display to a minimum of 1024 x 768 pixels. You can select an option from the \texttt{View} menu to maximize the Distributions table or Distribution Details views.

Note: For information about how to maintain your Tivoli environment and troubleshoot problems that can occur during normal operations, see the \textit{Tivoli Management Framework Maintenance and Troubleshooting Guide}.

MDist 2 Consoles

This section provides an overview of the following consoles:

\textbf{Tivoli Distribution Status console}

Enables administrators to monitor the status of a distribution and take action, if necessary. Administrators can see which target nodes received the distribution, which experienced errors, and estimate when a distribution will finish.

\textbf{Tivoli Mobile Computing console}

Enables end users to control distributions sent to their Windows systems. This gives end users the ability to download and install distributions at their convenience. If the workstation disconnects at any time (such as in the middle of a download), when the user reconnects, operations resume where they left off.
Note: Administrators can retain control of distributions by sending hidden or mandatory distributions to an end user’s system. They also can limit console functionality; for example, disable the reject function.

These consoles are available to administrators using applications that use the MDist 2 service. For more information, consult the online help information provided with the consoles. For installation instructions, see the Tivoli Enterprise Installation Guide.

Tivoli Distribution Status Console

The Tivoli Distribution Status console provides administrators with real-time reporting and control of software distributions. Administrators can keep track of the progress of a distribution, intervene (if necessary), and analyze the details of a distribution graphically. The console provides color-coded charts and graphs to enable administrators to identify patterns and relationships in the data. These are helpful when identifying items of interest to be focused on, such as unavailable targets, which prevent a distribution from completing successfully.

Figure 12-1 illustrates the main parts of the console.

Figure 12-1. Tivoli Distribution Status console
MDist 2 Consoles

Note: To monitor status and control distributions, a database is required. For MDist 2 installation information, see the Tivoli Enterprise Installation Guide.

Starting the Console

Start the Tivoli Distribution Status console to keep track of a distribution, view its progress, and intervene, if necessary. You can log in to any Tivoli management region server (Tivoli server) or managed node that has the Tivoli desktop installed and access to the database.

Keep in mind that the Distribution Status icon on the Tivoli desktop appears on all desktops but is only available when the console is installed on the same system where the desktop is running. On UNIX systems, this is the system where you started the desktop. If you are running Tivoli Desktop for Windows, this is the system on which 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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start the Tivoli Distribution Status console</td>
<td>TMR</td>
<td>RIM_view or senior</td>
</tr>
</tbody>
</table>

You can start the Tivoli 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 system, you must enable connections to the X Window System on the UNIX 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 environment variable to the X Window System display on which to display the Tivoli 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 the following commands:

```
DISPLAY=zeus:0.0
export DISPLAY
```

2. Enable remote connections to the X Window System. For example, to start the Tivoli Distribution Status console on the `zeus` display, enter the following command:

```
xhost +zeus
```

- Ensure that remote logins are enabled on the system on which you start the console. To ensure that remote logins are enabled, enter the following command:

```
odadmin odinfo
```

The following message is displayed:

```
Remote client login allowed = value
```

where `value` is either `TRUE` or `FALSE`.

If `FALSE`, enter the following command to enable remote client logins:

```
odadmin set_allow_rconnect TRUE
```

**Desktop**

To start the Tivoli Distribution Status console from your desktop, follow these steps:

1. From the Tivoli desktop, double-click the **Distribution Status** icon. The login dialog is displayed.
2. In the login dialog, follow these steps:
   a. Type the name of the host machine on which the Tivoli Distribution Status console is installed. Do not type the IP address.
   b. Type your login name and password for that host. These fields are case sensitive.
   c. Click OK to display the Tivoli 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.

3. To view one or more distributions, select a query from the list in the upper-left pane.

**Command Line**

Use the `wmdistgui` command to start the Tivoli Distribution Status console from the command line. For installation instructions, see the *Tivoli Enterprise Installation Guide*.

To start the Tivoli Distribution Status console, follow these steps:

1. Source the appropriate setup file to ensure that your system environment is set correctly.

2. Enter the following command on the managed node where you plan to run the console:

   ```
   wmdistgui
   ```

3. In the login dialog, follow these steps:
   a. Type the name of the host machine on which the Tivoli Distribution Status console is installed. Do not type the IP address.
   b. Type your login name and password for that host. These fields are case sensitive.
   c. Click **OK** to display the Tivoli Distribution Status console.

4. To view one or more distributions, select a query from the list in the upper-left pane.

**Note:** For more information about `wmdistgui`, see the *Tivoli Management Framework Reference Manual*.
MDist 2 Consoles

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 task:

<table>
<thead>
<tr>
<th>Activity</th>
<th>Context</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>View one or more distributions</td>
<td>TMR</td>
<td>RIM_view or senior</td>
</tr>
</tbody>
</table>

You can view distribution status from the Tivoli Distribution Status console, command line, or a custom SQL script.

Tivoli Distribution Status Console

To view one or more distributions, select a query from the query list. For example, select All Distributions to display distributions in the Distributions table as shown.
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, see the Tivoli Management Framework Reference Manual.

Viewing Details of a Distribution

Use the Tivoli Distribution Status console to view details of a specific distribution. Simply 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 any given 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 distribution’s name. The distribution name also is displayed on the Distribution Details title bar as shown in Figure 12-2 on page 12-24.
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

The Status Chart view displays a color-coded pie chart representing the states of targets for a selected distribution. You can quickly 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 as shown.
Time Spent Chart

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

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

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 a better 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. Click View→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 as shown.

![Distribution Management](image)

6. To view information about a specific node, double-click the object. The **Node Properties** dialog is displayed.

![Node Properties](image)
Tivoli Mobile Computing Console

The Tivoli Mobile Computing console provides end users with notification and control of distributions sent to their Windows endpoints. This enables mobile users the flexibility to install distributions at their convenience.

Figure 12-3 illustrates 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.

Figure 12-3. Tivoli Mobile Computing console
Users can view distributions queued at the gateway, sort them by different criteria (size, priority, download time), 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.

Note: For instructions on how to perform these tasks in the console, consult the online help information.

The Tivoli Mobile Computing console also enables users to control distributions while in the process of downloading. 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 left off.
Keep in mind that although the console gives end 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 (see page 12-33).

*Hidden distributions* are automatically downloaded and run when its targets connect. The distribution is hidden in that the distribution is invisible to the end user. For example, an administrator might send an inventory scan that gathers information about hardware and software on a specific workstation.

In contrast to hidden distributions, end 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 Tivoli Mobile Computing console installed, consult the documentation that came with your Tivoli application.
Configuring the Console

After you install the console on specified endpoints, you can configure the console to set limitations on what tasks that your end users can and cannot perform. This is accomplished by editing the `mobile.cfg` file, installed on the endpoint in the system root directory:

- For Windows 98 systems:
  ```
  ..Tivoli/mobile/mobile.cfg
  ```
- For Windows NT and Windows 2000 systems:
  ```
  ..Tivoli/mobile/mobile.cfg
  ```

An example of the `mobile.cfg` file is as follows:

```ini
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
```

**Note:** These statements can be specified 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.

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 General tab is inaccessible to the user.

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.

confirmCancel
If TRUE, displays an “Are you sure?” prompt before rejecting a distribution. If FALSE, does not display a confirmation when the user rejects a distribution that is in the process of downloading.

connectionSpeed
Specifies the dial-up connection of your computer so that the console can accurately determine the download time of a distribution. The default value is 56 KB.

depotDirectory
Specifies the storage directory where distributions are downloaded for installation at a later date.

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.

**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 (0–4) in the **mobile.log** file.

**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 (0–4) in the **mobile.log** file.

**logsize**
Specifies the maximum size in KB of the **mobile.log** file. The **mobile.log** file is located in the directory where you installed the Tivoli 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 end 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 (from 1 to 30 minutes) that the console checks to see if your computer has reconnected. The default value 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.
showMessage If TRUE, notifies the end user with a visual prompt when the console detects a new distribution. If FALSE, this pop-up window is not displayed.

upcallTimeout Specifies the repeater timeout, which is the length of time (from 30 seconds to 5 minutes) that the console waits for the gateway to return the list of waiting distributions or start a distribution. The default value 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 Console

To use the Tivoli Mobile Computing console, the administrator first must issue the `wep set login_mode` command to designate the endpoint as mobile. This allows an end user to receive and control MDist 2 distributions through the Tivoli Mobile Computing console. For information about installing and enabling an endpoint for mobile computing, see the *Tivoli Enterprise Installation Guide*.

To start the console after it is installed, double-click the Tivoli Mobile Computing icon on your Windows desktop or the Windows taskbar:

Note that the taskbar icon changes to the following icon when there is a pending distribution:

You also can access the console from the pop-up dialog, the **Start** button, or add the console to the Windows **Startup** folder so that the console opens each time you start your operating system.
Glossary

A

application management package

See AMP.

AMP

A compressed file in the Java JAR format. An AMP contains all the description files for an application.

application description files

Files that describe an application, list and call other description files, and provide data necessary to manage an aspect of an application.

authorization roles

A role assigned to Tivoli administrators to enable them to perform their assigned systems management tasks. A role may be granted over the entire Tivoli management 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 primary mechanism by which the Tivoli Management Framework and Tivoli applications communicate with Tivoli administrators. The bulletin board is represented as an icon on the Tivoli desktop through which the administrators can access notices. Tivoli applications use the bulletin board as an audit trail for important operations that the administrators perform.
C

**collection**
A container that groups objects on a Tivoli desktop, thus providing the Tivoli administrator with a single view of related resources. Either Tivoli Management Framework or a Tivoli administrator can create a collection. The contents of a collection are referred to as its members. Examples of collections include the administrator collection, the generic collection, and the monitoring collection; the administrator collection being an example of one generated by the Tivoli Management Framework.

**configuration repository**
In the Tivoli environment, the relational database that contains information collected or generated by Tivoli applications. Following are examples of the information stored in the configuration repository:
- Tivoli Inventory — Stores information concerning hardware, software, system configuration, and physical inventory
- Tivoli Software Distribution — Stores information concerning file package operations
- Tivoli Enterprise Console — Stores information concerning events

D

**default policy**
A set of resource property values assigned to a resource when the resource is created.

**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 invocation, or call, from the Tivoli management region server or gateway “down” to an endpoint.

E

equipment

(1) A Tivoli client machine running an endpoint service (or daemon). Typically, an endpoint communicates only with its assigned gateway and is not used to perform daily management operations.
(2) Any managed resource representing the final destination for a profile distribution. Tivoli Distributed Monitoring also uses proxy endpoints, which are representations for non-Tivoli entities (such as a network devices or hosts) that subscribe to Tivoli Distributed Monitoring profiles. A Tivoli administrator associates each proxy endpoint with a managed node; however, several proxy endpoints can be associated with a single managed node.
(3) In the Tivoli environment, a managed node or SQL server on which a task is run.

equipment client

See endpoint.

equipment gateway

See gateway.

equipment list

A list of all endpoints in the Tivoli management region and their assigned gateways. This list is maintained by the endpoint manager.

equipment manager

A service on the Tivoli server that controls and configures gateways and endpoints, assigns endpoints to gateways, and maintains the endpoint list.
endpoint method
A method that runs on an endpoint as the result of a request from other managed resources in the Tivoli management region. Results of the method are forwarded to the gateway and then to the calling managed resource.

event repository
In the Tivoli environment, the relational database in which the Tivoli Enterprise Console product stores Tivoli Enterprise Console events.

F

fanout
In communications, the process of creating copies of a distribution to be delivered locally or sent over the network.

G

gateway
A service running on a managed node that provides all communications between a group of endpoints and the rest of the Tivoli environment. The gateway also has the multiplexed distribution repeater functionality built in, enabling it to act as the fanout point for distributions to a very large number of endpoints.

gateway method
A method that runs on the gateway’s proxy managed node on behalf of the endpoint. Results of the method are forwarded to the calling managed resource.

I

instance
A single occurrence of a resource.
J

job

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 execute.

K

Kerberos

The security system of the Massachusetts Institute of Technology’s Project Athena. The system uses symmetric key cryptography to provide security services to users in a network.

Kerberos master machine

In Kerberos, the host machine on which the Kerberos database resides.

Kerberos master password

In Kerberos, the password required to change or access the Kerberos database.

Kerberos principal

In Kerberos, a service or user that is known to the Kerberos system. See also principal name.

Kerberos realm

In Kerberos, a set of managed nodes that share the same Kerberos database.

M

managed node

Any managed resource on which Tivoli Management Framework is installed.
managed resource
In the Tivoli environment, any hardware or software entity (machine, service, system, or facility) that is represented by a database object and an icon on the Tivoli desktop. Managed resources are subject to a set of rules and must be a supported resource type in a policy region. Managed resources include, but are not limited to, managed nodes, task libraries, monitors, profiles, and bulletin boards.

MDist
A multiplexed distribution service provided by Tivoli Management Framework that enables efficient transfer of data to multiple targets. In contrast to MDist, another multiplexed 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. In contrast to MDist 2, another multiplexed distribution service, MDist, lacks these management features. See also Distribution Status console.

member
The contents of a collection. Examples of collections include the administrator collection, the generic collection, and the monitoring collection; the administrator collection being an example of one generated by the Tivoli Management Framework.

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.
name registry
A name service consisting of a two-dimensional table that maps resource names to resource identifiers and corresponding information within a Tivoli management region.

notice
A Tivoli 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
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 administrator's bulletin board contains only the notices that reside in a notice group to which the administrator is subscribed.

NT repeater
The first Windows NT machine on which the Tivoli Remote Execution Service is installed. Using fanout, the NT repeater distributes the Tivoli Remote Execution Service to all other Windows NT clients during the client installation process.

object path
An absolute or relative path to a Tivoli object, similar to a path in a file system.

object reference
The object identifier (OID) given to an object during its creation.
**oserv**

The name of the CORBA-compliant object request broker used by the Tivoli environment. The `oserv` runs on the Tivoli management region server and each of its clients.

**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. Tivoli administrators use policy regions to model the management and organizational structure of a network computing environment. The administrators can group similar resources as well as define access to, control, and associate rules for governing them. The policy region contains resource types and the list of resources to be managed. A policy region is represented on the Tivoli desktop by an icon that resembles a domed building. When a Tivoli management region is created, a policy region with the same name is also created. At that point, the region contains only one policy region. However, a Tivoli administrator can create other policy regions and subregions to represent the organization of the Tivoli management region.

**Note:** A Tivoli management region addresses the physical connectivity of resources; a policy region addresses the logical organization of resources.

**policy subregion**

A policy region created or residing in another policy region.

**principal name**

A name by which the Kerberos principal is identified. The principal name consists of three parts: a service or user name, an instance name, and a realm name.
principal password
The password that corresponds to the principal name. This password is used to authenticate services and users to each other.

profile
A container for application-specific information about a particular type of resource. A Tivoli application specifies the template for its profiles; the template includes information about the resources that can be managed by that Tivoli application. Following are some examples of profiles:
- In Tivoli Distributed Monitoring, a monitor
- In Tivoli Software Distribution, a file package
- In Tivoli User Administration, a user or group profile
A profile is created in the context of a profile manager, which links the profile to a Tivoli resource (for example, a managed node) that uses the information contained in the profile. A profile has no direct subscribers.

profile manager
A container for profiles that links them to a set of resources, called “subscribers.” Subscribers can be managed nodes or other profile managers. A profile manager can contain (a) profiles of multiple types or (b) multiple profiles of the same type. Tivoli administrators use profile managers to organize and distribute profiles. A profile manager is created in the context of a policy region and is a managed resource in that policy region. See also subscription list.

proxy endpoint
In Tivoli Distributed Monitoring, representations for non-Tivoli entities (such as a network devices or a hosts) that subscribe to Tivoli Distributed Monitoring profiles. A Tivoli administrator associates each proxy endpoint with a managed node; however, several proxy endpoints can be associated with a single managed node.

pull
An operation that initiates an action by requesting it of a resource.
push
An operation (for example, a file package distribution) that sends information to other resources.

Q
query
In the Tivoli environment, a combination of statements used to search the configuration repository for systems that meet certain criteria.

query facility
In the Tivoli Management Framework, a facility that enables you to use SQL functions to access information in an RDBMS Interface Module (RIM) repository.

query library
In the Tivoli environment, a facility that provides a way to create and manage Tivoli Management Framework queries.

R
RDBMS
See relational database management system.

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 management region.

registered name
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 range
The Tivoli clients that receive data from a repeater site.

repeater
In a Tivoli management region, a managed node that is configured with the multiplexed distribution feature. A repeater receives a single copy of data and distributes it to the next tier of clients.

resource
See managed resource.

resource type
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 the Tivoli environment, the relational database management system (RDBMS) database that a Tivoli application accesses through the RIM API. For example, the RIM repository can store data from the following applications:
- Tivoli Enterprise Console
- Tivoli Inventory
- Tivoli Software Distribution

root administrator
An account for the initial Tivoli administrator that is created during the installation of Tivoli Management Framework.
scalable

Pertaining to the capability of a system to adapt readily to a greater or lesser intensity of use. For example, a scalable system can efficiently adapt to work with larger or smaller networks performing tasks of varying complexity.

subscriber

A managed node or profile manager that is subscribed to a profile manager. Although profiles are distributed to a subscriber, the subscriber may or may not be the final destination of the profile distribution. See also endpoint.

subscription

The process of identifying the managed resources to which profiles are distributed. Managed resources and profiles are associated with each other in profile managers.

subscription list

A list that identifies the managed resources subscribed to a profile manager. The managed resources (which can include other profile managers) are the recipients of profile distributions. Including a profile manager on a subscription list (in effect, a list within a list) is a way of subscribing several managed resources simultaneously rather than adding each one individually. In Tivoli Application Management modules, a profile manager functions as a subscription list.

T

TAP

See Tivoli Authentication Package.

task

The definition of an action that must be routinely performed on various managed nodes throughout the network. A task defines the executable files to be run when the task is executed, the authorization role required
to execute the task, and the user or group name under which the task executes.

task library
A container in which a Tivoli administrator can create and store tasks and jobs.

Tivoli ADE
Tivoli Application Development Environment. A Tivoli 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 the Tivoli environment.

Tivoli administrator
In the Tivoli environment, a system administrator authorized to perform systems management tasks and manage policy regions in one or more networks. Each Tivoli administrator is represented by an icon on the Tivoli desktop.

Tivoli AEF
Tivoli Application Extension Facility. A Tivoli 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, capable of creating Windows NT and Windows 2000 security tokens for a different user context. Such 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 and Tivoli management region server.
Tivoli desktop
In the Tivoli environment, the desktop that system administrators use to manage their network computing environments.

Tivoli Distributed Monitoring
A Tivoli product that monitors system resources, initiates any necessary corrective actions, and informs system administrators of potential problems. Tivoli Distributed Monitoring consists of a group of monitors installed on each Tivoli client to be monitored; it resolves events on its own or sends them to the Tivoli Enterprise Console product.

Tivoli EIF
Tivoli Event Integration Facility. A Tivoli toolkit that provides a simple application programming interface (API) to enable customers and Tivoli Partners to develop new event adapters that can forward events to the Tivoli Enterprise Console product. A customer can also translate events from third-party or in-house applications.

Tivoli Enterprise Console
A Tivoli product that collects, processes, and automatically initiates corrective actions for system, application, network, and database events; it is the central control point for events from all sources. The Tivoli Enterprise Console product provides a centralized, global view of the network computing environment; it uses distributed event monitors to collect information, a central event server to process information, and distributed event consoles to present information to system administrators.

Tivoli environment
The Tivoli applications, based upon the Tivoli Management Framework, that are installed at a specific customer location and that address network computing management issues across many platforms. In a Tivoli environment, a system administrator can distribute software, manage user configurations, change access privileges, automate operations, monitor resources, and schedule jobs.
Tivoli Inventory
A Tivoli product that enables system administrators to gather hardware and software information for a network computing environment. Tivoli Inventory scans the managed resources and stores inventory information in the configuration repository.

Tivoli Management Framework
The base software required to run any of the Tivoli systems management 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)
- Distributed object database
- Basic administration functions
- Basic application services
- Basic desktop services, such as the graphical user interface (GUI)

In a Tivoli environment, Tivoli Management Framework is installed on every client and every server with this exception: The Tivoli management region server is the only server that contains the full object database.

Tivoli management region
In the Tivoli environment, a Tivoli management region server and the set of clients it serves. An organization can have more than one region. A Tivoli management region addresses the physical connectivity of resources; a policy region addresses the local organization of resources.

Tivoli management region client
Any computer—except the Tivoli management region server—on which Tivoli Management Framework is installed. A Tivoli management region client runs the object request broker (oserv) and maintains a local object database. Contrast with Tivoli management region server.
**Tivoli management region server**  
The Tivoli server that holds or references the complete set of Tivoli software, including the full object database. *Contrast with Tivoli management region client.*

**Tivoli Remote Execution Service**  
A service that enables the Tivoli environment to perform remote operations on machines. These operations include remotely installing clients, connecting Tivoli management regions, and starting the object request broker (*oserv*) from a remote machine.

**Tivoli server**  
*See Tivoli management region server.*

**Tivoli Software Distribution**  
A Tivoli product that automates software distribution to clients and servers in a network computing environment. An organization can use this product to install and update applications and software in a coordinated, consistent manner across a network. Tivoli Software Distribution creates file packages and distributes them to predefined subscribers.

**Tivoli User Administration**  
A Tivoli product that provides a graphical user interface (GUI) for centralized management of user and group accounts. Tivoli User Administration offers efficient, automated management of user and system configuration parameters, secure delegation of administrative tasks, and centralized control of all user and group accounts in a network computing environment.

**TMR**  
*See Tivoli management region.*

**transaction**  
A specific set of input data that triggers execution of a specific process or job; a message destined for an application.
TRIP

See Tivoli Remote Execution Service.

U

upcall

A method invocation, or call, from an endpoint “up” to the gateway.

user login map

A mapping that associates a single user login name with a user account on a specified operating system. User login maps enable Tivoli administrators to log in to the Tivoli environment or perform operations within the Tivoli environment with a single user login name, regardless of the system that they are currently using.

V

validation policy

Policy that ensures that all resources in a policy region comply with the region’s established policy. Validation policy prevents Tivoli administrators from creating or modifying resources such that they do not conform to the policy of the policy region in which they were created.

virtual login

See virtual user.

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 machines and Administrator on Windows NT machines.
Symbols
.aof file 11-4, 11-5
.cdf file 11-4, 11-5
.gdf file 11-4, 11-5

A
adding
See also creating
IP interfaces 2-7
login names 3-11
managed resource types to policy regions 5-8
repeaters 12-2, 12-5
resource roles 3-13
resources to desktop 3-15, 3-16
administrator's tag 11-8, 11-13
administrators
access to resources 3-15
adding resources to desktops
using the desktop 3-16
wln command 3-17
creating 3-7
database object 3-27
deleting 3-28
description 3-1
editing
logins 3-25
wsetadmin command 3-27
group names 3-9
icon 1-25
logins 3-2, 3-3
names 3-2
remote TMR resources 4-11
removing TMR roles 3-10, 3-21
restoring 3-28
root authority 3-28
setting
logins 3-10, 3-24
notice group subscriptions 3-29
notice groups 3-13, 3-29
properties 3-17
resource roles 3-12, 3-21
TMR roles 3-9, 3-19
subscribing to notice groups 3-14, 3-30
viewing
as data objects 3-28
procedure 3-4
removed administrators 3-28
wlookup command 3-6
Administrators Collection icon 1-25
after_install policy script 2-2
AMP, See application management package (AMP)
AMS, See Application Management Specification (AMS)
application management
collection scripts 11-3
data 11-3
description 11-1, 11-2
examples of
distribution 11-19
monitoring 11-19
troubleshooting 11-25
application management package (AMP)
application description files 11-12
application source files 11-4, 11-12
contents 11-4
description 11-12
table 11-19
staging area  11-13
Application Management Specification
(AMS)
AMS-compliant files  11-5
description  11-3
desktop icons  11-7
development tools  11-4
superseded commands  11-6
versions 1.1 and 2.0  11-6
application object file (.aof)  11-4,  11-5
applications
components  11-4,  11-5,  11-8,  11-20
configuring  11-2
dependency checking  11-2
description files  11-4
distributing  11-2,  11-21
installing  11-2
maintaining  11-2
management-ready  11-3
monitoring  11-2,  11-24
policy region  11-7
secondary policy region  11-8
tagged versions  11-8
troubleshooting  11-25
uninstalling  11-2
updating  11-2
using multiplexed distribution  12-1
assigning policy to resource types  5-9
viewing  3-4
clients
adding IP interfaces  2-7
ingating IP interfaces  2-10
moving clients  2-5
toggling icons  2-29
expiring notices  8-24
jobs
creating  9-22
deleting  9-31,  10-20
editing  9-28,  10-20
enabling  10-20
running  9-25
saving output  9-26
scheduling  10-16
sorting  10-26
viewing  10-20
notices
combining  8-19
displaying  8-21
filtering  8-16
forwarding  8-8
marking as read  8-11
reading  8-2
saving  8-5
sorting  8-13
openin an xterm session  2-14
policies
adding or removing managed
resource types  5-7
assigning policy to resource types  5-10
creating policy subregions  5-5
creating top-level policy regions  5-4
profiles
cloning  6-34
copying  6-33
creating  6-27
distributing 6-29
moving 6-35
removing subscribers 6-22
synchronizing with profile endpoints 6-31
queries
creating 7-2, 7-5
editing 7-11
running 7-16
selecting subscribers or targets 7-19
task libraries, creating 9-10
tasks
creating 9-12
deleting 9-31
running 9-15
saving output 9-18
TMR connections
determining status 4-10
disconnecting 4-19
remote 4-6
secure 4-2
updating resources 4-14
managed node icons 2-29
managed resource types 5-7
policy region name 5-6
profile properties 6-5
queries 7-11
check boxes 1-11
checking policy in policy regions 5-11
clients
endpoints 2-4
icons 1-26
moving to another policy region 2-4, 2-5
properties 2-6
cloning profiles 6-34
collections 1-23
creating 1-23
description 1-23
icons 1-25
populating 1-24
combining notices 8-19
commands
lcfd 2-15, 2-21
lcfd.sh start 2-24
lcfd.sh stop 2-24
odadmin 4-3, 12-19
wchkdb 4-18
wchkpol 5-14
wconnect 4-5, 4-10
wrctadmin 3-15
wrctjob 9-25
wrctp 5-5, 5-6
wrctpfr 6-28
wrctprfmgr 6-19
wrctqlib 7-4
wrctquery 7-10
wrcttask 9-14
wrcttlib 9-11
wdel 3-29, 6-27, 6-37
wdeljob 9-31
wdeltask 9-31
wdisconn 4-20

B
Backup icon 1-26
before using multiplexed distribution 12-1
browser dialog buttons 1-16
browsing resources 1-21
bulletin board 8-1
buttons, example 1-10

C
canceling jobs 10-9
changing
icon labels 1-24

Tivoli Management Framework User’s Guide  Index–3
wdistrib   6-30
wdisttask   9-7
wedsched   10-23
wep        2-22
wexpnotif  8-2, 8-24
wgetadmin  3-7
wgetpr     5-9, 5-11
wgetquery  7-13
wgetsched  10-23
whostid     2-7
widmap      3-4
wifconfig   2-9, 2-12, 2-13
wimprtcdfp  11-6
wimprtcdfmon 11-6
wimprtcdftl 11-6
winstruct  11-1, 11-6, 11-9, 11-12
winstruct_event 11-10
winstruct_file 11-10
winstruct_inventory 11-10
winstruct_monitor 11-10
winstruct_plus   11-10
winstruct_task   11-10
wln         1-21, 3-17, 3-28
wlookup     3-7
wls         3-6, 3-28, 8-5
wlsconn     4-11
wlsnotif    8-5, 8-7, 8-10
wmannode    2-7
wmdist      12-23
wmdistgui   12-21
wmemsize    2-7
wmv         2-2, 2-5
wrm         3-28
wrpt        12-4
wruninvquery 7-15, 7-21
wrunjob     9-26
wrunquery   7-14, 7-18
wruntask    9-18
wschedjob  10-19
wsetadmin  3-21, 3-24, 3-27, 3-31
wsetjob     9-31
wsetpm      6-13, 6-26
wsetpr      5-9, 5-11
wsetquery   7-13
wsettask    9-22
wstartesvr  11-17
wstopesvr   11-17
wsub        6-22
wname       2-7
wunsub      6-24
wupdate     4-18
wxterm      2-15

component description file (.cdf) 11-4
component description file (.gdf) 11-5
components
  configuring MDist and MDist 2 12-2
  Exchange AMP 11-23
  Exchange Policy Region 11-20
  installing MDist 2 12-2
  of an application 11-4, 11-5, 11-8
configuration management, overview 6-1
configuration scripts, application management 11-3
configuring MDist 2 components 12-9
configuring MDist components 12-2

connections, TMR
  description 4-1
  determining status 4-10
disconnecting
  using the desktop 4-19
  wdisconn command 4-20
displaying status
  wlsconn command 4-11
displaying status using the desktop 4-10
encryption 4-3, 4-7
icon 1-26
one-way and two-way 4-4
remote
  using the desktop 4-5
  wconnect command 4-10
resource exchange or update description 4-13
scheduling 4-14
using the desktop 4-16
wupdate command 4-18
secure
using the desktop 4-2
wconnect command 4-5
connections, TMR
disconnecting 4-18
console, Distribution Status 12-17, 12-18
controlling
profile distribution 6-13
profiles 6-2
task creation and execution 9-9
copying profiles 6-33
creating
administrators
using the desktop 3-7
wrtadmin command 3-15
collections 1-23
desktop resources 1-21
jobs in task library 9-22
policy subregion 5-5
profile managers 6-17
queries 7-4, 7-5
query libraries 7-2
repeaters 12-2, 12-5
task libraries 9-10
tasks 9-11
Tivoli administrators 3-1
top-level policy regions 5-3
customizing Tivoli Management Framework 5-1

administrators 3-27, 3-28
creating 11-12
for management-ready applications 11-12
policy regions 11-15
profile managers and profiles 11-15
wstruct command 11-8
databases, application management data 11-6
dataless profile managers 11-18
default policies 2-4, 5-3, 5-9, 6-13, 9-8
defining
distribution targets 7-14
subscription targets 7-14
deleting
administrators 3-28
icons 1-21
profile managers 6-26
profiles from profile manager 6-36
scheduled jobs 10-22
tasks or jobs 9-31
designing a repeater hierarchy 12-1
desktop
description 1-1
menus 1-19
Navigator 1-21
refresh 1-21
Desktop icon 1-26
Desktop Management Task Force (DMTF) 11-3
Desktop Navigator 1-21
destination profile manager 6-33
development tools
Application Management Specification 11-4
Tivoli Module Builder 11-4
Tivoli Module Designer 11-4
dialogs
administrators
Create Administrator 3-7

D
data
for application management 11-3
MTEG 11-7
data objects
Set Login Names 3-26
Set Notice Groups 3-14, 3-30
Set TMR Roles 3-20
Browser 1-16
clients
Add IP Interface 2-8
Client/Server Icon Toggle 2-29
Endpoint List 2-16
Endpoint Properties 2-17
Gateway List 2-15
Managed Node 2-6
Create Collection 1-23
description 1-2
Desktop Navigator 1-21
elements 1-4
File Browser 1-18
jobs
Create Job 9-23
Edit Job 9-28
Save Job Output 9-27
notices
Filter Notices 8-18
Forward Notice 8-10
Notice Message Viewer 8-4
Read Notices 8-2
Sort Notices 8-15
policies
Check Policy 5-12
Create Policy Region 5-4
Policy Region Properties 5-7
Set Managed Resources 5-8
Set Managed Resources Policies 5-10
profiles
Clone Profile 6-34
Create Profile 6-27
Create Profile Manager 6-18
Delete Profiles 6-37
Distribute Profiles 6-15
Edit Profile Manager 6-25
Profile Differences 6-32
Subscribers 6-20
Synchronize Profiles 6-31
queries
Create Query 7-4
Create Query Library 7-3
Edit Query 7-12
Run Query 7-14
Table Description 7-8
scheduler
Set Retry/Cancel Options 10-11
tasks
Create Task 9-13
Create Task Library 9-10
Destination of Task Output 9-17
Edit Task 9-20
Execute Task 9-16
Save Task Output 9-19
TMR connections
Connect to a Remote TMR 4-6
Securely Connect to a Remote TMR 4-2
TMR Connection Status 4-10
Update Resources from Multiple TMRs 4-14
discharging jobs 10-13, 10-21
disconnecting TMRs 4-18, 4-19
displaying notices previously read 8-21
unread 8-2
distributing data 12-1
profiles 6-29
task executables 9-7
distribution management 12-1
profiles
data preservation 6-15
levels 6-15
Distribution Status console
  Distribution Topology 12-28
  Node Table 12-27
  Status Chart 12-25
  Time Spent Chart 12-26
  using 12-17
distributions
  viewing details of 12-23
  viewing status 12-22

DMTF, See Desktop Management Task Force (DMTF)

E
  editing
    IP interfaces
      description 2-9
      using the desktop 2-10
      wifconfig command 2-12
    jobs 9-28
    logins
      administrators 3-25
      wsetadmin command 3-27
      notice group subscriptions 3-29, 3-31
      profile managers 6-25
      properties, administrators 3-17
      queries 7-11, 7-12
      resource roles, wsetadmin command 3-24
      scheduled jobs 10-19, 10-22
      tasks 9-19
      TMR authorization roles
        wsetadmin command 3-21
    electronic mail, forwarding notices 8-8
    elements in dialogs and windows 1-4
    emulators 2-14
    enabling jobs 10-21
    encryption, connected TMRs 4-3, 4-7
  assigned gateway 2-18, 2-20
  configuration settings 2-20
dataless profile managers 2-20
description 2-1, 2-4
  hostname 2-18
  icons 1-26
  interpreter type 2-18
  last restart 2-19
  log file 2-19
  method cache 2-19
  network address configuration 2-20
  operating system 2-18
  properties
    description 2-15
    from Web browser 2-17
    viewing 2-15
    statistics 2-19
    status 2-18
    subscribing 11-18
    trace log 2-20
    version number 2-18
  environment, system 1-1
  event classes, adding to Tivoli Enterprise
    Console rule base 11-17
  exchanging resources
    after connecting TMRs 4-13
    description 4-1
    using the desktop 4-12
  executing tasks 9-5
  execution targets, for tasks 9-6
  expiration of notices 8-23
  expression characters, regular 1-14

F
  failed jobs 10-11
  file package 11-14, 11-22
  files
    AMS-compliant 11-4, 11-5
    application description 11-4
application object file (.aof) 11-4, 11-5
component description file (.cdf) 11-4, 11-5
distributing 11-14
global description file (.gdf) 11-4, 11-5
filter 1-22
filtering notices 8-16
finding resources 1-21
scheduled jobs 10-27
forwarding notices with electronic mail 8-8
function, calling a 11-11

G
global description file (.gdf) 11-4, 11-5
group names 3-9, 3-18

I
icons
changing 2-29
deleting 1-21
examples and descriptions
Administrators 1-25
Administrators Collection 1-25
Backup 1-26
Collection 1-25
Connect TMRs 1-26
Desktop 1-26
Distribution Status 12-18
Endpoint 1-26
Endpoint Manager 1-25
Install Client 1-26
Install Tivoli Server 1-26
Job 1-25
managed nodes 1-26
Notification Bulletin Board 1-24
Patch Install 1-26
PC managed nodes 1-26
Policy Region 1-24
Profile Manager (Database) 1-25
Profile Manager (Dataless) 1-26
Scheduler 1-24
Task 1-25
Task Library 1-25
Tivoli 1-24
Unknown 1-27
labels, changing 1-24
removing 1-20
restoring administrators 3-28
secondaries applications 11-8
toggling 2-4, 2-29
import commands, superseded 11-6
Install Client icon 1-26
Install Tivoli Server icon 1-26
instances of resource types
associated time stamp 4-17
interpreter type xiv
IP interfaces 2-7, 2-9, 2-10
iterative instruction 11-15, 11-18

J
Job icon 1-25
jobs
See also tasks
creating
using the desktop 9-22
wctjob command 9-25
deleting
using the desktop 9-31, 10-22
wdeljob command 9-31
disabling
set for a specified time 10-13
set to repeat 10-13
using the desktop 10-13, 10-21
editing
using the desktop 9-28, 10-22
wgetsched command 10-23
wsetjob command 9-31
enabling 10-21
execution mode 9-24
in multiple TMRs 10-15
purpose in task library 9-3
repeat time conflict 10-12
rescheduled 10-5, 10-10
restricting schedules 10-7
running
using drag and drop 9-25
using the desktop 9-26
wrunjob command 9-26
saving output 9-26
scheduled
across TMRs 10-14
allowable start-time period 10-9
editing 10-19
finding 10-27
for the past 10-6
retry intervals 10-11
run a specified number of times 10-5
run at specified times 10-3
run frequently 10-3
run monthly 10-5
run once 10-1
sorting 10-25
wschedjob command 10-19
scheduler notification 10-14
scheduling 10-16
specifying display of job attributes 10-24
start times across TMRs 10-15
task execution information 9-5
timeout 9-24

K
Kerberos 3-3, 3-11, 3-24, 3-26

L
labels, icons 1-24
lcfd 2-15, 2-21
lcfd.cfg file 2-20
lcfd.log file 2-19
lcfd.sh 2-15
libamsi shared library 11-11
limiting when jobs run 10-7
links 12-28
lists, scrolling 1-12
locking profile items 6-2
logical operators 6-2
login names
adding 3-11
administrator and user 3-2
editing 3-25
managing 3-3
removing 3-12, 3-27
setting 3-10, 3-24
using to change administrator’s
properties 3-18
loopback interfaces 2-7, 2-11, 2-13

M
making
remote TMR connections 4-5
secure TMR connections 4-2
managed nodes
changing icons 2-29
client icons 1-26
description 2-1, 2-3
IP interfaces
adding 2-7
Index–10

Version 3.7.1

creating repeaters 12-2, 12-5
MDist 2
before using this service 12-1
configuring repeaters 12-2, 12-9
creating repeaters 12-2
Distribution Status console 12-18
installing components 12-2
troubleshooting 12-15
using the Distribution Status console 12-17
viewing distribution details 12-23
menus
Backup 1-19
Create 1-21
description 1-4
desktop 1-19
distribution 11-3
example 1-5
Install 1-20
Maintenance 1-20
Navigator 1-19
option 1-12
pop-up 1-8
submenus 1-7
tear-off 1-8
TMR Connections 1-20
View 1-21
MIF 11-3
mnemonics 1-6
monitor collections 11-22, 11-24
moving
managed nodes to another policy region 2-4, 2-5
profiles from profile manager 6-35
MTEG 11-7
multiple logins 3-3
multiplexed distribution, See MDist and MDist 2

management
monitoring applications 11-24
of applications 11-1
management data
automated delivery 11-6
description 11-3
manual entry 11-6
Management Information Format, See MIF
Management Tool Extension Group, See MTEG
management tools
adding to Tivoli environment 11-15
Application Management Modules 11-5
failure 11-16
managing applications in Tivoli 11-5
receiving data 11-6
Tivoli Distributed Monitoring 11-5
Tivoli Enterprise Console 11-5
Tivoli Inventory 11-5
Tivoli Management Framework 11-5
Tivoli Software Distribution 11-5
management-ready applications
description 11-3
example distribution 11-19
example of monitoring 11-19, 11-24
unique versions 11-13
MDist
before using this service 12-1
configuring repeaters 12-2, 12-5

managed resources 2-2
managing
pop-up menu 2-3
properties 2-6
viewing properties 2-7
xterm sessions 2-14
removing 2-12
moving to another policy region
description 2-4
using drag and drop 2-5
wmv command 2-5
Index – 11

N
name registry
  time stamps  4-17
  updating "All" resources  4-18
naming conventions
  special characters  3-8, 5-4, 5-6, 6-18, 6-26, 6-28, 6-35, 7-6, 9-11, 9-13, 9-23, 10-17
Navigator  1-21
network administration, See management
network management, See management
nobody account  3-2
nodes  12-28
notice groups
  setting for administrators  3-13, 3-29
  subscribing  3-14, 3-30
  subscriptions
    editing  3-29
    wsetadmin command  3-31
  unsubscribing  3-14, 3-30
notice groups, See also notices
  attributes  8-1
  combining  8-19
  description  8-1
  displaying previously read  8-21
  expiration
    description  8-23
    wexpnotif command  8-2, 8-24
  filtering  8-16
  for specific applications  11-9
  forwarding with electronic mail  8-8
  marking
    as all read  8-13
    as read  8-11
    as unread  8-12
  reading
    description  8-2
    using the desktop  8-2

O
objects, data  11-8
odadmin  4-3, 12-19
one-way TMR connections  4-4
opening xterm sessions  2-14, 2-15
option menus, example  1-12
organizing
  groups of profiles  6-13
  queries into groups  7-2

P
parallel task execution  9-6
Patch Install icon  1-26
pattern matching  1-14
PC managed nodes
  client icons  1-26
  moving a client  2-4
performance, exchanging resources  4-13
pm_def_profile_managers default policy  6-13
pm_def_subscribers default policy  6-13
pm_val_remove_subscribers validation policy  6-14
pm_val_remove_subscription validation
removing subscribers 6-23
removing subscriptions
  wunsub command 6-24
subscribing
  description 6-19
  using drag and drop 6-20
  using the desktop 6-20
  wsub command 6-22
validation policies 6-14
profiles
  cloning from profile manager 6-34
  common elements 6-8
  copying from profile manager 6-33
    creating
      from profile managers
        wcrtprf command 6-28
      using the desktop 6-27
    winstruct command 11-15
  default policies 6-2
  deleting
    from profile manager 6-36
    profile managers 6-26
    using the desktop 6-37
    wdel command 6-37
description 6-1
differences 6-32
disabling policy validation 6-3
distributing
  levels 6-15
  replacing or preserving local data 6-15
  using drag and drop 6-29
  using the desktop 6-29
  wdistrib command 6-30
endpoint database 6-15
getting new copy 6-16
hierarchies 6-36
locking items 6-2
modifying 6-5
moving from profile manager 6-35
name 6-12
navigating the hierarchy tree 6-10
policies
  default 6-3
  validation 6-3
populating 6-4
properties 6-11
sorting 6-7
status 6-12
synchronizing
  system files 6-6
  using the desktop 2-4
    with a profile endpoint 6-30
using the desktop 6-27
validation policies 6-2, 6-5
viewing 6-10, 6-11
properties
  administrators 3-17
  clients 2-6
  endpoints 2-15
  managed nodes 2-6
  profiles 6-5, 6-11
  tasks 9-3

Q
queries
  creating
    description 7-4
    using the desktop 7-5
    wcrtquery 7-10
  editing
    using command line 7-13
    using the desktop 7-12
libraries
  creating using command line 7-4
  creating using the desktop 7-2
  description 7-1, 7-2
logical operators 7-9
names 7-4
<table>
<thead>
<tr>
<th><strong>RIM</strong></th>
<th><strong>7-1</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>running</td>
<td><strong>7-15</strong></td>
</tr>
<tr>
<td>saving results</td>
<td><strong>7-17</strong></td>
</tr>
<tr>
<td>searching RIM repositories</td>
<td><strong>7-1</strong></td>
</tr>
<tr>
<td>subscribers or targets</td>
<td><strong>7-15, 7-18</strong></td>
</tr>
<tr>
<td>using</td>
<td><strong>7-21</strong></td>
</tr>
<tr>
<td>viewing results</td>
<td><strong>7-15</strong></td>
</tr>
<tr>
<td>views</td>
<td><strong>7-1</strong></td>
</tr>
<tr>
<td>where clauses</td>
<td><strong>7-5, 7-7</strong></td>
</tr>
<tr>
<td>wildcard characters</td>
<td><strong>7-10</strong></td>
</tr>
</tbody>
</table>

### R

- **radio buttons, using** | **1-11**
- **RDBMS Interface Module, See RIM**
- **reading notices** | **8-2**
- **realms, Kerberos** | **3-3, 3-11**
- **receiving notices** | **8-1**
- **refreshing the desktop** | **1-21**
- **regular expressions** | **1-14, 1-16, 1-18, 1-22**
- **relational database management system, See RDBMS**
  - **removing**
    - administrator icon | **3-27**
    - wrm command | **3-24**
  - administrators, TMR roles | **3-10, 3-21**
  - icons | **1-20**
  - IP interfaces
    - using the desktop | **2-12**
    - wifconfig command | **2-13**
  - login names | **3-12, 3-27**
  - managed resource types from policy regions | **5-8**
  - notices, automatically | **8-23**
  - profile managers | **6-26**
  - profiles | **6-37**
  - resource roles | **3-13, 3-23**
  - subscribers from a profile manager | **6-22**

- **repeat time conflict, jobs** | **10-12**
- **repeated jobs, See scheduler**
- **repeater**
  - configuration | **12-5**
  - reports, system administration activity, See notices
- **rescheduled jobs** | **10-5, 10-10**
- **resource roles**
  - adding | **3-13**
  - editing
    - using the desktop | **3-22**
    - wsetadmin command | **3-24**
  - removing | **3-13, 3-23**
  - setting | **3-12**
  - setting for administrators | **3-21**
- **resource types**
  - adding to policy regions | **5-8**
  - assigning policy | **5-9**
  - changing | **5-7**
  - removing from policy regions | **5-8**
  - time stamps | **4-17**
- **resources**
  - adding to desktop | **3-15**
  - collections | **1-23**
  - exchanging | **4-1, 4-12, 4-13**
  - restoring, administrators | **3-28**
  - restricting scheduled jobs | **10-7**
  - retry intervals, jobs | **10-11**
- **RIM**
  - description
  - searching repositories | **7-1, 7-4**
  - root administrator, root authority | **3-28**
  - rule base, adding event classes | **11-17**
  - running jobs
    - a specified number of times | **10-5**
    - at specified times | **10-3**
    - frequently | **10-3**
    - monthly | **10-5**
    - once | **10-1**
tasks 9-1
storing See task libraries
Structured Query Language (SQL) functions, See queries
subcommands
invoking 11-16
sequence of winstruct calls 11-11
winstruct 11-9
submenus, example 1-7
subregions, creating 5-5
subscribers
adding 6-19
removing 6-22
selecting for queries 7-15, 7-18
subscription
default policies 6-13
hierarchy 6-5, 6-10
levels 6-15
notice groups 3-14, 3-30
profile managers 6-19
validation policies 6-14, 6-19, 6-22
synchronizing
profiles
using the desktop 2-4
with profile endpoints 6-30
profiles and system files 6-6
system
files, synchronizing 6-6
management tasks, administrators 3-1
system administrators, See administrators
system environment 1-1

T
tagged versions of applications 11-8
targets, selecting for queries 7-15, 7-18
task libraries
creating
using the desktop 9-10
wcrttlib command 9-11
icons 1-25
policy 9-8
purpose 9-1
Task Library Language (TLL) 9-2
tasks
authorization roles 9-4
creating
description 9-3
using the desktop 9-11
wcrttask command 9-14
creation process 9-4
default policy 9-4
deleting
using the desktop 9-31
wdeltask command 9-31
editing
using the desktop 9-20
wsettask command 9-22
executable distribution 9-7
executables in bin directory 9-4
execution
information 9-5
mode 9-6, 9-16
process 9-4
execution targets, defined 9-6
icons 1-25
information 9-3
output
saving 9-17, 9-18
specifying 9-6
running
using drag and drop 9-15
using the desktop 9-16
wruntask command 9-18
scheduling 9-6
staging count 9-6
staging interval 9-6
timeout setting 9-6, 9-17
user or group ID 9-2, 9-4
validation policies 9-2, 9-4

Index–16

Version 3.7.1
with task arguments 9-2
tear-off menu, example 1-8
terminal emulators 2-14
text boxes, using 1-11
Time Spent Chart 12-26
time stamp in name registry 4-17
timeout settings, tasks 9-6
Tivoli 11-4
Tivoli Desktop for Windows 2-1
Tivoli Enterprise Console 11-17
Tivoli Module Builder
description 11-4, 11-12
producing an AMP 11-4
Tivoli Module Designer
description 11-4, 11-12
producing an AMP 11-4
tl_def_dist_mode 9-4
tl_def_dist_mode default policy 9-8
tl_def_man_nodes default policy 9-9
tl_def_prof_mgrs default policy 9-9
tl_def_set_gid default policy 9-9
tl_def_set_uid default policy 9-9
tl_val_man_nodes validation policy 9-9
tl_val_prof_mgrs validation policy 9-9
tl_val_set_gid validation policy 9-10
tl_val_set_uid validation policy 9-10
tmersrvd account 3-2
TMR
collections
determining status 4-10
encryption 4-3, 4-7
one-way and two-way 4-4
remote 4-5, 4-10
secure 4-2, 4-5
updating resources 4-14
description 4-1
disconnecting
description 4-18
using the desktop 4-19
wdisconn command 4-20
displaying status
wlsconn command 4-11
displaying status using the desktop 4-10
icons 1-24
jobs
run across boundaries 10-15
start times 10-15
number 4-3
remote region number 4-3
resource exchange or update
description 4-13
using the desktop 4-14, 4-16
wupdate command 4-18
roles
mapping 3-19
removing 3-21
setting 3-9, 3-19
scheduler 10-14
updating "All" resources 4-18
toggling
managed node icons 2-4, 2-29
top-level policy regions 5-3, 11-7
topology
distribution 12-28
tracking system administration activity, See notices
troubleshooting
application description files 11-25
application management 11-25
MDist 2 12-15
winstruct command 11-25
trusted host facility 4-5
two-way TMR connections 4-4

U
UNIX
group names 3-9, 3-18
nobody account | 3-2
opening an Xterminal session | 2-14
Unknown icon | 1-27
unsubscribing notice groups | 3-14, 3-30
updating, resources | 4-12, 4-13
user login names
  adding | 3-11
  changing administrator properties | 3-18
  description | 3-2
  mapping | 3-3, 3-8
  removing | 3-12, 3-27
  setting
    description | 3-24
    using the desktop | 3-25
wsetadmin command | 3-27

V
validation policies
  for managed resource types | 5-11
  in policy regions | 5-3
  profiles | 6-3, 6-5
  subscription | 6-22
  task library | 9-8
  tasks | 9-2, 9-4
  when moving clients | 2-4
validation policies See policies, policy methods
viewing
  administrators
    as data objects | 3-28
    using the desktop | 3-5
    wls command | 3-6
details of a distribution | 12-23
distribution status | 12-22
endpoint properties with Web browser | 2-17
managed resources in a policy region | 5-2
notices | 8-2
previously read notices | 8-21
profiles | 6-10, 6-11
query results | 7-15
scheduled jobs | 10-19
viewing from the endpoint manager
  endpoint properties | 2-15
views, within RIM | 7-1

W
wchkdb | 4-18
wchkpol | 5-14
wconnect | 4-5, 4-10
wcrtadmin | 3-15
wcrtjob | 9-25
wcrtpr | 5-5, 5-6
wcrtprf | 6-28
wcrtprfmr | 6-19
wertqlib | 7-4
wrtquery | 7-10
wrttsk | 9-14
werttlib | 9-11
wdel | 3-29, 6-27, 6-37
wdeljob | 9-31
wdeltask | 9-31
wdisconn | 4-20
wdistrib | 6-30
wdisttask | 9-7
Web browser, endpoint properties | 2-17
wedsched | 10-23
wep | 2-22
wexpnotif | 8-2, 8-24
wgetadmin | 3-7
wgetpr | 5-9, 5-11
wgetquery | 7-13
wgetsched | 10-23
where clauses | 7-5, 7-7
whostid | 2-7
widmap 3-4
wifconfig 2-9, 2-12, 2-13
wildcard characters 7-10
wimprtcdfpf 11-6
wimprtcdfmon 11-6
wimprtcdfh 11-6
windows
  Administrators 3-5
description 1-2
elements 1-4
  Notice Group Messages 8-3
  Policy Region 7-3
  Profile Manager 6-25, 6-27, 7-19
  Task Library 9-12
winstruct 11-1, 11-6, 11-9, 11-12
winstruct subcommands 11-9
winstruct_event 11-10
winstruct_file 11-10
winstruct_inventory 11-10
winstruct_monitor 11-10
winstruct_plus 11-10
winstruct_task 11-10
wln 1-21, 3-17, 3-28
wlookup 3-7
wls 3-6, 3-28, 8-5
wlsconn 4-11
wlsnotif 8-5, 8-7, 8-10
wmanode 2-7
wmdist 12-23
wmdistgui 12-21
wmemsize 2-7
wmv 2-2, 2-5
wrm 3-28
wrpt 12-4
wruninvquery 7-15
wrunjob 9-26
wrunquery 7-14, 7-18
wruntask 9-18
wschedjob 10-19
wsetadmin 3-21, 3-24, 3-27, 3-31
wsetjob 9-31
wsetpm 6-13, 6-26
wsetpr 5-9, 5-11
wsetquery 7-13
wsettask 9-22
wstartesvr 11-17
wstopesvr 11-17
wsub 6-22
wuname 2-7
wunsub 6-24
wupdate 4-18
wxterm 2-15

X
xterm sessions 2-14