Tivoli® Provisioning Manager

IBM

Version 5.1.1

Installation Guide for Linux on System z

GC23-9723-00

Note

Before using this information and the product it supports, be sure to read the general information under "Notices" on page 151.

June 2008

Contents

About this publication v
Intended audience v
What's new for installation v
Product changes vi
Publications vi
Tivoli Provisioning Manager library vi
Prerequisite publications vi
Accessing terminology online vii
Accessing publications online vii
Ordering publications vii
Accessibility vii
Tivoli technical training viii
Support information viii
Conventions used in this guide viii
Typeface conventions viii

Chapter 1. Installation overview 1
Product components 1
Installation types 2
User considerations for a default installation. . . 3
Installation process 3
Preinstallation 3
Installation 5

Chapter 2. Preinstallation checklist for Linux on System z 9
Preinstallation Step 1: Read the release notes . . . 10
Preinstallation Step 2: Verify operating system requirements 11
Required packages 11
Preinstallation Step 3: Plan the topology 12
Default installation 12
Custom installation 12
Preinstallation Step 4: Allocate disk space 14
Default installation 14
Custom installation 15
Disk space for database growth. 18
Preinstallation Step 5: Set up required users . . . 18
Default installation 18
Custom installation 19
Preinstallation Step 6: Verifying the environment . . 21
Default installation 21
Custom installation 23
Preinstallation Step 7: Prepare installation media . . 25

Chapter 3. Installing Tivoli Provisioning Manager 27
Installation Step 1: Run the installer 29
Installation Step 2: Identify the topology. 30
Installation Step 3: Select the installation type . . . 33
Installation Step 4: Configure the installation . . . 34
Default installation 35
Custom installation 36
Installation Step 5: Identify installation media . . . 46
Installation Step 6: Verify system requirements . . 48
Installation Step 7: Perform required configuration 49
Updating WebSphere Application Server . . . 49
Configuring a shared WebSphere Application Server environment. 51
Configuring the DB2 database registry 51
User passwords stored in the installation log . . 52
Installation Step 8: Verify your installation 52
Step 8: Perform recommended configuration . . . 52

Chapter 4. Verifying installation 53
Starting and stopping Tivoli Provisioning Manager 53
Starting Tivoli Provisioning Manager 53
Stopping Tivoli Provisioning Manager 56
Verifying core components 57
Verifying SSL configuration 58

Chapter 5. Post-installation configuration 63
Backing up the database 63
Configuring a read-only directory server 63
Choosing an authentication method 63
Directory server requirements 64
Configuring Tivoli Provisioning Manager to use the LDAP server. 65
Importing LDAP users 68
Authenticating with a client certificate 70
Recommended configuration for better performance 71
Setting the maximum heap size. 71
Setting the db-truncation value 72
Setting the MAXAPPS and MAXCONNECTION parameters 72
Setting Ulimit value 72
Importing sample data 73
Next steps 73

Chapter 6. Recovering from installation errors 75
Recovery first steps. 75
Requirement verification by the installer. 81
Existing installation. 81
Operating system and hardware 82
Networking 83
Connectivity 86
Required packages 87
User management and permissions 88
Prerequisite applications 88
Other requirements. 90
Recovering from other errors 90
Before prerequisite software is installed 90
During installation of software 91
Preinstalled software not detected 91
Installer unable to copy from disks 91
Installation of DB2 fails when node name is different than host name 91

After DB2 installation 92
Missing WebSphere Application Server installation causes Tivoli Provisioning Manager installation to fail 92
The device manager federator installation fails . 93
Installation using a Reflection X connection fails 94
After Tivoli Provisioning Manager installation . . . 94
SOAP services fail to start 94
Installation of dynamic content delivery management center fails 95
Out Of Memory error 96

Chapter 7. Upgrading Tivoli Provisioning Manager to Tivoli Intelligent Orchestrator. 97

Appendix A. Values for a default installation 99
Tivoli Provisioning Manager default settings . . . 99
Core component default settings 100
WebSphere Application Server default settings . . 101
DB2 default settings 101

Appendix B. Uninstalling and reinstalling Tivoli Provisioning Manager 103
Uninstall core components 103
Uninstall the device manager federator 103
Uninstall the dynamic content delivery management center 104
Uninstall the agent manager 105
Uninstalling Tivoli Provisioning Manager 105
Remove or unconfigure prerequisite applications 107
Uninstalling DB2 107
Uninstalling WebSphere Application Server . . 108
Remove items remaining after uninstallation . . . 108
Application files and configuration settings . . 109
Global Unique Identifier. 109
Reinstalling Tivoli Provisioning Manager 110

Appendix C. Performing a silent installation 111
Creating a response file 111
Running a silent installation 112
Silent installation exit codes 113

Appendix D. Preinstalling required software 115
Preinstalling WebSphere Application Server . . . 115
Preinstalling DB2 115
Installing the DB2 server 116
Installing the DB2 client 118

Appendix E. Installing the directory server 121
Installing and configuring Tivoli Directory Server 121
Requirements 121
Installing Tivoli Directory Server 123
Configuring Tivoli Directory Server 124

Appendix F. Manually configuring read-only LDAP 127
Disable WebSphere Application Server security settings 127
Configure WebSphere Application Server to use custom user registry 127
Read-only LDAP sample information 128
Replace the user-factory.xml file 130
Restart Tivoli Provisioning Manager. 132
Enable WebSphere Application Server security . . 132
Import the Tivoli Provisioning Manager administrator user. 132
Update user password information 132

Appendix G. Common tasks for Tivoli Provisioning Manager installation . . 135
Creating users and groups 135
Creating a group 135
Creating a user. 135
Setting user passwords 136
Other user commands 137
Changing default passwords 137
DB2 tasks 139
Checking the status of DB2. 139
Starting DB2. 139
Stopping DB2 139
Reorganizing DB2 tables. 140
Configuring the DB2 database. 141
Managing the transaction logs. 142
Dropping a DB2 database 142
Tivoli Directory Server tasks 143
WebSphere Application Server tasks. 144
Checking WebSphere Application Server status 144
Starting and stopping the WebSphere Application Server 144
Logging on to the WebSphere Application Server administrative console 145

Appendix H. Backing up the database 147
Before backing up or restoring the database . . . 147
Backing up a DB2 database. 147
Restoring a DB2 database 148

Notices 151
Trademarks 152

About this publication

The IBM® *Tivoli®* *Provisioning Manager Installation Guide* provides information on how to install and configure Tivoli Provisioning Manager installations on the Linux® on System z™ operating system.

Intended audience

This book should be read by system administrators, operators or anyone else responsible for installing and configuring Tivoli Provisioning Manager.

People who are installing and configuring Tivoli Provisioning Manager should have knowledge in the following areas:

- Linux on System z operating system
- Networking concepts.
- Basic operating system commands
- Operation, configuration and maintenance for IBM DB2® Enterprise Server Edition 8.1
- Operation, configuration and maintenance for Tivoli Directory Server 6.1.
- IBM WebSphere® Application Server 6.0.2.11.
- Basic SQL commands

What's new for installation

This topic highlights what is new or changed in Version 5.1.1 for users who plan to install the product. The enhancements have many positive ramifications for preparing, installing, maintaining, and removing installations.

Default installation option
The installer provides a default installation option for performing an installation on a single computer with default settings. This installation option automates creation of required users and configuration of all product components. If you want to customize your installation settings, you can choose the custom installation option instead.

Automatic verification of prerequisites
The installer now verifies most installation prerequisites automatically before installing software so that you can address any requirements that are not met and then continue with installation. Error messages also include a message ID that you can look up in this guide for details.

Local installation for all supported platforms
In Tivoli Provisioning Manager Version 5.1.0, some operating systems required remote installation of the product from a separate computer. In Version 5.1.1, all installations are local: you run the installer on the same computer where you are installing the product.

Supported topologies
The installer now supports a single node topology and a two-node topology with a remote database server. By default, authentication is handled by the operating system. If you want to use a read-only directory server on a separate computer, you can configure Tivoli Provisioning Manager to work with the directory server after installation.

Product changes

In previous versions of Tivoli Provisioning Manager the `reinit` and `reinit-exec` commands were available to initialize the data model. These commands are not available in Tivoli Provisioning Manager Version 5.1.1 and are not supported.

In Version 5.1.1, the `reinit-exec` command is used by the installer but it cannot be used to initialize the database. Running the command will render your database unusable. To recover, it is necessary to restore your database.

Publications

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

Tivoli Provisioning Manager library

The following documents are available in the Tivoli Provisioning Manager library:

- *Tivoli Provisioning Manager Installation Guide*, SC32-2234 (AIX®), SC32-2233 (Linux on Intel®), SC32-2235 (Solaris), SC32-2232 (Windows®)

  Describes how to perform a regular installation of the product that supports a full production environment.
- *Tivoli Provisioning Manager Migration and Coexistence Guide*, SC32-2245

  For existing Tivoli Configuration Manager users, this guide describes how to set up an environment in which you can continue using the Tivoli Management Framework and take advantage of several Tivoli Provisioning Manager features. After this environment is set up, you can gradually migrate from the coexistence environment to the new distribution infrastructure provided with Tivoli Provisioning Manager.
- *Tivoli Provisioning Manager Problem Determination Guide*, SC32-2236

  Provides detailed problem determination information and describes product messages, log files, and troubleshooting tools.
- *Tivoli Provisioning Manager Release Notes*, SC32-2238

  Describes the latest product changes and enhancements Tivoli Provisioning Manager Version 5.1.1.

Prerequisite publications

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

- WebSphere Application Server Information Center , available from `http://www.ibm.com/websphere`.
- DB2 Information Center, available from `http://www.ibm.com/db2`.
- IBM Directory Server documentation., available from the Tivoli Software Information Library at `http://www.ibm.com/tivoli/library`.

Because every environment is unique, it is expected that users following the instructions in this book have the necessary prerequisite knowledge to install, configure and administer this software in their unique environment.

Accessing terminology online

The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available at the following Tivoli software library Web site:

http://publib.boulder.ibm.com/tividd/glossary/tivoliglossarymst.htm

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

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

Accessing publications online

The documentation CD contains the publications that are in the product library. The format of the publications is PDF, HTML, or both. Refer to the readme file on the CD for instructions on how to access the documentation.

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center Web site at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp.

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

Ordering publications

You can order many Tivoli publications online at http://www.elink.ibmlink.ibm.com/public/applications/ publications/cgibin/pbi.cgi.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

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

1. Go to http://www.elink.ibmlink.ibm.com/public/applications/publications/cgibin/pbi.cgi.
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

Accessibility

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

Tivoli technical training

For Tivoli technical training information, refer to the following IBM Tivoli Education Web site at http://www.ibm.com/software/tivoli/education.

Support information

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

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

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

Problem Determination Guide
For more information about resolving problems, see the Problem Determination Guide for this product.

Conventions used in this guide

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

Typeface conventions

This guide uses the following typeface conventions:

Bold

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

Italic

- Emphasis of words
- New terms in text
- Variables and values you must provide

`Monospace`

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

Path variables

This guide uses the following variables to represent installation directory paths.

Table 1. Path variables

Path variable	Component	Default directory
AM_HOME	The agent manager	/opt/IBM/AgentManager
DB2_HOME	DB2	`/opt/IBM/db2/V8.1`
$WAS_HOME	WebSphere Application Server	`/opt/IBM/WebSphere/AppServer`
$TIO_HOME	Tivoli Provisioning Manager	`/opt/ibm/tivoli/tpm` **Note:** The dynamic content delivery management center and the device manager federator are also installed in subdirectories of this path.
Tivoli_common_dir	The Tivoli Common Directory	`/var/ibm/tivoli/common`
$TIO_LOGS	The location of Tivoli Provisioning Manager runtime logs	`/var/ibm/tivoli/common/COP/logs`

Chapter 1. Installation overview

A complete Tivoli Provisioning Manager product installation is composed of multiple application components, including the Tivoli Provisioning Manager application itself. To better understand the installation process, you should have a basic understanding of the installation components and the overall installation process.

Product components

Tivoli Provisioning Manager includes the following components.

Table 2. Product components

Component	Description	Installation media provided?
Application server: WebSphere Application Server	Tivoli Provisioning Manager runs as an application within a WebSphere Application Server environment.	Yes
Database server: DB2	The Tivoli Provisioning Manager database stores all the data about the IT environment managed by Tivoli Provisioning Manager.	Yes
Directory server: Tivoli Directory Server	By default, Tivoli Provisioning Manager is installed and configured so that user authentication is managed by the operating system. After installation, you can configure Tivoli Provisioning Manager so that it can work with a read-only directory server.	Yes

Table 2. Product components (continued)

Component	Description	Installation media provided?
Core components	Several core components are installed with Tivoli Provisioning Manager to support software distribution processes and communication with managed computers. **Tivoli Provisioning Manager for Dynamic Content Delivery management center** The dynamic content delivery management center provides centralized control of the upload, replication, and download of files. It also monitors the state of depot servers in distributed locations and stores file data. **Tivoli Provisioning Manager for Job Management Service federator** Also called the device manager federator, this component acts as a federated server that manages job distribution. It pushes incoming jobs to all of the endpoint agents or regional agents. **The agent manager** Tivoli Provisioning Manager uses the Tivoli Common Agent Services for software distribution and compliance. The agent manager is the server component of the Tivoli Common Agent Services and provides secure connections with managed computers on which the common agent is installed.	Yes

Installation types

There are two installation types.

Table 3. Installation types

Default installation	Custom installation
Recommended for demonstration or evaluation purpose, or for a small production environment.	Recommended for installing a production environment.
Installs Tivoli Provisioning Manager with default settings.	Enables you to customize settings such as user names, installation directories, or port numbers.
Required users are created for you. **Note:** Some security settings that are configured in your environment might prevent user creation. For more information, see "User considerations for a default installation" on page 3.	You must manually create all required users before installation.

Table 3. Installation types (continued)

Default installation	Custom installation
You cannot use an existing database or application server.	You can use an existing database server or an existing WebSphere Application Server installation. The installer can also install DB2 or WebSphere Application Server for you.
All components are installed on a single computer.	You can install Tivoli Provisioning Manager for a topology with the database server on a separate computer.
Silent installation is not supported.	Silent installation is supported.

User considerations for a default installation

Some security controls configured in your environment can prevent the Tivoli Provisioning Manager installer from creating the required user accounts on your system for a default installation. Some factors include:

Permissions
Permissions or access control lists configured for the computer can prevent the installer from creating users, creating user-related files and directories, or assigning permissions.

Password policy
In the installer, you must specify the passwords for users that are created. If these passwords to not conform to the password policy configured in your environment, the user creation process will fail.

If you encounter problems with user creation for a default installation, you might need to create the required users manually to ensure compliance with all security policies and compliance with Tivoli Provisioning Manager requirements. The installer can then use the configured user accounts and user settings to perform the default installation.

Installation process

The following sections outline the installation process.

Preinstallation

The steps in this section are described in detail in Chapter 2, “Preinstallation checklist for Linux on System z,” on page 9.

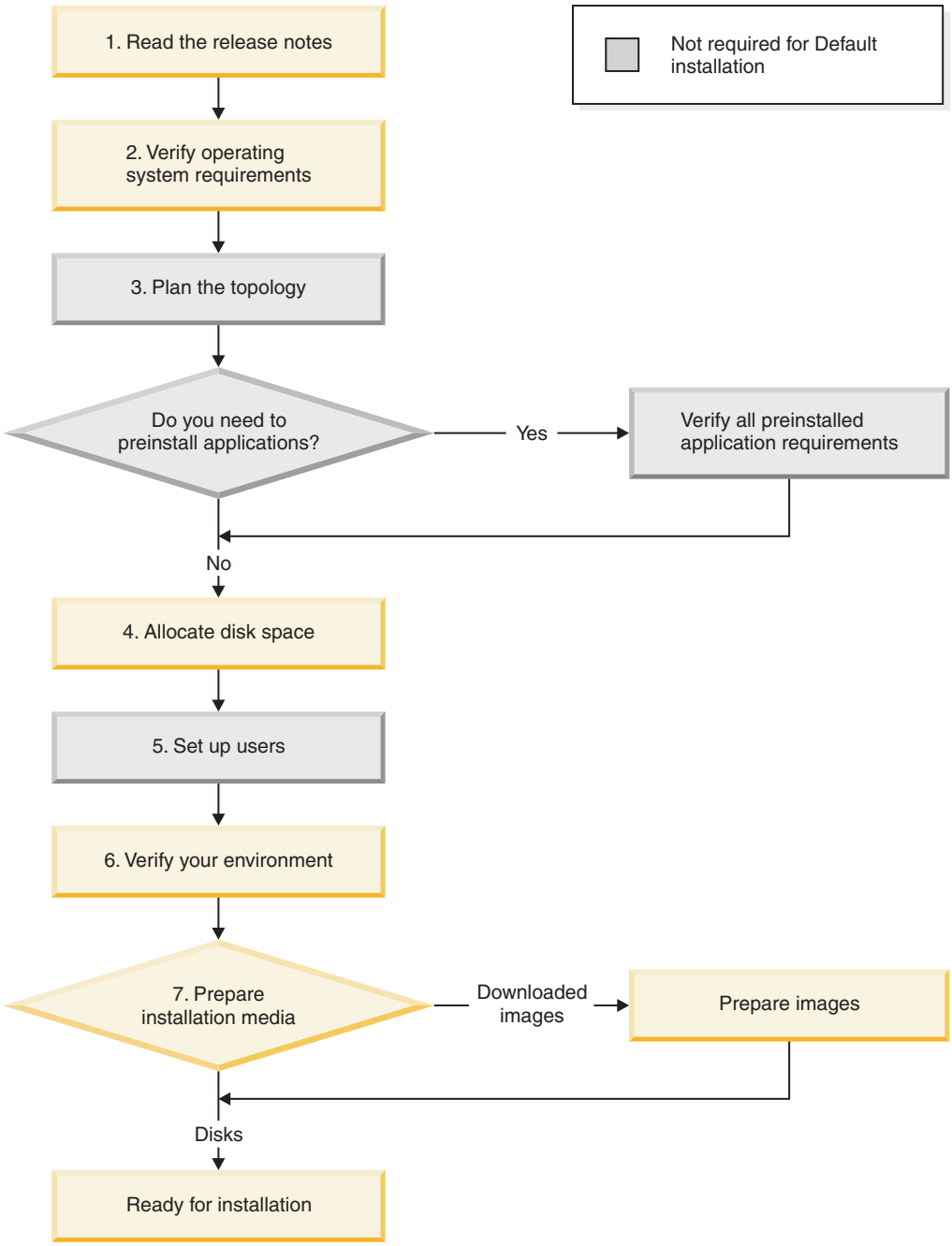

Figure 1. Installation roadmap

1. Check the release notes first for the latest updates to the documentation. Ensure that you check the release notes for any changes that might apply to installation.
2. Ensure that you are using a supported operating system version.
3. **Custom installation only**

   A *topology* is the distribution of software components on one or more computers or nodes. The topology that you select affects some of the steps that you must perform before you begin installation.

For some topologies, you must preinstall software. For example, if you want the DB2 server on a separate computer, it must be preinstalled and meet requirements specified in this documentation.

4. Ensure that you have enough disk space for installation. Disk space planning is important because Tivoli Provisioning Manager supports different topologies and includes multiple components. Carefully review the disk space requirements in this guide as you prepare for installation.
5. **Custom installation only**

   In many organizations, user accounts are created by a security department or by administrators with the authority to create users. To ensure that the users required by Tivoli Provisioning Manager meet the policies of your organization and meet Tivoli Provisioning Manager installation requirements, you must create the user accounts yourself before starting installation.
6. Check system requirements that must be met before you run the installer.
7. You can install the product using CD-ROM disks or downloaded images. If you want to use downloaded images, follow the steps in this guide to set them up.

After you have performed these steps, you are ready to start installation.

Installation

These steps describe the installation of the software, post-installation configuration, and verification of the installation. Details for the installation steps are in Chapter 3, “Installing Tivoli Provisioning Manager,” on page 27.

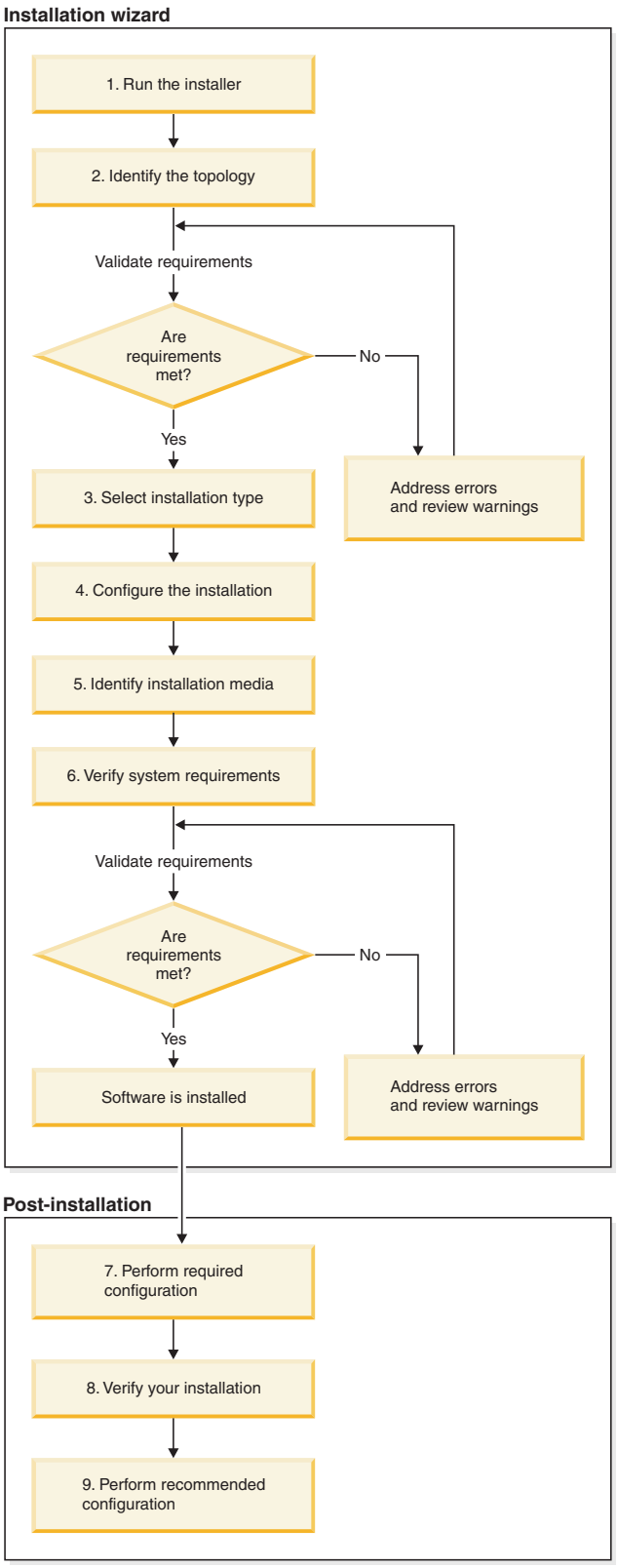

Figure 2. Installation roadmap

1. Start the installer. The installation wizard is launched.

2. In the installer, define information about your installation such as the host name of the computer, your administrator user name and password for the computer, and the database that you are using.

   The installer validates your information and checks for installed components. When you have addressed any errors or warnings, you can continue with installation.

3. If you selected options that are supported for a default installation, you can choose an installation type. If your system does not meet the requirements for a default installation, you must perform a custom installation.
4. In the installer, specify settings for the installation:

   Default installation
   Specify log on information for required users.

   Custom installation
   Specify settings for all the software that the installer will install or configure.

5. Identify the location where installation images will be stored. If you are using disks, this location is also used to copy installation files from the disks.
6. The installer validates information that you specified in steps 4 and 5 and system requirements.

   When you have addressed any errors or warnings, you can continue with installation. The installer summarizes your installation. When you confirm the summary, the software is installed.

7. After the software is installed, important configuration steps must be performed. Ensure that you perform the required configuration tasks.
8. Verify that Tivoli Provisioning Manager and core components are operational.
9. Some additional configuration steps are recommended for a production installation. If you are using the installation for demonstration or evaluation purposes, these steps are optional.

Chapter 2. Preinstallation checklist for Linux on System z

Use this preinstallation checklist to verify that your environment meets basic requirements for a new *Tivoli Provisioning Manager* installation. The product installer automatically verifies additional requirements and displays error messages if these requirements are not met. For details about these messages and the corresponding requirements, see "Requirement verification by the installer" on page 81.

The following diagram summarizes the preinstallation steps:

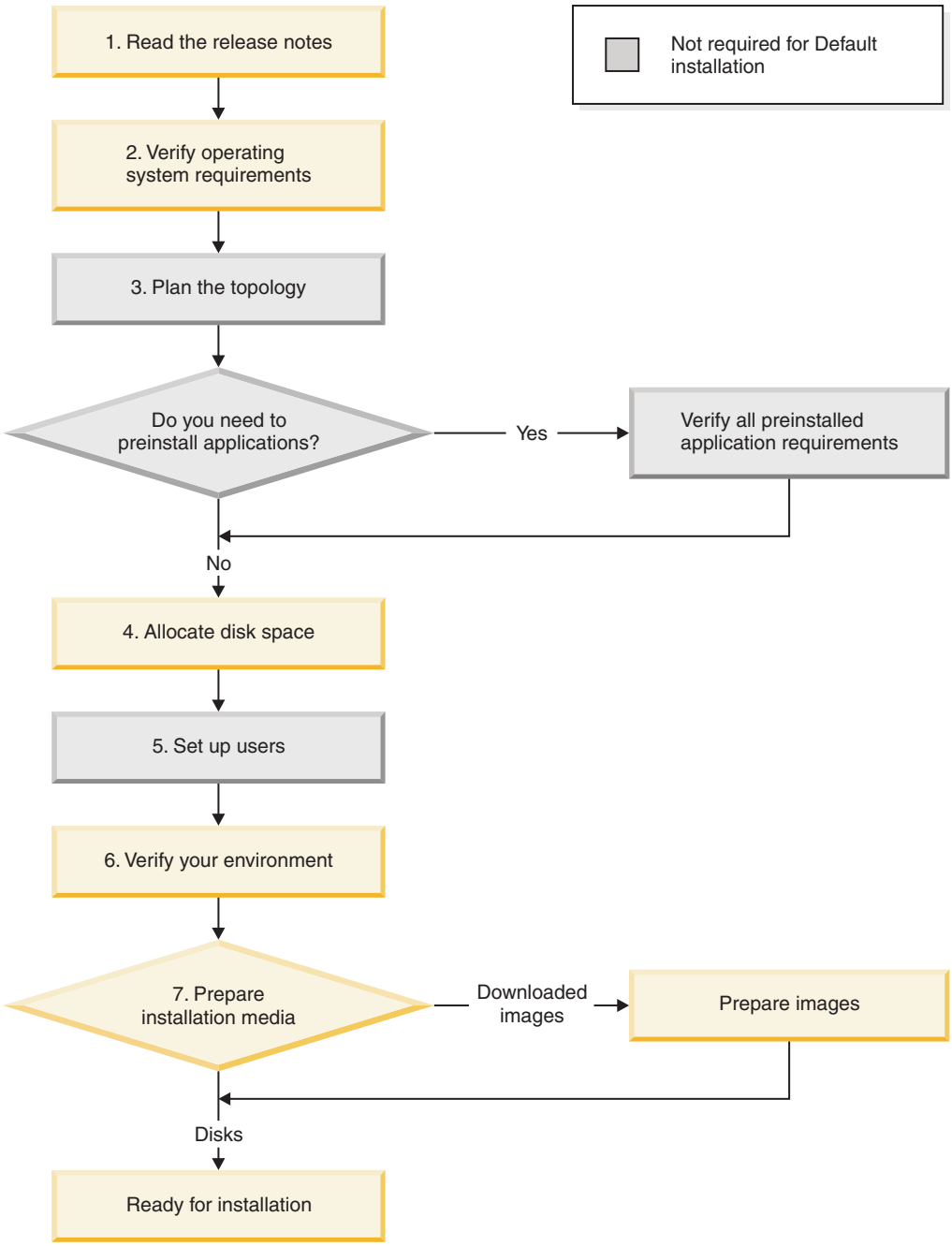

Figure 3. Installation roadmap

Preinstallation Step 1: Read the release notes

The release notes describe product changes and enhancements in the Tivoli Provisioning Manager product releases and updates to the documentation.

Preinstallation Step 2: Verify operating system requirements

Ensure that you are using a supported operating system at the correct version level. The following operating system versions are supported:

The following Linux distributions and versions are supported:

- Red Hat Advanced Server 5
- SUSE Linux Enterprise Server 9

Verify the following information:

1. Run the appropriate command to verify your version of Linux:

Table 4. Verifying the operating system version

Distribution	Command	Output
Red Hat	`cat /etc/redhat-release`	`Red Hat Enterprise Linux Server release 5.1 (Tikanga)`

SUSE Linux	`cat /etc/SuSE-release`	`SUSE LINUX Enterprise Server 9 (s390x)`
		`VERSION = 9`
		`PATCHLEVEL = 4`

2. Run the following command to verify the kernel version:

   ```
   uname -r
   ```

   Version 2.6 of the kernel is required.
3. For SUSE Linux, do the following:
   a. Set the LANG environment variable to work around an embedded messaging issue. Run the following command:

      ```
      export LANG=$LC_CTYPE
      ```

Required packages

Table 5. Required packages for Linux

Operating system	Packages

Red Hat	`An SSH client (for example, openssh)`
	`Expect 5.42`
	`telnet`
	`ftp`
	`gtk`
	`perl`
	`tcl`
	`tk`
	`wget`
	`compat-gcc-32-3.2.3-47.3`
	`compat-gcc-32-c++-3.2.3-47.3`
	`compat-db-4.1.25-9`
	`rpm-build-4.3.3-22_nonptl`
	`rpm-build-4.3.3-13xorg-x11-xfs`
	`fonts-xorg-base`
	`fonts-xorg-75dpi`
	`fonts-xorg-100dpi`
	`xorg-x11-font-utils`

Table 5. Required packages for Linux (continued)

Operating system	Packages
SUSE Linux	An SSH client (for example, openssh) Expect 5.42 telnet ftp gtk perl tcl tk wget compat-2004.7.1-1.2.i586.rpm[1]
[1] You can get the package from the SUSE Linux Server 9, Enterprise Edition CD (disc 1)	

If a specific version of the package is not listed, use the native version of the package that is included with your operating system at the current update level. For example, if you are using Red Hat Enterprise Linux Server release 5.1 (Tikanga), use the native `ftp` package included with Red Hat Enterprise Linux Server release 5.1 (Tikanga). Other FTP packages might not work with the installation.

The following example shows the command to check for installed packages that only contain the letters `ftp` in the file name. Other packages that have `ftp` and additional letters in the name are not returned in the results of the command.

```
rpm -qa | grep -w ftp
```

The following example shows the command to show installed packages that start with `compat`.

```
rpm -qa | grep compat
```

Package path requirements

- Some utilities are required by Tivoli Provisioning Manager and must be available from the following locations:
  - **Bash**: `/bin/bash`
  - **Expect, tar, gzip**: `/usr/bin`

  If they are not installed in these locations, create a symbolic link from those directories to the actual location.

Preinstallation Step 3: Plan the topology

Default installation

For an default installation, a predefined topology is used. All components are installed on the same computer.

Proceed to “Preinstallation Step 4: Allocate disk space” on page 14.

Custom installation

You must use one of the supported topologies. The topology that you choose determines how to plan for other installation requirements. For example, if you want to use a database installation on a separate computer, you must install the database server and database client yourself before running the Tivoli Provisioning Manager installer.

Table 6. Supported topologies

Topology	Node 1	Node 2
One node	• Tivoli Provisioning Manager and core components • WebSphere Application Server • Database server: DB2 • Tivoli Provisioning Manager user authentication is handled by the operating system	*Not applicable*
Two nodes, separate database server	• Tivoli Provisioning Manager and core components • WebSphere Application Server • Preinstalled database client • Tivoli Provisioning Manager user authentication is handled by the operating system	Preinstalled database server: DB2

Note:

- By default, Tivoli Provisioning Manager is configured for authentication by the operating system. After your installation, you have the option of

configuring Tivoli Provisioning Manager to work with a read-only directory server that is installed on a separate node.

Preinstalling applications for your topology

If you want to use an existing installation of one of the following applications, it must be preinstalled, at the correct version level, and configured to meet Tivoli Provisioning Manager requirements. For some applications, preinstallation is optional because Tivoli Provisioning Manager can perform the installation for you.

- For details about preinstalling and configuring these applications, see Appendix D, "Preinstalling required software," on page 115.
- If you do not need to preinstall these applications, proceed to "Preinstallation Step 4: Allocate disk space."

Table 7. Applications to preinstall

Application	Preinstallation required?
WebSphere Application Server 6.0.2.11 (64-bit version only)	**No** **Note:** If you want to preinstall WebSphere Application Server ensure that you install WebSphere Application Server with the provided installation media. Do not apply fix packs to the provided WebSphere Application Server installation before you start the Tivoli Provisioning Manager installation.
DB2 Enterprise Server Edition 8.1, Fix Pack 11	**No** Preinstallation is not required if you want DB2 installed on the Tivoli Provisioning Manager computer. **Yes** Preinstallation is required if you want DB2 to be installed on a separate computer. You must preinstall the database server on the second computer and preinstall the database client on the Tivoli Provisioning Manager computer.

Preinstallation Step 4: Allocate disk space

Ensure that you have enough disk space for software installed by Tivoli Provisioning Manager. During installation, the installer checks for the required disk space and will stop installation if the computer has insufficient disk space.

Default installation

An default installation installs all required components on a single computer. The total disk space requirements for a default installation include:

- 1.2 GB for the installer, and the installation image for the Common Inventory Technology tool. Common Inventory Technology is used to discover existing software on the computer.
- 4.4 GB for temporary files.
- 5 GB for the image repository. This is the location where the installation image files are stored. If you are using CD-ROM disks, the installation images will be copied from the disks to the image repository location that you select in the installation wizard.

  For details about disk space requirements for specific software components, see Table 8 on page 15 in the description for a custom installation.
- 15.9 GB for the software installed by the installation wizard.
- Additional disk space for growth of the database as described in "Disk space for database growth" on page 18.

Custom installation

The following table identifies:

- Installation components
- The default installation directory, if you have the option of choosing a different directory.
- The required disk space

Table 8. Required disk space on the Tivoli Provisioning Manager computer

Component	Location	Disk space
Temporary files	/	400® MB Files in this location are removed when installation is complete.
	/tmp	1 GB for temporary files
	/var/tmp (default)	• 1.2 GB for the installer, the Common Inventory Technology installation image and expansion of the image. • 4 GB for other temporary files. The default location is /var/tmp for these files. If you want to use a different location, allocate 4 GB in that directory and specify the directory in the **Temp Location** field in the installer. **Note:** Permissions for /var/tmp must be set to 1777. The 777 means that any user can read or write to the directory. The initial 1 means that only the owner of a file in the directory can modify or delete the file. This is the default permission setting for the directory.
Image repository	The location where you are storing installation images. This directory is used for both downloaded image and CD-ROM installations.	5 GB
Tivoli Provisioning Manager, the device manager federator and the dynamic content delivery management center	/opt/ibm/tivoli/tpm (default)	6.5 GB (4.5 GB + 2 GB for future updates)
The agent manager	/opt/IBM/AgentManager (default)	200 MB (150 MB + 50 MB for future updates)
Common Inventory Technology (used for discovery of installed components)	/opt/tivoli (cannot be changed)	300 MB (250 MB + 50 MB for future updates)
WebSphere Application Server	/opt/IBM/WebSphere/AppServer (default)	3 GB (2 GB + 1 GB for future updates)
DB2 server	/opt/IBM/db2/V8.1 (cannot be changed)	2.5 GB (2 GB + 500 MB for future updates)

Table 8. Required disk space on the Tivoli Provisioning Manager computer (continued)

Component	Location	Disk space
DB2 database files	The server instance location. For example, `/home/db2inst1/sqllib`, if `db2inst1` is the instance owner on the DB2 server.	3.5 GB for the database created during installation. Additional space is required for growth of the database. See "Disk space for database growth" on page 18.

Table 9. Required disk space for a database server on a separate computer

Component	Location	Disk space
DB2 database files	The server instance location. For example, `/home/db2inst1/sqllib`, if `db2inst1` is the instance owner on the DB2 server.	3.5 GB for the database created during installation. Additional space is required for growth of the database. See "Disk space for database growth" on page 18.

Examples

Table 10. Installation example 1

Requirement	Selected option
Topology	One-node topology
Preinstalled applications	None
Installation method	CD-ROM disks
Changes to default directories?	No
Number of managed endpoints	50 000
Disk space by component	**Temporary files** 5.2 GB • 400 MB in / • 1.2 GB `var/tmp` for the installer • 4 GB in `var/tmp` for other temporary files **Image repository** 5 GB for CD-ROM installation **Tivoli Provisioning Manager** 6.5 GB **The agent manager** 200 MB **Common Inventory Technology** 200 MB **WebSphere Application Server** 3 GB **DB2 server** 2.5 GB **DB2 database files** 53.5 GB. 3.5 GB for installation and 50 GB for database growth.

Table 10. Installation example 1 (continued)

Requirement	Selected option
Total disk space	76.2 • 26.2 GB for installation • 50 GB for growth of the database

Table 11. Installation example 2

Requirement	Selected option
Topology	Two node, DB2 server on a separate computer.
Preinstalled applications	• DB2 server is preinstalled on the second node. • DB2 client is preinstalled on the Tivoli Provisioning Manager computer. • An existing WebSphere Application Server installation at the required version level is already installed.
Installation method	Installation images
Changes to default directories?	Yes. • Tivoli Provisioning Manager will be installed in `/opt/tivoli/provision` instead of the default directory. • You want the installer to put user temporary files in `/tmp/tivoli`.
Number of managed endpoints	50 000
Disk space by component	**Temporary files** 5.2 GB • 400 MB in `/` • 1.2 GB `/tmp/tivoli` for the installer • 4 GB in `/tmp/tivoli` for other temporary files **Image repository** 5 GB **Tivoli Provisioning Manager** 6.5 GB **The agent manager** 200 MB **Common Inventory Technology** 200 MB **WebSphere Application Server** 0 MB. The application is already installed. **DB2 server** 0 MB. The files are preinstalled. **DB2 database files** 53.5 GB on the database server. 3.5 GB for installation and 50 GB for database growth.
Total disk space	70.7 • 17.2 GB for installation on the Tivoli Provisioning Manager computer • 3.5 GB for database files on the database server. • 50 GB for growth of the database on the database server.

Disk space for database growth

Ensure that you allocate additional disk space for growth of the database and log files. The required disk space depends on various factors, including the configuration of the database and the number of managed endpoints. For example, if you are managing 50,000 endpoints, allocate 50 GB of free disk space.

Consider storing the database on a separate, dedicated storage device so that performance is not affected by other applications accessing the same device.

Preinstallation Step 5: Set up required users

Several operating system users are required by Tivoli Provisioning Manager.

Default installation

- Required users and groups are created for you as shown in Table 13.
- The following additional requirements must be configured for the root user:
  - The umask must be set to `002` for the `root` user. Make the following changes:

Table 12. Setting umask for root

Shell used by `root`	Required setting
Korn	In home directory for `root`, add the following line to the file `.profile` `umask 002`
Bash	In home directory for `root`, add the following line to the files `.bash_profile` and `.bashrc` `umask 002`

    If a umask setting already exists, change the value to `002`. You can return the setting to its original value after installation.
  - User limits for the root user must be configured so resources available to perform the installation. See "User limits" on page 20 for information about the limits required by the root user.

Table 13. Tivoli Provisioning Manager users

User name		Primary group	Secondary group
tioadmin	This user name is used for the following users. • Tivoli Provisioning Manager system administrator. The user for installing the product and starting and stopping the provisioning server after installation. • The DB2 database instance owner. • The DB2 fenced user.	tioadmin	• tivoli
admin (default)	The default Web interface administrator.		

If user with the same name as a required user already exists:

- The installer modifies the existing user settings to meet installation requirements.
- You must specify the existing password for the user during installation. The installer will not change the password for an existing user.

During installation, the groups are also created if they do not exist, and the required users are assigned to them.

Custom installation

To ensure compliance with the security policies for user accounts, user permissions, and passwords in your organization, you must create required users before installation and verify that you can log on with the user name and password.

1. Create required users and assign them to the required primary and secondary groups as indicated in the following table. If you preinstalled the database in "Preinstalling applications for your topology" on page 14, database users are already created.

   If you are not familiar with creating users and groups, see "Creating users and groups" on page 135 for basic instructions. Refer to your operating system documentation for additional information.

Table 14. Tivoli Provisioning Manager users

User	User name	Primary group	Secondary group	Default shell
The user who owns the Tivoli Provisioning Manager installation and starts Tivoli Provisioning Manager services.	tioadmin[1]	tioadmin[1]	• tivoli • db2grp1[5]	Bash
The default user for logging on to the Web interface. You can use the default user name or specify a different user name.	admin[2] (default)			Bash
For DB2: The DB2 fenced user.	db2fenc1	db2fgrp1		Bash
For DB2: The DB2 instance owner.	db2inst1	db2grp1		Bash

[1] You must use the name `tioadmin` for the user name and user group. You cannot chose a different name.

[2] You cannot use the name `tioadmin` for the Web interface administrator. A separate user name is required.

[5] You must assign the user `tioadmin` to the same group that you set as the primary group for the database administrator user.

User name requirements

- User names can only contain English alphanumeric characters or the following characters: period (.), at sign (@) number sign (#), plus sign (+), hyphen (-), and underscore (_).
- DB2 places the following restrictions on DB2 user names:
  - Names cannot begin with a number or with the underscore character.
  - Names must be in lower case.
  - Group names can contain up to 8 characters.
  - User names can contain up to 8 characters.
  - Names and IDs cannot:
    - Be USERS, ADMINS, GUESTS, PUBLIC, LOCAL or any SQL reserved word
    - Begin with IBM, SQL or SYS.

Password requirements

- Ensure that the password is not configured to expire at next login. Log in with the user name and password to verify that the password is not expired and that you know the correct password. Set the number of days for the password expiry period according to your password policy.

- Ensure that you can make an SSH connection with each user name and password. On some systems, users must change their password when they make their first SSH connection.
- Some restrictions apply to passwords that you can use. Verify the following requirements:
  - Passwords can only contain English alphanumeric characters or the following characters: period (.), at sign (@) number sign (#), plus sign (+), hyphen (-), and underscore (_).
  - If you are using DB2 as your database, the following rules apply to DB2 user passwords. Refer to your DB2 documentation for further information.
    - Passwords can be a maximum of 8 characters.
    - Passwords cannot begin with an ampersand (&).

Home directory requirements

- A home directory for each user must exist as `/home/user_name` where `user_name` is the user name.
- Verify that the `root` user has write access to each home directory. You can test write access by logging on as `root` and running the **touch** command.

  ```
  touch filename
  ```

  If write access is permitted, the time stamp of the specified file is updated. If the file does not exist, it is created.
- The user must have 755 permissions to the home directory. The permission can be set in the operating system or using a file system access control list.

  Note: If you preinstalled DB2, the database instance owner, `db2inst1` home directory already has the required permissions and must not be changed.
- The home directory for `db2inst1` must have the following files

  ```
  .bash_profile
  .bashrc
  ```

  .

2. The umask must be set to `002` for the `root` user. Make the following changes:

Table 15. Setting umask for root

Shell used by `root`	Required setting
Korn	In home directory for `root`, add the following line to the file `.profile` `umask 002`
Bash	In home directory for `root`, add the following line to the files `.bash_profile` and `.bashrc` `umask 002`

If a umask setting already exists, change the value to `002`. You can return the setting to its original value after installation.

User limits

The users `root` and `db2inst1` must have sufficient disk space, memory, and permissions to successfully install Tivoli Provisioning Manager.

The preinstallation script checks disk quota values and the following **ulimit** limits:

- data segment size

- physical memory size
- stack size
- maximum CPU time
- virtual memory size
- maximum file size

Ensure that the users `root` and `db2inst1` have unlimited file system and memory resources for the types of limits listed above. To verify current resource limits, run the following command:

```
ulimit -a
```

Perform™ the following steps:

1. Log on as `root`.
2. Check the file `/etc/security/limits.conf`. When a limit is not specifically configured for a user, the default value is used. The default is typically `unlimited` for all the required limits except stack size.
   - Remove any existing entries for `db2inst1` so that the default limits are assigned. Ensure that the default limits are set to `unlimited`.
   - To change the stack size to the maximum value for `db2inst1` and `root`, add the following entries to the file:

     ```
     db2inst1 - stack unlimited
     root - stack unlimited
     ```
3. If DB2 is preinstalled, restart the database instance that the `db2inst1` user owns.

Also ensure that the disk quotas for `db2inst1` are large enough to meet all disk space requirements described in "Preinstallation Step 5: Set up required users" on page 18, including space for future growth of the database.

After installation, you can return the limits that you have changed to their original values.

Preinstallation Step 6: Verifying the environment

This section describes key environment requirements to check before running the installer. Some requirements cannot be validated by the installer, so ensure that you verify all requirements listed in this section.

Default installation

Table 16. Environment requirements

Software or system requirement	**Action**
Linux	On Red Hat Enterprise Linux Server release 5.1, the `tmpwatch` utility is installed. By default, the script runs daily and removes files in `/tmp` that have not been accessed in 10 days. The `anacron` scheduler also runs scripts in `etc/cron.daily` when the computer is booted. By default, the Tivoli Provisioning Manager installer is installed under `/tmp`. Before you start Tivoli Provisioning Manager installation, ensure that the automated cleanup of `/tmp` is disabled. 1. Check `/etc/crontab` and `/etc/anacrontab` to verify the scripts in `/etc/cron.daily` that are called. 2. If scripts in `/etc/cron.daily` are called, open the `/etc/cron.daily/tmpwatch` script and comment out the lines that perform the cleanup of `/tmp`.
Command prompt	The command prompt must end in one of the following three characters: $, #, >.

Table 16. Environment requirements (continued)

Software or system requirement	Action
Files left from a previous installation	Files and configuration settings that remain after some applications are uninstalled can cause an installation of Tivoli Provisioning Manager to fail. Ensure that you check for files and settings that need to be removed. **DB2** If DB2 was previously installed, ensure that registered DB2 instances are removed from `/etc/services`. A default installation uses port `50001` as the port for communicating with DB2. If this port is registered from a previous DB2 installation or used by another service, a default installation will fail. If you want to configure a different port for DB2, you must use a custom installation. **Tivoli Provisioning Manager** If you uninstalled Tivoli Provisioning Manager, ensure that the Tivoli Provisioning Manager installation directory has been deleted. The default location is /opt/ibm/tivoli/tpm. If this directory remains after uninstallation, reinstallation of the product will fail. **WebSphere Application Server** If WebSphere Application Server was previously installed on the computer, verify the following items: • Ensure that the WebSphere Application Server installation directory is deleted. The default location is /opt/IBM/WebSphere/AppServer. If this directory remains after uninstallation, reinstallation of the product will fail. • The `vpd.properties` file lists program components that are currently installed. It helps installers to recognize previous installations of WebSphere Application Server. When WebSphere Application Server is uninstalled, entries in `vpd.properties` are normally removed automatically. In some situations, however, the entries are not removed properly when WebSphere Application Server is uninstalled. If these entries remain when you start a Tivoli Provisioning Manager installation, the installer cannot properly validate whether WebSphere Application Server is installed and if WebSphere Application Server is currently running and installation will fail. Check the `vpd.properties` for entries that must be removed. The file is located the `root` directory. For more information about the file, see the following topic in the WebSphere Application Server information center: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.base.doc/info/aes/ae/rins_vpd.html
Antivirus software or process-intensive software	Check the Tivoli Provisioning Manager computer for processes that consume a lot of system resources, such as a scheduled thorough antivirus scan. These processes can cause some installation operations to time out. Stop or reschedule these processes before proceeding with installation.
Installation media	A read-only mounted drive cannot be used for installation images. Installing from images that are stored in a read-only mounted drive will fail.
Running applications	Close all programs so the installation program can update files as required.

Custom installation

Table 17. Environment requirements

Software or system requirement	**Action**

Hosts file	If you are using the file `/etc/hosts` to resolve IP addresses, the file must be configured correctly. The file must include:
	• The IP address, fully-qualified domain name, and host name of the computer where you are running the installer as the first entry.
	• The IP address `127.0.0.1`, the fully-qualified domain name `localhost.localdomain`, and the host name `localhost`
	
	The following example shows settings for a computer with the host name `river`.
	`#IP address  Fully Qualified Domain Name   Short Name`
	`10.0.0.12    river.example.com             river`
	`127.0.0.1    localhost.localdomain         localhost`
	
	Note: Linux installations differentiate between the IP address for the `localhost` host name and the actual host name of the computer. Ensure that your `/etc/hosts` file includes the static IP address for both `localhost` and the actual host name of the computer.

WebSphere Application Server 6.0.2.11	If you preinstalled WebSphere Application Server:
	
	Ensure that WebSphere Application Server is stopped:
	1. Change to the `bin` subdirectory of the WebSphere Application Server installation, the default is /opt/IBM/WebSphere/AppServer/`bin`.
	2. Run the command:
	`./stopServer.sh` *`app_server`* `-username` *`was_adminID`* `-password` *`password`*
	`app_server`
	The name of the application server. The default is `server1`.
	`was_adminID`
	The WebSphere Application Server administrator user name. After a new installation of Tivoli Provisioning Manager, the user name is `tioadmin`.
	`password`
	The WebSphere Application Server administrator password for the specified user name.
	
	Stop Java™ processes:
	
	Some Java processes might still be running and can cause installation to fail. Ensure that the processes are stopped.
	1. Run the following command:
	`ps -ef | grep java`
	2. If processes are still running, stop them with the command:
	`pkill -9 java`
	
	Version level:
	
	Do not apply fixes to WebSphere Application Server before Tivoli Provisioning Manager installation.

Table 17. Environment requirements (continued)

Software or system requirement	Action

DB2 Enterprise Server Edition 8.1, Fix Pack 11	If DB2 is preinstalled, ensure that it is running. To verify that DB2 is running:
	1. Switch to the DB2 instance owner. For a default installation, the Tivoli Provisioning Manager database owner is `tioadmin`. For a custom installation, the default Tivoli Provisioning Manager database owner is `db2inst1`.
	For example, if the instance owner is `db2inst1`, run the command.
	`su - db2inst1`
	2. Run the command to start DB2:
	`db2start`
	DB2 is started if it is not running already. If DB2 is already running, the following message is displayed.
	`SQL1026N The database manager is already active`

Linux	On Red Hat Enterprise Linux Server release 5.1, the `tmpwatch` utility is installed. By default, the script runs daily and removes files in `/tmp` that have not been accessed in 10 days. The `anacron` scheduler also runs scripts in `etc/cron.daily` when the computer is booted. By default, the Tivoli Provisioning Manager installer is installed under `/tmp`. Before you start Tivoli Provisioning Manager installation, ensure that the automated cleanup of `/tmp` is disabled. 1. Check `/etc/crontab` and `/etc/anacrontab` to verify the scripts in `/etc/cron.daily` that are called. 2. If scripts in `/etc/cron.daily` are called, open the `/etc/cron.daily/tmpwatch` script and comment out the lines that perform the cleanup of `/tmp`.
Command prompt	The command prompt must end in one of the following three characters: $, #, >.

Table 17. Environment requirements (continued)

Software or system requirement	Action
Files left from a previous installation	Files and configuration settings that remain after some applications are uninstalled can cause an installation of Tivoli Provisioning Manager to fail. Ensure that you check for files and settings that need to be removed. **DB2** If DB2 was previously installed, ensure that registered DB2 instances are removed from `/etc/services`. The default port for communicating with DB2 is `50001`. If you reinstall Tivoli Provisioning Manager and you specify a DB2 port that is already registered or is in use by another application, installation will fail. If you want to choose a different port, you can specify an available port number in the installer. **Tivoli Provisioning Manager** If you uninstalled Tivoli Provisioning Manager, ensure that the Tivoli Provisioning Manager installation directory has been deleted. The default location is /opt/ibm/tivoli/tpm. If this directory remains after uninstallation, reinstallation of the product will fail. **WebSphere Application Server** If WebSphere Application Server was previously installed on the computer, verify the following items: • Ensure that the WebSphere Application Server installation directory is deleted. The default location is /opt/IBM/WebSphere/AppServer. If this directory remains after uninstallation, reinstallation of the product will fail. • The `vpd.properties` file lists program components that are currently installed. It helps installers to recognize previous installations of WebSphere Application Server. When WebSphere Application Server is uninstalled, entries in `vpd.properties` are normally removed automatically. In some situations, however, the entries are not removed properly when WebSphere Application Server is uninstalled. If these entries remain when you start a Tivoli Provisioning Manager installation, the installer cannot properly validate whether WebSphere Application Server is installed and if WebSphere Application Server is currently running and installation will fail. Check the `vpd.properties` for entries that must be removed. The file is located the `root` directory. For more information about the file, see the following topic in the WebSphere Application Server information center: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.base.doc/info/aes/ae/rins_vpd.html
Antivirus software or process-intensive software	Check the Tivoli Provisioning Manager computer for processes that consume a lot of system resources, such as a scheduled thorough antivirus scan. These processes can cause some installation operations to time out. Stop or reschedule these processes before proceeding with installation.
Installation media	A read-only mounted drive cannot be used for installation images. Installing from images that are stored in a read-only mounted drive will fail.
Running applications	Close all programs so the installation program can update files as required.

Preinstallation Step 7: Prepare installation media

The Tivoli Provisioning Manager package includes installation media for, Tivoli Provisioning Manager and prerequisite software. There are two forms of installation media:

- Product CDs or DVDs.

- The IBM Passport Advantage® Web site. Licensed customers can download installation images for each of the CDs.

Using installation images instead of disks can reduce installation time.

Note:

- You must use installation images for a silent installation because the installer does not prompt for media when running silently.

Perform the following steps to create the directory structure for a central installation image repository

1. Download the software from Passport Advantage. Information about the download is described in the download document:

   http://www.ibm.com/support/docview.wss?rs=1015 &uid=swg24017302http://www.ibm.com/support/docview.wss?rs=1016 &uid=swg24017304http://www.ibm.com/support/docview.wss?rs=59 &uid=swg24017305
2. Place all the downloaded installation images in a single directory on the computer where you are running the installer. For example, `/install_images`.
3. Extract the contents of **Disk 1**. Do not extract the contents of the other downloaded installation images. The contents will be extracted automatically during installation.

The installation images are now ready. During installation, you will be prompted for the **Root directory for the images**. Specify the installation image directory that you have set up.

Chapter 3. Installing Tivoli Provisioning Manager

The Tivoli Provisioning Manager installer is a wizard that prompts you for all the information required for installation. If you are performing multiple installations or if you want to perform an unattended installation with predefined settings, you can run the installer in silent mode. For information about performing a silent installation, see Appendix C, "Performing a silent installation," on page 111.

- If you encounter errors during installation, see Chapter 6, "Recovering from installation errors," on page 75.
- You can click **Cancel** at any time to end the installation.

Approximate installation time

- Initialization of the installer: 2 minutes
- Specifying options in the installer: 5 minutes for a default installation. 15-20 minutes for a custom installation.
- Installation of the software: 2.5 hours. If a prerequisite application is already installed, the installation time is shorter.

To make it easier to complete the installation wizard, this chapter is divided into sections for the main stages of the installation as shown in the following diagram:

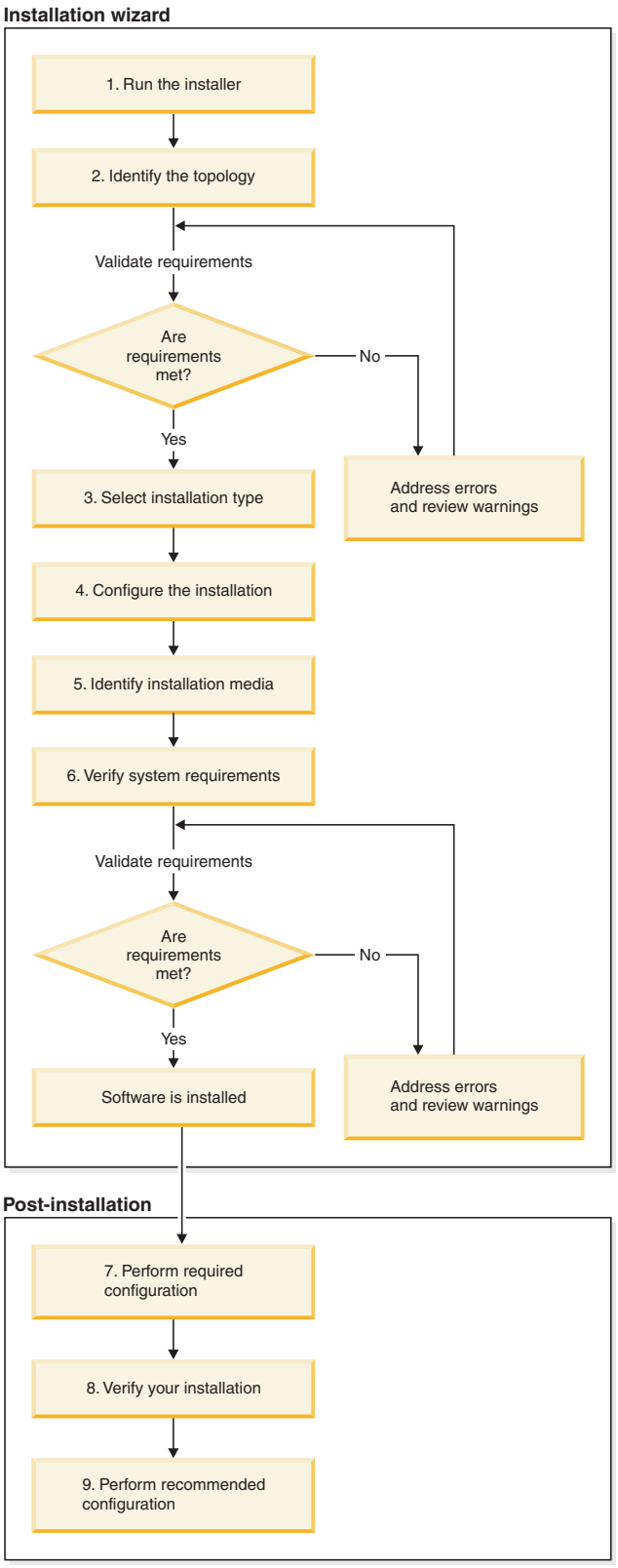

Figure 4. Installation roadmap

Installation Step 1: Run the installer

To start the Tivoli Provisioning Manager wizard:

Important: Before you begin, ensure that you meet all the requirements described in Chapter 2, "Preinstallation checklist for Linux on System z," on page 9.

1. Log on as `root`.

   Note: If you are using the `su` command to change to root, ensure that you use `su -`. Note the hyphen after `su`.

2. Start the installer:

   For disks:

   a. Insert the first disk and mount the CD-ROM drive, but do not change directory to the mount point.

      Note: Changing directories to the mount point will lock the CD-ROM and prevent you from being able to swap CDs. You must unmount the CD-ROM before trying to eject the CD. Otherwise the CD-ROM tray will be locked and you will be unable to switch CDs.

   b. If you are using CDs, type *`mount_point`*`/install.sh`. Replace *`mount_point`* with the mount point for Disk 1.

   For downloaded images:

   a. Change to the directory where you extracted the contents of **Disk 1**.

   b. Run `./install.sh`.

   Additional parameters:

   The following optional parameters can be used to run the installer

   -locale

   The installer attempts to detect the language configured for the computer. If the locale cannot be detected correctly, use the command `install.sh -locale`. For example, if the locale is Japanese and you want to start the installer in Japanese, run the following command:

   `./install.sh -locale ja_JP`

   -tiLocation *directory*

   Specifies a different temporary directory for installer files. Use this option if the default user temporary directory does not have sufficient disk space or if you want to use an alternate user temporary directory.

   The files for the installer are extracted and configured on the computer. This process takes about 2 minutes. When the configuration is complete, the **Welcome** panel is displayed.

3. Click **Next** to continue with the installation.

4. On the **Software License Agreement** panel, review the terms of the license agreement. You must accept the license agreement to proceed with installation. Click **Accept** to accept the terms of the agreement. If you click **Decline**, you cannot proceed with the installation.

The **Configure the target servers** is displayed. Proceed to the next section.

Installation Step 2: Identify the topology

In this part of the installation, you specify information about the computer where you are installing Tivoli Provisioning Manager, identify your database server, and select the installation type.

1. On the **Configure the target servers** panel, specify information about the Tivoli Provisioning Manager computer and your installation. For most fields, values are automatically detected or are set to defaults.

   Note: If you need to scroll contents of the panel, but the scroll bar is not visible, resize the window until the scroll bar appears.

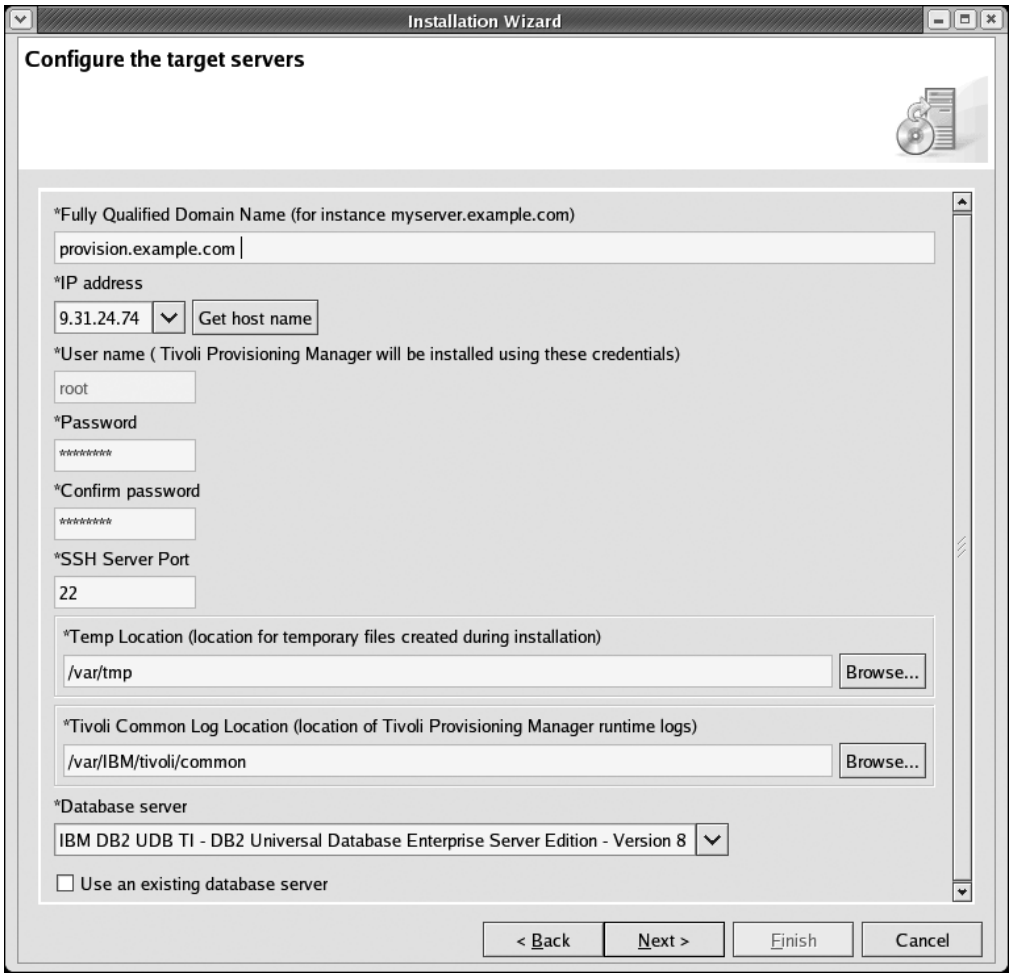

Figure 5. Configure the target servers panel

Fully Qualified Domain Name
The fully-qualified domain name of the computer associated with the IP address specified in the **IP address** field. For example, `tpmserver.example.com`. A computer can have multiple fully-qualified domain names, so ensure that the one that you select is the one that you are using for Tivoli Provisioning Manager.

IP address
Specify the IP address of the computer. This is the static IP address that you have assigned to the computer for Tivoli Provisioning Manager.

You can click **Get Host Name** to obtain the host name of the server using the specified IP address and update the **Fully Qualified Domain Name** field.

User name

Type `root`.

Password

Type the password for `root`.

Confirm password

Retype the password for `root`.

Tivoli Common Log Location
Specify the location for Tivoli Provisioning Manager runtime log files, this includes logs for starting and stopping the provisioning server and for the product engines. The default is /var/ibm/tivoli/common. Ensure that there are no extra spaces before or after specified path.

SSH Server Port
Specify the port used for SSH connections. The default is port 22.

Temp Location
Specify the default location for temporary files created during installation. The default is `/var/tmp`. Ensure that there are no extra spaces before or after specified path.

Database server
Select the database server from the options provided.

Use an existing database server
If you preinstalled the database server, select this check box.

Note: This option is not available for a default installation.

Database Server Fully Qualified Domain Name
Specify the fully-qualified domain name of the computer where you installed the database server. This field is only available if you have selected the **Use an existing database server** check box.

2. Click **Next**.

   The **Target servers validation** panel is displayed. The installer checks for credentials, root privileges, and prerequisites. It also discovers components.
3. The **Validation summary** page displays the results of validation. Correct any validation errors and review any validation warnings.

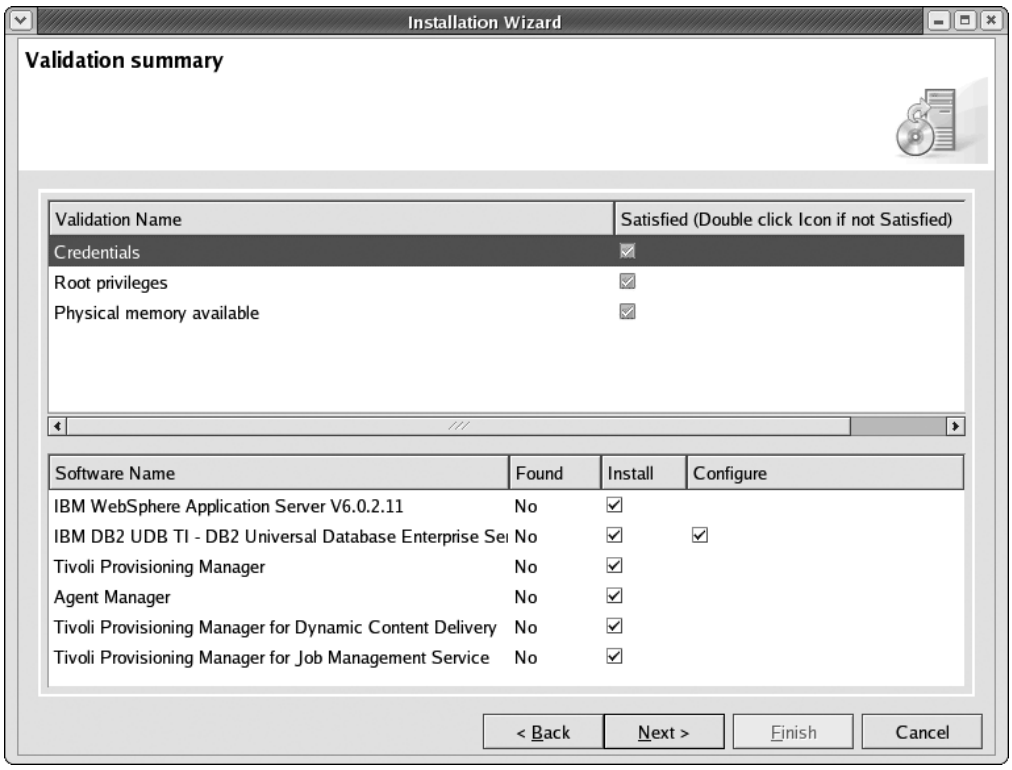

Figure 6. Validation summary panel

Validation table

Lists the prerequisites that were checked and the status of the validation. Validation includes:

- Verifying the password for the computer.
- Verifying hardware and software prerequisites.

Validation Name

The name of the requirement.

Satisfied

A check mark appears if the target server passes the validation. An **X** icon appears if a prerequisite is not met and must be fixed to continue. A **!** icon appears if there is a warning that you must review before continuing with installation. Double-click the row with the unsatisfied requirement for more information.

Software table

Lists the status for each piece of prerequisite software required for installation. Preinstalled software must be at the correct product level, including all required updates. Previous product levels or multiple installations of the same application at different levels are not supported. See "Prerequisite applications" on page 88 for information about the required product levels.

Software Name

The name of the software.

Found Displays **Yes** if the software is found. Displays **No** if it is not found.

Install Select the **Install** check box to install the required software component. You cannot install the software component if an existing installation was found.

Configure
Select the **Configure** check box to configure the required software.

Note: The **Configure** checkbox is only available for the **Database software entry** and it should always be selected unless the Tivoli Provisioning Manager database already exists due to a previous installation attempt.

4. Click **Next**. The **Select the installation method that you want to perform** panel is displayed. Proceed to "Installation Step 4: Configure the installation" on page 34.

Installation Step 3: Select the installation type

If your computer meets requirements for a default installation, you can select an installation type. Otherwise, only the custom installation option is available. For example, if DB2 Enterprise Server Edition 8.1, Fix Pack 11 is already installed, you must use the custom installation option because the default installation does not support an existing installation of DB2.

Select the type of installation to perform and then proceed to "Installation Step 4: Configure the installation" on page 34. For a comparison of the installation types and considerations for selecting an installation type, see "Installation types" on page 2.

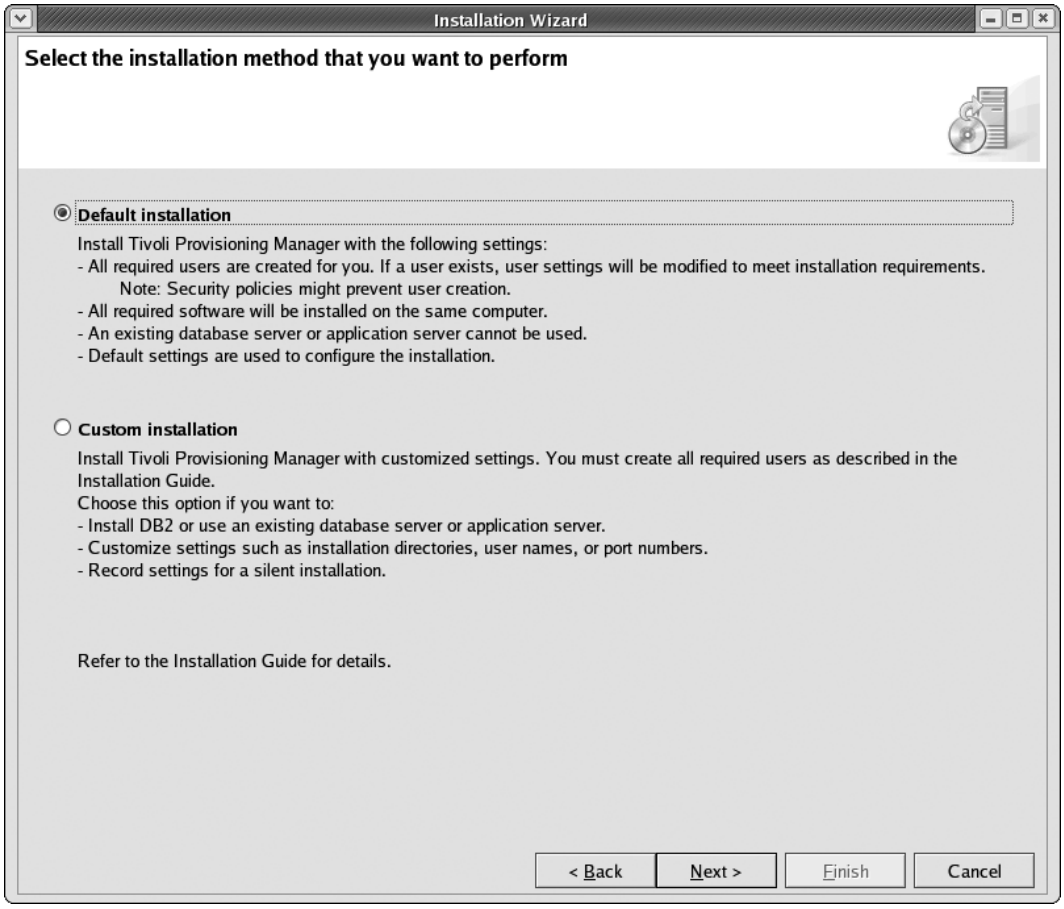

Figure 7. Select the installation method that you want to perform panel

Installation Step 4: Configure the installation

Specify information about how to configure the installation.

Default installation

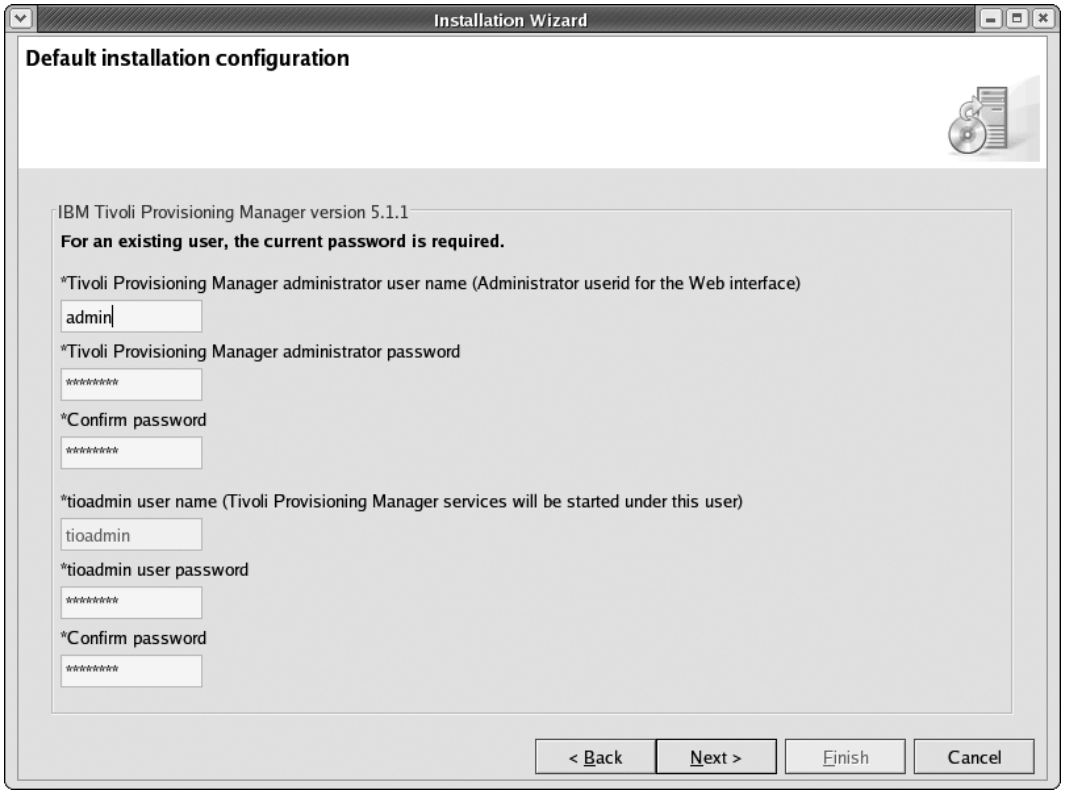

Figure 8. Default installation configuration panel

On the **Default Installation Configuration** panel, specify the required information. The installer uses the information that you have specified so far and configures the remaining settings for the product using default values. When you complete installation, you can review information about the default values in Appendix A, "Values for a default installation," on page 99.

Tivoli Provisioning Manager administrator
: The Tivoli Provisioning Manager administrator is the default user for the Tivoli Provisioning Manager Web interface. Specify the user name for this user. The default is `admin`.

  Note: You cannot use the name `tioadmin` for this user.

Tivoli Provisioning Manager administrator password
: Specify the password for the Tivoli Provisioning Manager administrator.

Confirm password
: Retype the password for the Tivoli Provisioning Manager administrator.

tioadmin user name
: Displays the user name `tioadmin`. You cannot change this user name. It is the user name that starts Tivoli Provisioning Manager services and it is also used as the DB2 instance owner user name.

tioadmin password
: Specify the password for `tioadmin`.

Confirm password
: Retype the password for `tioadmin`.

Important: The following restrictions apply to specified passwords:

- Passwords can only contain English alphanumeric characters or the following characters: period (.), at sign (@) number sign (#), plus sign (+), hyphen (-), and underscore (_).
- The `tioadmin` user is used as the DB2 administrator. The following DB2 restrictions apply this user password. Refer to your DB2 documentation for further information.
  - Passwords can be a maximum of 8 characters.
  - Passwords cannot begin with an ampersand (&).

Custom installation

The **Custom option configuration** panel displays a tab for the applications that the installer will install or configure. Default values are automatically entered for most fields. Complete the additional required information on all tabs, and then click **Next** to proceed to the next panel in the wizard.

Important:

- The following limitations apply to user names and passwords on the tabs described in this section:
  - User names and passwords can only contain English alphanumeric characters or the following characters: period (.), at sign (@) number sign (#), plus sign (+), hyphen (-), and underscore (_).
  - For additional limitations on names and passwords that apply to DB2, see "Preinstallation Step 5: Set up required users" on page 18.
- Directory paths cannot contain a slash as the last character of the path `(/)`.

Tivoli Provisioning Manager tab

Specify settings to configure Tivoli Provisioning Manager.

Tivoli Provisioning Manager settings:

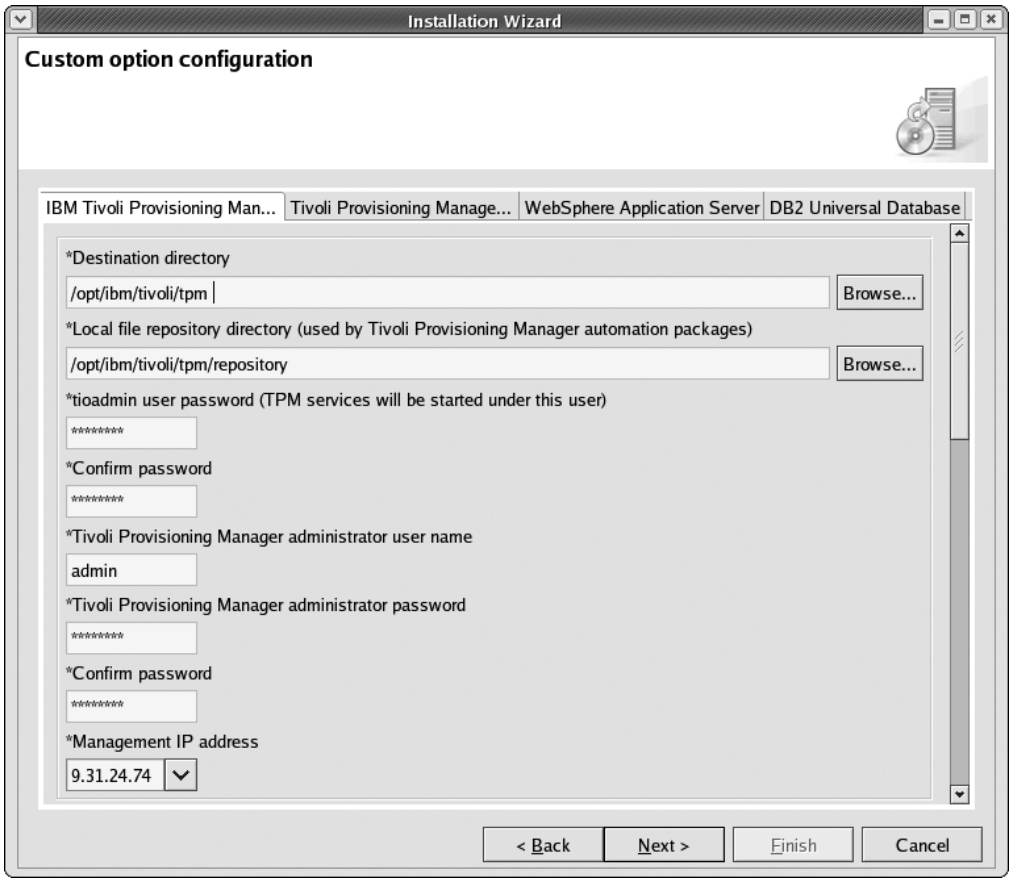

Figure 9. Tivoli Provisioning Manager configuration

Destination directory
Type the installation directory for Tivoli Provisioning Manager. Ensure that there are no extra spaces before or after specified path.

Local file repository directory
The installer will install software required by automation packages that perform installation configuration. Specify the directory where you want to store these files.

Important: Make sure that you specify a valid path. The installer does not validate the format of the path that you type. If you type the path in an invalid format, you cannot successfully apply a fix pack after installation. Check for typing errors and correct any mistakes. For example:

- Ensure that all directory separators in the path are in the right direction. Use the forward slash (/) to separate directories.
- Ensure that there are no extra spaces before or after specified path.

tioadmin user password
Type the password for the user `tioadmin`. This user starts Tivoli Provisioning Manager services.

Confirm Password
Type the password for the user `tioadmin`.

Tivoli Provisioning Manager administrator user name
Type the user name for the Tivoli Provisioning Manager administrator that you created in "Preinstallation Step 5: Set up required users" on page 18. This is the administrator user that you use to log on to the Web interface. The default user name is `admin`.

Tivoli Provisioning Manager administrator password
Type the Tivoli Provisioning Manager administrator password.

Confirm password
Type the Tivoli Provisioning Manager administrator password.

Management IP address
Select the IP address that corresponds to the network adapter that you are using to manage Tivoli Provisioning Manager.

WebSphere Application Server settings:

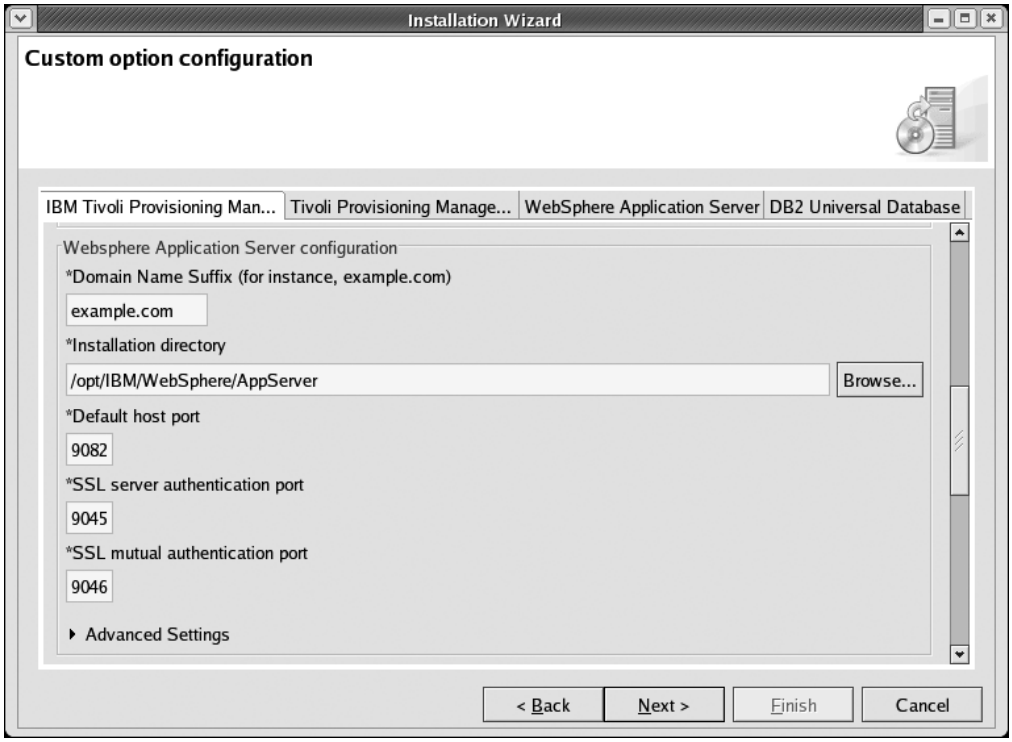

Figure 10. Tivoli Provisioning Manager configuration tab - WebSphere Application Server options

Domain Name Suffix
Type the value for the domain name portion of the fully-qualified domain name. For example, if your fully-qualified domain name is `tpmserver.admin.example.com`, the domain name suffix is `admin.example.com`. This information is used by WebSphere Application Server.

Installation directory
Displays the installation directory for WebSphere Application Server. Verify that the location is correct.

Default host port
The *default_host* port for WebSphere Application Server. The default port is 9082.

SSL server authentication port
A port using server side SSL to provide encryption and to authenticate WebSphere Application Server to the other servers. The default value is 9045.

SSL mutual authentication port
A port using mutually authenticated SSL. The default value is 9046.

Cell Name
This field appears if you preinstalled WebSphere Application Server. Specify the name of the WebSphere Application Server cell. The default is *hostname*Node01Cell, where *hostname* is the host name of the computer where WebSphere Application Server is installed.

Node Name
This field appears if you preinstalled WebSphere Application Server. Specify the name of the WebSphere Application Server node. The default is *hostname*Node01, where *hostname* is the host name of the computer where WebSphere Application Server is installed.

Advanced settings
The installer automatically creates a profile while installing WebSphere Application Server. You can review the default port number settings and accept the port settings recommended by the wizard or you can specify your own port settings. When you configure WebSphere Application Server or assign port numbers to other applications, you must avoid conflicts with other assigned ports. In addition, you must explicitly enable access to particular port numbers when you configure a firewall. For more information on the definition of the ports, refer to the WebSphere Application Server documentation.

Admin host port
WebSphere Application Server provides an *admin host*, which is the virtual host for the administrative console system application. The default port number is 9061.

Admin host secure port
The default port number is 9044.

Bootstrap port
The default port number is 2810.

SOAP connector port
The default port number is 8881.

SAS SSL server authentication listener port
The default port number is 9402.

CSIV2 SSL server authentication listener port
The default port number is 9404.

CSIV2 mutual authentication listener port
The default port number is 9403.

ORB listener port
The default port number is 9101.

DCS unicast port
The default port number is 9354.

SIB endpoint port
The default port number is 7277.

SIB endpoint secure port
The default port number is 7287.

SIB MQ endpoint port
The default port number is 5559.

SIB MQ endpoint secure port
The default port number is 5579.

DB2 settings:

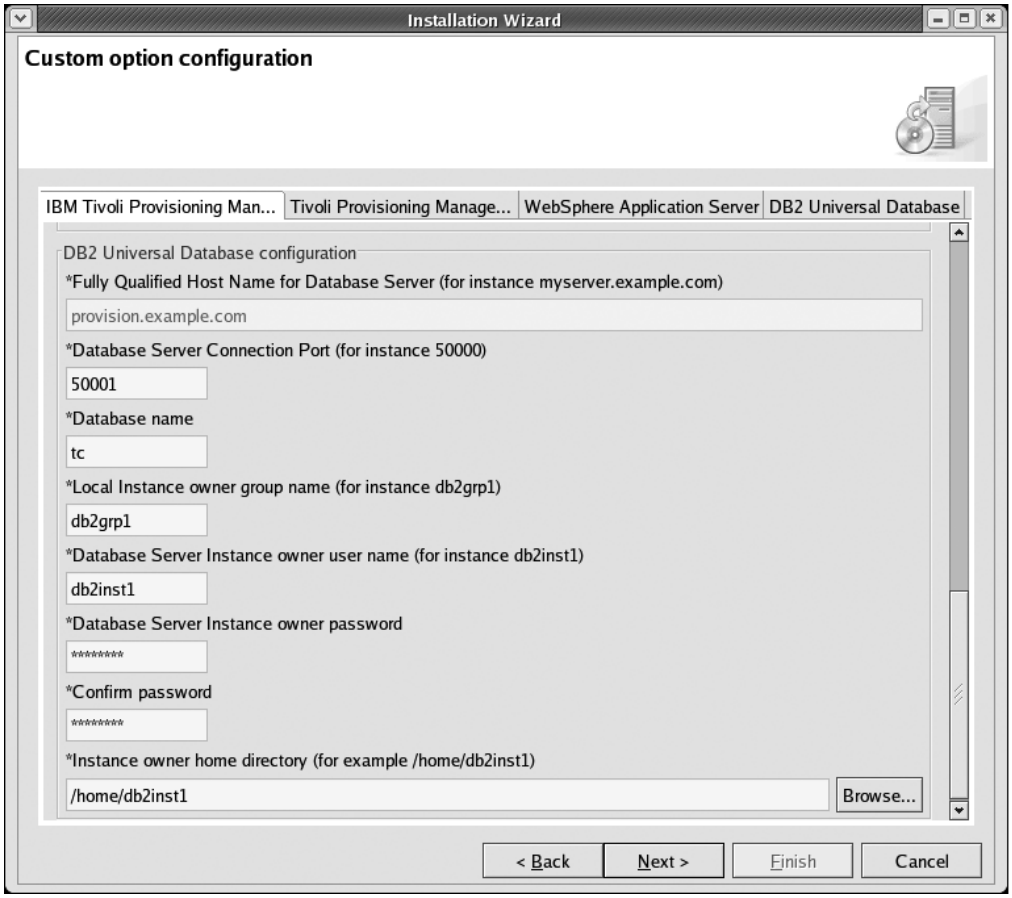

Figure 11. Tivoli Provisioning Manager configuration tab -DB2 options

Fully Qualified Host Name for Database Server
If DB2 is preinstalled, specify the fully-qualified domain name of the computer where the DB2 server is installed. If DB2 is not preinstalled, the fully-qualified domain name of the Tivoli Provisioning Manager computer is displayed.

Database Server Connection Port
Specify the TCP/IP port number that will be used by this server instance to listen for connection requests from clients. The default value is 50001 when it is installed with Tivoli Provisioning Manager. The default value is if you installed DB2 with the DB2 installer.

Database name
Specify the name of the DB2 database for Tivoli Provisioning Manager. The database name can only contain uppercase letters, lowercase letters, and numbers.

Local instance owner group name
Specify the name of the group for the DB2 instance owner. If the DB2 server is on a separate computer, use the group name of the DB2 client instance owner on the Tivoli Provisioning Manager computer. This group was created manually in "Preinstallation Step 5: Set up required users" on page 18 or by preinstalling DB2 as described in "Preinstalling DB2" on page 115. The default group name is `db2grp1`.

Database Server Instance owner user name
Specify the name of the DB2 instance owner. If the DB2 server is on a separate computer, specify the instance owner for the database on the DB2 server. This owner was created manually in "Preinstallation Step 5: Set up required users" on page 18 or by preinstalling DB2 as described in "Preinstalling DB2" on page 115. The user name `db2inst1` is the default user name for a DB2 installation. This user connects to the database server to manage data and controls all DB2 processes and owns all file systems and devices used by the databases contained within the instance. The default user is `db2inst1`.

Database Server Instance owner password
Specify the database instance owner password.

Confirm password
Type the password for the instance owner.

Instance owner home directory
Specify the home directory of the database instance owner user. Ensure that there are no extra spaces before or after specified path.

Tivoli Provisioning Manager Components Configuration tab

Specify settings for core components.

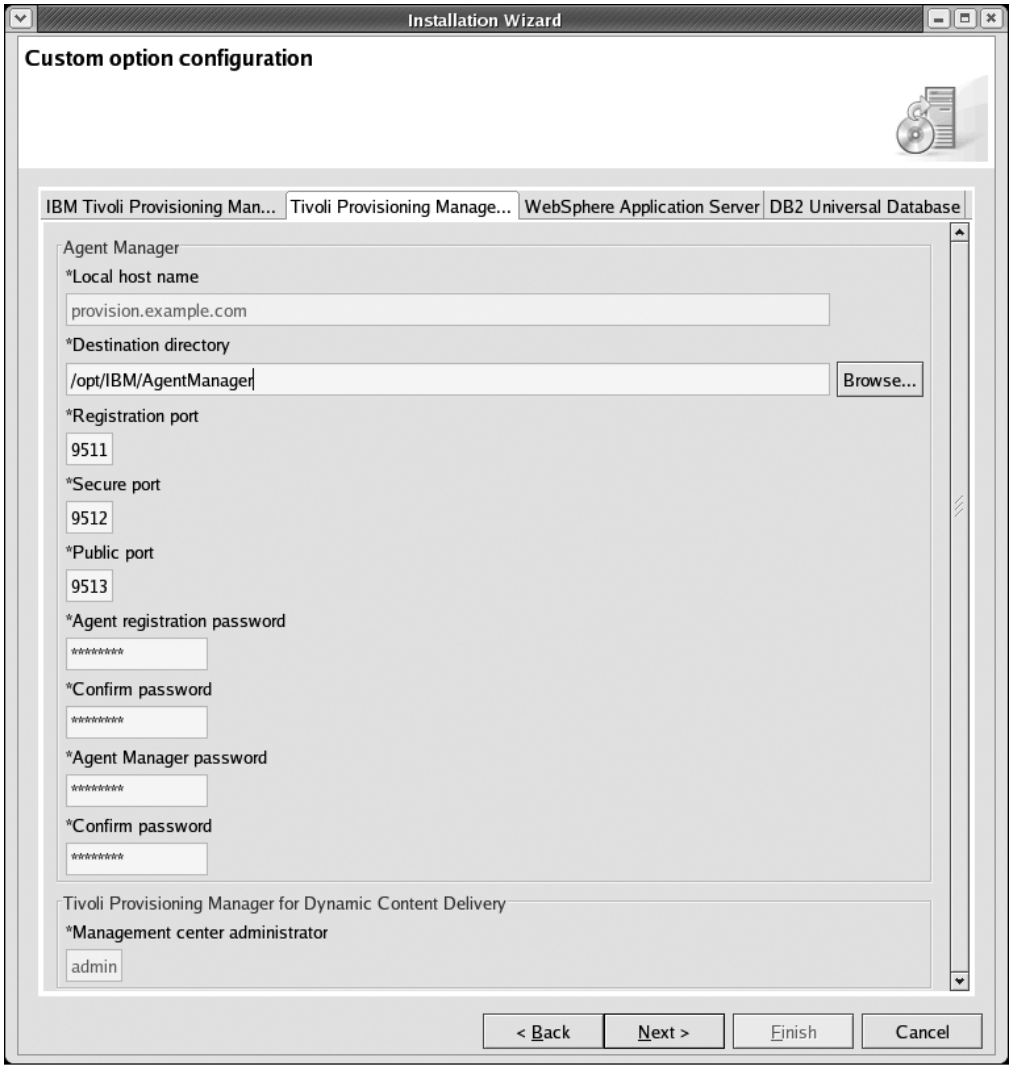

Figure 12. Tivoli Provisioning Manager components configuration

Agent Manager:

The agent manager is the server component of the common agent services. It enables secure connections between managed systems in your deployment, maintains the database of information about the managed systems and the software running on those systems, and processes queries against that database from resource managers. The agent manager is an X.509 registration authority and certificate authority as well as a registry with current configuration and addressability information for agents and resources managers. All network operations are exposed as Web services using SOAP over HTTP. You can review the default port number settings and accept the port settings recommended by the installer or you can specify your own port settings.

When you configure the agent manager or assign port numbers to other applications, you must avoid conflicts with other assigned ports. In addition, you must explicitly enable access to particular port numbers when you configure a firewall.

Local host name
Displays the host name of the Tivoli Provisioning Manager computer.

Destination directory
The installation directory for the agent manager. Ensure that there are no extra spaces before or after specified path.

Registration port
The registration port uses server side SSL to provide encryption and authenticate the agent manager to clients. The default value is `9511`.

Secure port
A port using server side SSL with client authentication to provide encryption and authenticate the agent manager to clients. The default value is `9512`.

Public port
An unsecured port. The default value is `9513`. For your security, avoid using port 80 for this port.

Agent registration password
A common agent must provide this password to register with the agent manager and to unlock the `agentTrust.jks` file. A common agent or resource manager compares the certificate in its copy of the `agentTrust.jks` file with the certificate presented by the agent manager to ensure that it registers with the correct agent manager. This password is used to create the common agent.

Confirm password
Type the agent registration password again.

Agent manager password
This password is used by the agent manager to create the Certificate Authority Certificate and to unlock the agent manager trust keystore (`agentManagerTrust.jks`) and keystore (`agentManagerKeys.jks`) files.

Confirm password
Type the agent manager password again.

Tivoli Provisioning Manager for Dynamic Content Delivery:

The dynamic content delivery management center provides for distribution of files to depot servers throughout a network. The management center is installed on the provisioning server, and manages uploads and downloads to and from depot servers.

Management center administrator
Displays the administrator user name for logging on to the dynamic content delivery management center console. The default user name is `admin`. By default, authentication is not enabled, so a password is not required for this user name.

WebSphere Application Server tab

This tab is displayed if WebSphere Application Server is not preinstalled.

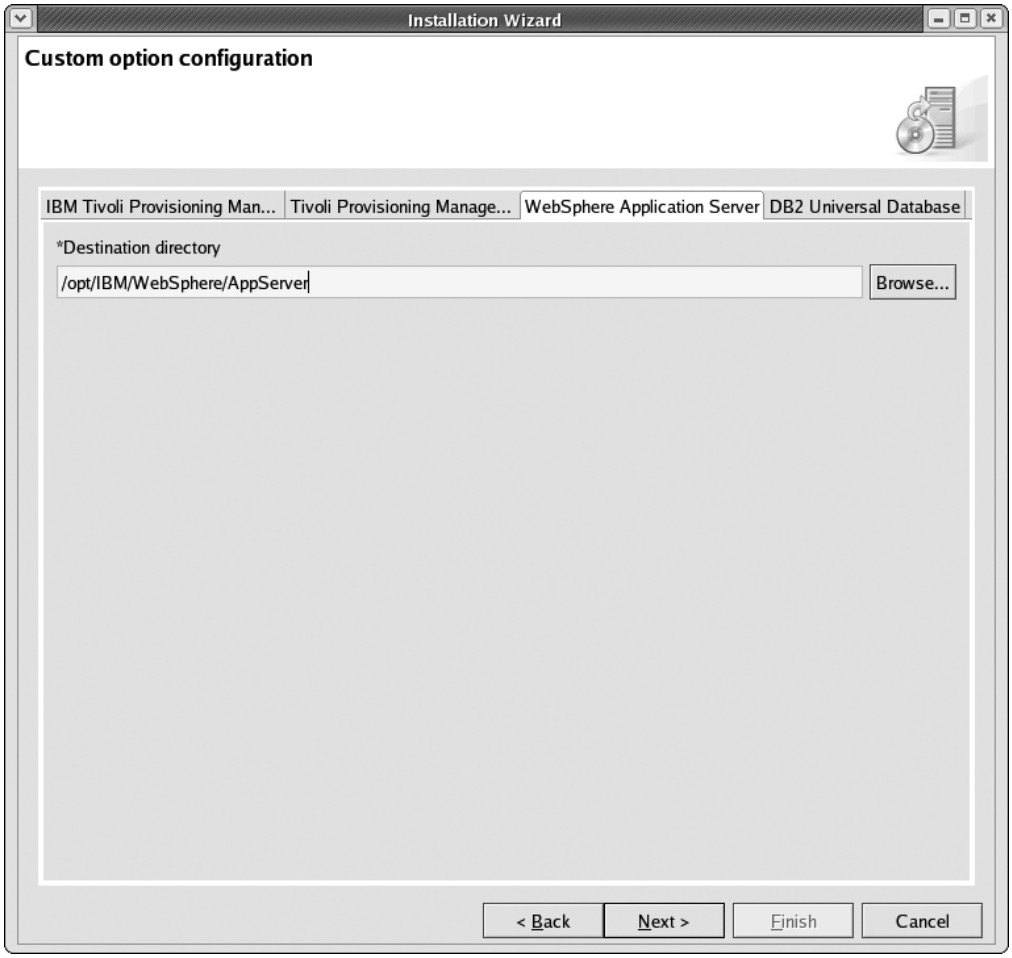

Figure 13. WebSphere Application Server configuration tab

Destination directory
Specify the directory where you want to install WebSphere Application Server. Ensure that there are no extra spaces before or after specified path.

DB2 tab

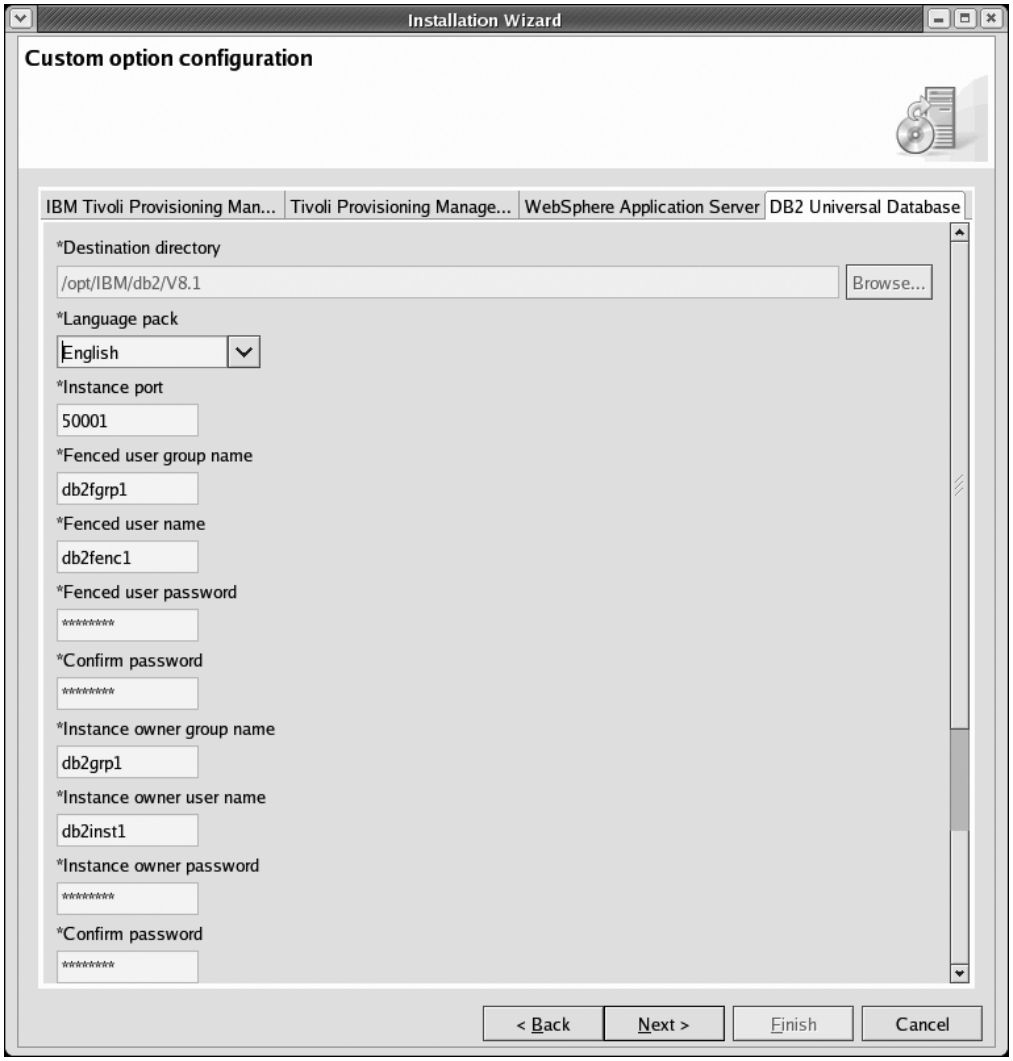

Figure 14. DB2 configuration tab

Destination directory
Displays the installation directory for DB2.

Language pack
Select the DB2 language pack that you want to install.

Instance port
Specify the TCP/IP port number that will be used by this server instance to listen for connection requests from clients. The default value is `50001`.

Instance owner user name
Specify the name of the DB2 instance owner. If the DB2 server is on a separate computer, specify the instance owner for the database on the DB2 server. This owner was created manually in "Preinstallation Step 5: Set up required users" on page 18 or by preinstalling DB2 as described in "Preinstalling DB2" on page 115. The user name `db2inst1` is the default user name for a DB2 installation. This user connects to the database server

to manage data and controls all DB2 processes and owns all file systems and devices used by the databases contained within the instance. The default user is `db2inst1`.

Instance owner password
Enter the password for the instance owner ID.

Confirm password
Retype the password for the instance owner.

Fenced user group name
Specify the name of the DB2 fenced group name. This group was created manually in "Preinstallation Step 5: Set up required users" on page 18 or by preinstalling DB2 as described in "Preinstalling DB2" on page 115. The default fenced group name is `db2fgrp1`.

Fenced user name
Specify the name of the DB2 fenced user name. This user was created manually in "Preinstallation Step 5: Set up required users" on page 18 or by preinstalling DB2 as described in "Preinstalling DB2" on page 115. The fenced user is used to run user defined functions (UDFs) and stored procedures outside of the address space used by the DB2 database. The default user is `db2fenc1`. If you do not need this level of security, for example in a test environment, you can use your instance owner as your fenced user.

Fenced user password
Specify the password for the fenced user.

Confirm password
Type the password for the fenced user again.

Instance owner group name
Specify the name of the group for the DB2 instance owner. If the DB2 server is on a separate computer, use the group name DB2 client instance owner on the Tivoli Provisioning Manager computer. This group was created manually in "Preinstallation Step 5: Set up required users" on page 18 or by preinstalling DB2 as described in "Preinstalling DB2" on page 115. The default group name is `db2grp1`.

Instance owner user name
Specify the name of the DB2 instance owner. If the DB2 server is on a separate computer, specify the instance owner for the database on the DB2 server. This owner was created manually in "Preinstallation Step 5: Set up required users" on page 18 or by preinstalling DB2 as described in "Preinstalling DB2" on page 115. The user name `db2inst1` is the default user name for a DB2 installation. This user connects to the database server to manage data and controls all DB2 processes and owns all file systems and devices used by the databases contained within the instance. The default user is `db2inst1`.

Instance owner password
Specify the database instance user password.

Confirm password
Retype the password for the instance owner.

Installation Step 5: Identify installation media

Specify the location of the software installation files.

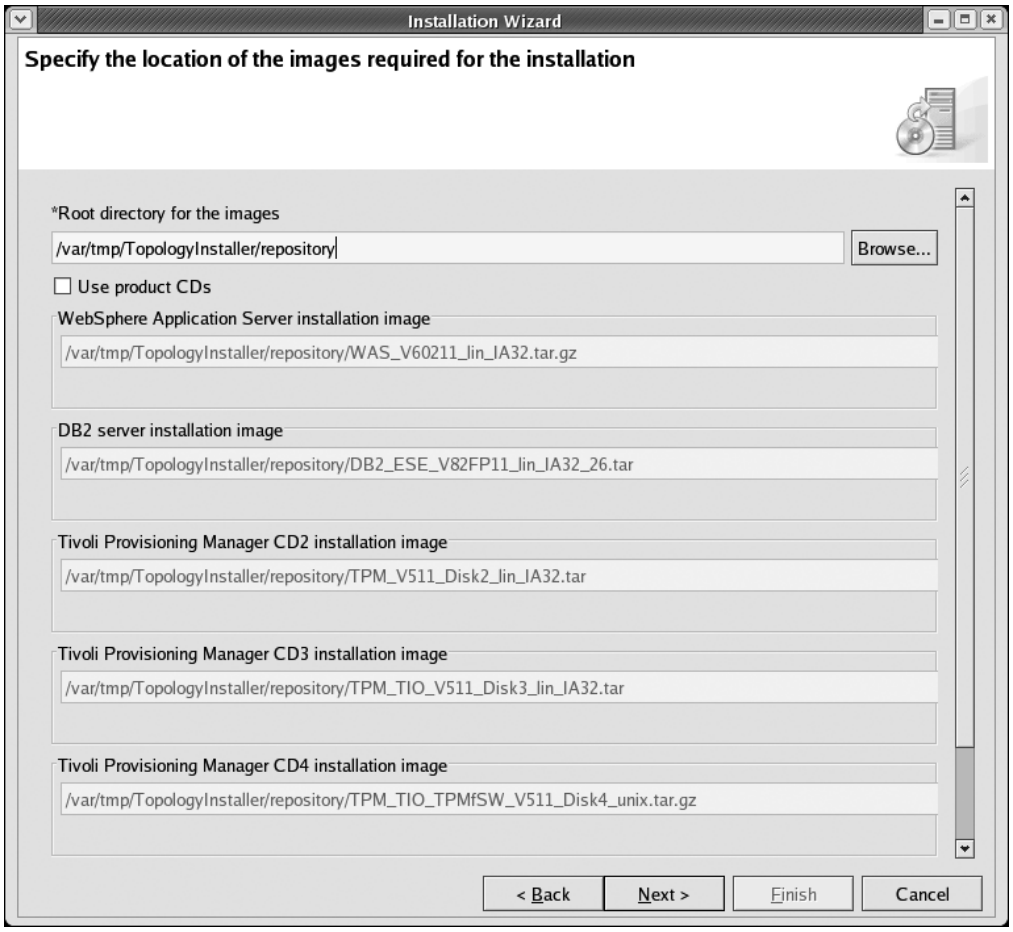

Figure 15. Installation image location panel

You can install the prerequisite software and Tivoli Provisioning Manager using the CD-ROM disks provided with Tivoli Provisioning Manager or using installation images. If you choose to install using installation images, you must copy all installation media to your hard drive or other file system. This includes all the prerequisite software media.

Note: For a silent installation, you must use installation images. If you are running the installer in record mode to create a response file, you must specify the location of installation images on this panel.

Root directory for the images
If you are using installation images, specify the root directory of your image repository that you created in "Preinstallation Step 7: Prepare installation media" on page 25. If you are using CD-ROM disks, specify the location where you want the installer to copy installation files from the disks. Ensure that there are no extra spaces before or after specified path.

Use product CDs
If you are using CD-ROM disks, select this check box.

When you are done, click **Next**. Check summaries are run on the installation files. The installer then validates the settings you have specified, available disk space, users, available memory on the target servers, and other requirements. It displays results on the **Validation summary** panel. Proceed to the next section.

Installation Step 6: Verify system requirements

The **Validation summary** panel indicates the results of validating system requirements and your installation options. When you have addressed errors and warnings on this panel, software installation can begin.

1. Review the information on the **Validation summary** panel. Correct errors and review warnings before continuing with installation.

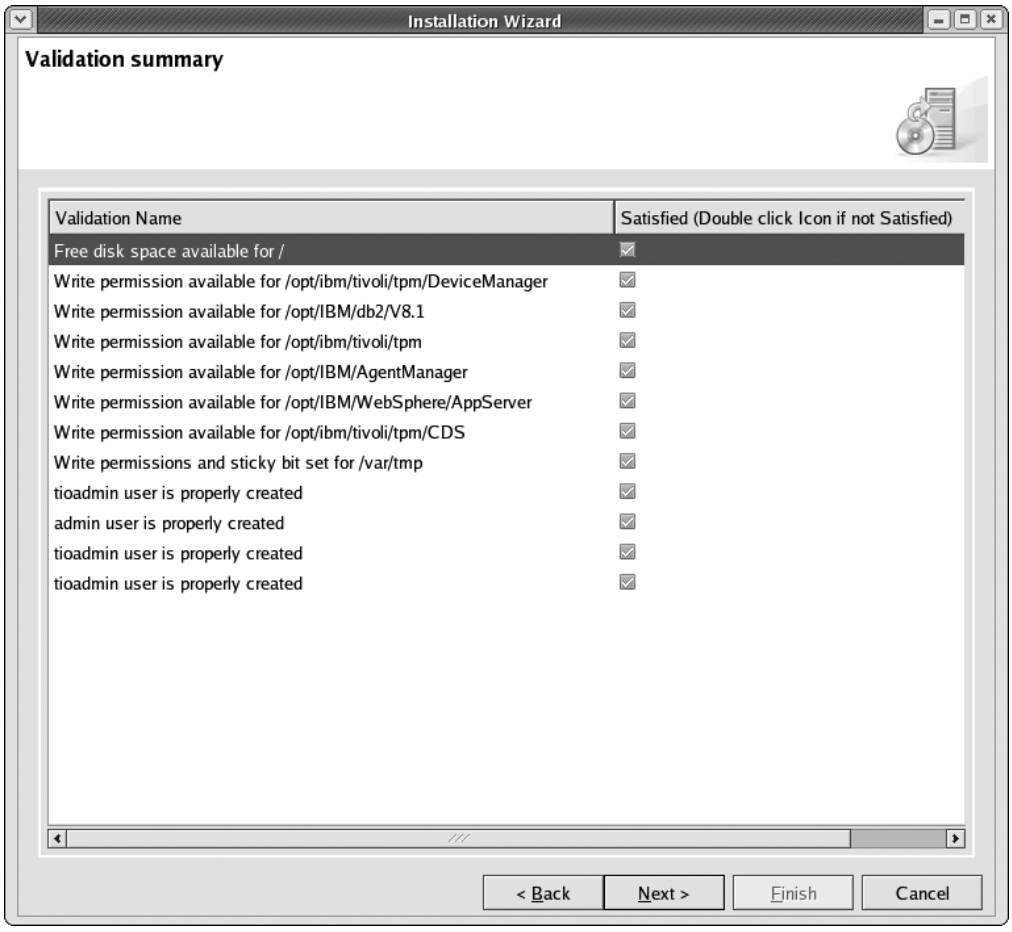

Figure 16. Second Validation summary panel

A check mark appears if the requirement is met. An **X** icon appears if a prerequisite is not met and must be fixed to continue. A **!** icon appears if there is a warning that you must review before continuing with installation. Double-click the row with the unsatisfied requirement for more information.

2. After you have addressed errors and warnings, click **Next**. The **Summary** panel displays a summary of your installation selections.
3. Review the summary information, and then click **Next** to proceed with the installation.

   A progress bar indicates the status of the installation tasks. To view the logs during the installation, click on the **Installation log** tab.

   The **Finish** panel is displayed when the installer completes its installation tasks.
4. Click **Next** and then click **Finish** to exit the installer.

5. Software installation is now complete. If you performed a default installation, you can review information about the values used for the installation in Appendix A, "Values for a default installation," on page 99.
6. You must perform some required configuration steps before using the product. Proceed to "Installation Step 7: Perform required configuration."

   Log files and recovery from errors:

   If you encountered an error during software installation, see Chapter 6, "Recovering from installation errors," on page 75 for information about installation log files and recovery from installation errors.

Installation Step 7: Perform required configuration

Some configuration is required after the product is installed. Ensure that you perform all the configuration described in this section. When you have completed the required configuration, you are ready to verify your installation. See Chapter 4, "Verifying installation," on page 53.

Updating WebSphere Application Server

If users log on to Tivoli Provisioning Manager and leave the session idle for longer than the HTTP Session timeout value configured in WebSphere Application Server, user information is not invalidated and user credentials stay active until the configured LTPA token timeout occurs.

To fix this behavior so that the user is automatically logged out after the HTTP Session timeout period, it is recommended that you install WebSphere Application Server Fix Pack 13 and above.

Requirements

- You must use the actual `root` user to extract the contents of the fix download and install the fix.
- For a Fix Pack, you need approximately 600 MB of free space in the system temporary directory. Another 600 MB is required in the file system that hosts the WebSphere Application Server installation. Space is also required for:
  - The *$WAS_HOME*/updateinstaller directory. The space required is about the same as the size of the Fix Pack, typically somewhere between 25 MB to 750 MB.
  - Backup files in the *$WAS_HOME*/properties/version/update/backup directory. The space required is about the same as the size of the Fix Pack, somewhere between 25 MB to 750 MB, varying by product and platform.
- Version 6.0.2.2 or newer of the Update Installer must be installed. Check the version level in file /opt/IBM/WebSphere/AppServer/updateinstaller/version.txt.

  If Update Installer is not installed, download it from the following link: http://www.ibm.com/support/docview.wss?rs=180&uid=swg24008401 and extract the contents under the *$WAS_HOME* directory. The files are extracted to a subdirectory called `updateinstaller`.

To install the fix and configure WebSphere Application Server:

1. Download the fix pack from its download page. Click the tab for your operating system to access the download you require.

   http://www.ibm.com/support/docview.wss?uid=swg24012915.

2. Extract the contents of the fix pack file to the *$WAS_HOME* directory. This unpacks the fix pack files into the *$WAS_HOME*/updateinstaller directory and subdirectories.
3. Stop WebSphere Application Server::
   a. Change to the bin subdirectory of the WebSphere Application Server installation, the default is /opt/IBM/WebSphere/AppServer/bin.
   b. Run the command:

      ./stopServer.sh *app_server* -username *was_adminID* -password *password*

      app_server
      The name of the application server. The default is server1.

      was_adminID
      The WebSphere Application Server administrator user name. After a new installation of Tivoli Provisioning Manager, the user name is tioadmin.

      password
      The WebSphere Application Server administrator password for the specified user name.
4. After stopping the provisioning server, some WebSphere client Java processes might still be running. Ensure that the processes are stopped.
   a. Run the following command:

      ps -ef | grep java

   b. If processes are still running, stop them with the command:

      pkill -9 java
5. **(Optional)** Delete the fix pack download file if you need more space.
6. Change to the *$WAS_HOME*/bin directory and run the following command:

   . ./setupCmdLine.sh

   Notice the space between the periods. The special format for this command sources the command to make the setting active for all processes started from the command shell.
7. Change to the *$WAS_HOME*/updateinstaller directory.
8. This step is only required if you are not using a fresh installation of WebSphere Application Server. Use the following command to clone the Java 2 Software Development Kit (SDK) that the product uses, so that you can update the original SDK when you install the maintenance package.

   ./update -silent -W relaunch.active=false
9. Launch Update Installer. In the *$WAS_HOME*/updateinstaller directory and run the following command:

   ./update -silent -W maintenance.package=./maintenance/6.0.2-WS-WAS-*platform*-FP00000023.pak

   Where *platform* is specific to your operating system. Check the file name in the *$WAS_HOME*/updateinstaller/maintenance directory.
10. Start WebSphere Application Server:

    $TIO_HOME/tioprofile/bin/startServer.sh server1
11. When the installation is complete, log on to the WebSphere Application Server administrative console as tioadmin at the following URL:

    https://*hostname*:*port*/admin

    where *hostname* is the fully-qualified domain name of theTivoli Provisioning Manager computer and *port* is the WebSphere Application Server **Admin host secure port** that you defined during installation. The default port number is 9044. For example:

    https://tpmserver.example.com:9044/admin

12. Click **Security > Global security**.
13. Under Custom properties, click **New**.
14. In the Name field, enter `com.ibm.ws.security.web.logoutOnHTTPSessionExpire`.
15. In the Values field, enter `true`.
16. Click **Apply and Save** to save the changes to your configuration.
17. Restart WebSphere Application Server.

Configuring a shared WebSphere Application Server environment

Custom installation only

If you installed Tivoli Provisioning Manager on a preinstalled installation of WebSphere Application Server that is hosting another profile, you must configure the default host port and default secure host port if the other profile is using the default ports 9080 and 9043.

1. Start the Tivoli Provisioning Manager profile **tioprofile** using the **startServer** command.

   ```
   $TIO_HOME/tioprofile/bin/startServer.sh server1
   ```

2. Log on to the WebSphere Application Server administration console as the WebSphere Application Server administrator.

   ```
   https://hostname:9043/ibm/console/logon.jsp
   ```

3. Navigate to **Servers** > **Application Servers** > **server1** > **ports**.
4. Change the value of **WC_defaulthost** to 9081.
5. Change the value of **WC_defaulthost_secure** to 9444.
6. Navigate to **Environment** > **Virtual Hosts** > **default_host** > **Host Aliases**.
7. Change port 9080 to 9081.
8. Change port 9043 to 9444.
9. Restart the profile **tioprofile**:

   ```
   $TIO_HOME/tioprofile/bin/stopServer.sh server1 -username wasadmin -password wasadmin
   $TIO_HOME/tioprofile/bin/startServer.sh server1
   ```

10. Start the other profile hosted by WebSphere Application Server. For example, to start the default profile, change to the `bin` subdirectory in the WebSphere Application Server installation location and run the **startServer** command.

    ```
    /opt/IBM/WebSphere/AppServer/bin/startServer.sh server1
    ```

Configuring the DB2 database registry

Custom installation only

If DB2 is installed on a separate computer from Tivoli Provisioning Manager, configure DB2 to reduce the possibility of database lock timeouts. DB2 is automatically configured with these settings if it is installed on the Tivoli Provisioning Manager computer.

DB2 uses *locks* as a means of preventing uncommitted changes made by one application process from being perceived by another application process and for preventing one application process from updating data that is being accessed by another process. A lock is designed to help protect the integrity of data by preventing concurrent users from accessing inconsistent data. Several factors affect the uses of locks and their effect on application performance. Run the following commands to configure the database registry:

```
db2set DB2_SKIPINSERTED=ON
db2set DB2_SKIPDELETED=ON
db2set DB2_EVALUNCOMMITTED=YES_DEFERISCANFETCH
```

For more information about database locks, refer to your DB2 documentation.

User passwords stored in the installation log

Passwords are stored in plain text in the main installation log file. During installation, the log file is:

installer_dir/workspace/.metadata/.log

where *installer_dir* is the directory where the installer is located.

When the installer exits, the log file is stored in:

var/tmp/tclog_TI_*timestamp*/ti_install_*timestamp*.log

where *timestamp* is the creation date and time.

For your protection, perform one of the following steps to ensure that the passwords are not accessible in the log.

- Remove the user passwords from the log file.
- Remove the log file.
- Change the user passwords. For information about changing passwords, see "Changing default passwords" on page 137.

Installation Step 8: Verify your installation

See Chapter 4, "Verifying installation," on page 53 for steps to verify your installation.

Step 8: Perform recommended configuration

For a full production installation, some additional configuration tasks are recommended. For details, see Chapter 5, "Post-installation configuration," on page 63.

Chapter 4. Verifying installation

After you have completed installation and performed the post-installation configuration, verify your installation by performing the following steps:

1. Verify that you can start Tivoli Provisioning Manager, log on to the Web interface, and stop Tivoli Provisioning Manager.
2. Configure the Web browser to use the Tivoli Provisioning Manager certificate
3. Verify that core components are installed correctly.
4. Verify SSL configuration.

When you have verified the installation, you can start configuring Tivoli Provisioning Manager for your environment. See Chapter 5, "Post-installation configuration," on page 63.

Starting and stopping Tivoli Provisioning Manager

Starting the Tivoli Provisioning Manager server starts the process of launching the product.

Starting Tivoli Provisioning Manager

Before you start Tivoli Provisioning Manager, provisioning server, verify the following requirements:

- WebSphere Application Server is stopped. It will be started when you start Tivoli Provisioning Manager.
- If you configured a read-only directory server, ensure that it is started. For information about starting Tivoli Directory Server, see "Tivoli Directory Server tasks" on page 143.
- Ensure that the database is started. For information about starting DB2, see "Starting DB2" on page 139.
- You are logged on to the Tivoli Provisioning Manager computer as **tioadmin**.

Starting the provisioning server

To start the provisioning server:

1. Log on to the computer with the user name `tioadmin`.
2. Switch to the *$TIO_HOME*`/tools` directory.
3. Run the command: `./tio.sh start`. The startup script starts.
4. For information about logging on to the Web interface, see "Logging on to Tivoli Provisioning Manager" on page 55

Note: If the provisioning server does not start, check the log files for errors:

* *$TIO_LOGS*/tio_start.log
* *$TIO_LOGS*/deploymentengine/deploymentengine_start.log
* *$TIO_LOGS*/policyengine/policyengine_start.log
* *$TIO_LOGS*/agentshellserver/agentshellserver_start.log

Configuring the Web browser

After Tivoli Provisioning Manager is installed with the installer, it can only be accessed through the SSL port 9045, using HTTPS protocol. The default certificate

provided by Tivoli Provisioning Manager is generated during the installation and has its own certificate authority (CA), `TivoliAgentManagerCA`. This certificate will not be trusted by your existing Web browser so you must import it for SSL communication to work properly.

Importing the certificate to Internet Explorer 7.0: To trust the default Tivoli Provisioning Manager certificate in Internet Explorer, complete the following steps:

1. Ensure that Tivoli Provisioning Manager is started.
2. Open the Tivoli Provisioning Manager logon page. For example, `https://`*`fully_qualified_domain_name`*`:9045/tcWebUI`. An error is returned stating that the security certificate was not issued by a trusted certificate authority.
3. Click **Continue to this Web site (not recommended)** to be directed to the Tivoli Provisioning Manager logon page.
4. On the security bar, click **Certificate Error**. Click **View certificates** on the Certificate Invalid window.
5. On the message that the certificate cannot be verified, click **Install Certificate** to launch the Certificate Import Wizard. Click **Next** on the Welcome page.
6. On the Certificate Store panel, select **Automatically select the certificate store based on the type of certificate**. Click **Next** and then **Finish** to import the certificate.
7. From the Certificate page, navigate to **Certificate Path** > **TivoliAgentManagerCA** > **View Certificate**. Click **Install Certificate** to install the root certificate authority.
8. A security warning alerts you that you are installing a certificate from a CA representing `TivoliAgentManagerCA`. Click **Yes** to continue the installation.
9. When the installation completes, restart the Web browser and return to the Tivoli Provisioning Manager logon page. This time, the Tivoli Provisioning Manager logon page is displayed without an error message.

Internet Explorer is now configured with the Tivoli Provisioning Manager certificate. To view the certificate:

1. Navigate to **Edit** > **Preferences** > **Privacy & Security** > **Certificates**.
2. Click **Manage Certificates** and then click **Web Sites**.

The certificate issued by `TivoliAgentManagerCA` is listed under `Intermediate Certificate Authorities`.

If you receive an error message that the security certificate was issued for a different Web site address, the certificate that you imported does not contain the fully-qualified domain name. To verify:

1. Select **Continue to this Web site (not recommended)**.
2. On the security bar, click **Certificate Error**. Click **View certificates** > **Details** > **Subject**. Ensure that the fully-qualified domain name is specified.

If the fully-qualified domain name is not specified, use one of the following methods to correct the problem:

- Import the correct certificate containing the fully-qualified domain name.
- This problem could have been caused when the Tivoli Provisioning Manager installer installed the agent manager. The installer specified the IP address of the agent manager so, the certificate generated by agent manager does not include the fully-qualified domain name of the Tivoli Provisioning Manager computer. To correct this, reinstall Tivoli Provisioning Manager and ensure that the host

name is selected. Alternatively, you can purchase a certificate from a well-known certificate authority (CA) or create a self-signed certificate to enable SSL communication.

Importing the certificate to Firefox 2.0: There are two methods that you can use to import the Tivoli Provisioning Manager certificate for Firefox 2.0:

Accepting the intermediate certificate authority: If you accept the intermediate certificate authority, Firefox will trust this one certificate. You will need to trust each certificate used. To trust the default Tivoli Provisioning Manager certificate, `TivoliAgentManagerCA`, perform the following steps:

1. Ensure that Tivoli Provisioning Manager is started
2. Access the Tivoli Provisioning Manager logon page. For example, `https://`*`fully_qualified_domain_name`*`:9045/tcWebUI`. An error is returned stating that the Web site is certified by an unknown authority.
3. Select **Accept this certificate permanently**. This is the only time you must accept the certificate until the certificate expires.

Note: You can select **Accept this certificate temporarily for this session** but you will be prompted to accept the certificate each time that you access Tivoli Provisioning Manager

The certificate is accepted. To view the certificate, navigate to **Tools** > **Options** > **Advanced** > **View Certificates** > **Web Sites**. The Tivoli Provisioning Manager certificate, `TivoliAgentManagerCA`, is listed.

Accepting the root certificate authority: If you install and accept the root certificate, any certificate used by the certificate authority is trusted. To trust the default Tivoli Provisioning Manager root certificate, `TivoliAgentManagerCA`, in Firefox, follow these steps:

1. Export the root certificate to a file. The file can be in the form of `Base-64 encoded X.509`, a standard format for public certificate keys.
2. Launch the Firefox. Navigate to **Tools** > **Options** > **Advanced** > **View Certificates** > **Authorities** and click **Import**.
3. Select your exported root certificate and click **Open**.
4. On the Downloading Certificate window, select **Trust this CA to identify websites** and click **OK**.
5. The Tivoli Provisioning Manager root certificate, `TivoliAgentManagerCA` will be listed in the Authorities window.
6. Restart Firefox and return to the Tivoli Provisioning Manager logon page.

The root certificate authority is accepted so you will no longer see an error message.

Logging on to Tivoli Provisioning Manager

Log on to the Web interface to start using Tivoli Provisioning Manager.

Requirements: Before you log on to the system, verify the following requirements:

- The Tivoli Provisioning Manager server is running.
- The computer you are using to access the Web interface must be on the same network as the provisioning server.
- You are using a supported Web browser:

  - Microsoft® Internet Explorer 7.0. You must use a full installation of Internet Explorer with Internet Tools with the latest critical security updates from Microsoft.
  - Firefox 2.0 or later.
  - For some Web interface features, such as setting a home page, cookies must be enabled.
- You have the fully qualified domain name (for example, `hostname.domain.com`) and port number for the provisioning server. The default port number is `9045` for an SSL encrypted connection.

Logging on: To log on to the Web interface:

1. Launch the Web browser and enter the appropriate URL. The URL is case sensitive.

   `https://`*`hostname`*`:`*`ssl_port`*`/tcWebUI`

   where *`hostname`* is the fully-qualified domain name of the provisioning server, *`ssl_port`* is the port number for an SSL encrypted connection. The default is `9045`.
2. In the Log On window, type your user name and password, and then click **Log On**. The default user name is `admin`. Use the Tivoli Provisioning Manager administrator user name and password that you specified during installation during installation as described in "Tivoli Provisioning Manager settings" on page 37.

Notes:

1. To log off from the system, click **Log off**. To stop Tivoli Provisioning Manager, see the section, "Stopping Tivoli Provisioning Manager" on page 56.
2. Bookmark the URL for the Web interface so that you do not need to type the URL in the future.

Diagnosing log on errors: Verify the following:

- Your system meets the requirements described in "Requirements" on page 55.
- Your user name and password are correct.
- If you are using Internet Explorer, check the security settings in the browser.
  1. Click **Tools** > **Internet Options**.
  2. Click the **Security** tab.
  3. If you are using customized settings for any of the Web content zones, click **Default Level** to use the default security level and then try to log on again.

  You can also try logging on with Firefox to verify if the log on issue is specific to Internet Explorer.

Stopping Tivoli Provisioning Manager

If you need to make configuration changes to the computer where Tivoli Provisioning Manager is installed, or if you change a default administrator password, you must stop Tivoli Provisioning Manager.

You can stop the application using a script.

Note: Use only one method to start and stop the provisioning server. For example if you start the provisioning server from the desktop, use the same method to stop the provisioning server.

Stopping the provisioning server

To stop the provisioning server:

1. Switch to the *$TIO_HOME*/tools directory.
2. Run the command ./tio.sh stop.
3. At the WebSphere Application Server user name prompt, type the WebSphere Application Server administrator user name and press **Enter**. After a new installation of Tivoli Provisioning Manager, the user name is tioadmin.
4. At the WebSphere Application Server password prompt, type the WebSphere Application Server administrator password and press **Enter**. The provisioning server is stopped.
5. Some WebSphere client Java processes might still be running. Ensure that the processes are stopped.
   a. Run the following command:
      ```
      ps -ef | grep java
      ```
   b. If processes are still running, stop them with the command:
      ```
      pkill -9 java
      ```

Note: If the provisioning server does not stop, check the log file *$TIO_LOGS*/tio_stop.log for errors.

Verifying core components

To verify installation of Tivoli Provisioning Manager and core components, perform the following steps:

1. Start Tivoli Provisioning Manager as described in "Starting Tivoli Provisioning Manager" on page 53.
2. Log on to the Web interface. To verify that Web Replay is installed, click **Web Replay** at the top of the page. The Web Replay pane appears at the bottom of the page.
3. Verify the device manager federator installation:
   a. In a supported Web browser, type the following URL:
      ```
      https://hostname:9045/dmserver/TraceServlet?trace=set
      ```
      If you see the word SUCCESS!, the device manager federator is successfully installed.
   b. Check the log file *$TIO_HOME*/tioprofile/logs/server1/DMSMsg1.log for any additional information.
4. Verify that you can log on to the dynamic content delivery management center management center:
   a. In a supported Web browser, type the following URL:
      ```
      https://hostname:9045/admin
      ```
   b. Log on with the Tivoli Provisioning Manager administrator user name and password that you specified during installation as described in "Tivoli Provisioning Manager settings" on page 37. The default user name is admin.

   If you can log in successfully, the dynamic content delivery management center management center was installed successfully.

   If the message The specified username or password is incorrect is displayed when you try to log on to the dynamic content delivery management center console and SOAP services do not start successfully, see "SOAP services fail to start" on page 94 for information about fixing the error.
5. Verify the agent manager installation:

a. Access the Web interface at the following URL:
   `https://hostname:9045/tcWebUI`
b. Log on with the Tivoli Provisioning Manager administrator user name and password that you specified during installation in step "Tivoli Provisioning Manager settings" on page 37. The default is `admin`.
c. In the navigation tree, type `TCA_PingAgentManager` in the **Find** field.
d. Click the TCA_PingAgentManager workflow link that is displayed in the search results. The workflow is displayed.
e. Click **Run** > **Run**.
f. Click **Run** in the Input Parameter for Workflow window. The workflow runs and the status is displayed.
g. On the right side of the Workflow Deployment Requests page, click **Refresh** to monitor the status of the workflow execution. If the status is `success`, the agent manager is installed properly.

Verifying SSL configuration

During installation, the Tivoli Provisioning Manager installer enables secure SSL communication for the Web applications hosted by WebSphere Application Server. You must use Tivoli Provisioning Manager with SSL enabled. The following configurations need to be verified:

- New HTTP transports are created for use by the SSL ports.
- Two virtual hosts are created.
- The Tivoli Provisioning Manager Web module is mapped to one of the two virtual hosts.
- SSL configuration repertoires are configured
- SSL ports are mapped to Web container transport chains

To verify the configurations:

1. Start Tivoli Provisioning Manager if it is not started. See "Starting Tivoli Provisioning Manager" on page 53 for instructions.
2. Access the WebSphere Application Server administrative console at the following Web address:
   `http://hostname:port/admin`

   where *hostname* is thefully-qualified domain name of theTivoli Provisioning Manager computer and *port* is the WebSphere Application Server **Admin host secure port** that you defined during installation. The default port number is 9044. For example:
   `https://tpmserver.example.com:9044/admin`
3. Log on as `tioadmin`.
4. Check the virtual hosts
   a. Click **Environment** > **Virtual Hosts**.
   b. Verify that two virtual hosts are created: AgentManagerHost and TPMVirtualHost
   c. Select **AgentManagerHost** > **Host Aliases**.

d. Verify that the following information is displayed for the virtual host:

Table 18. Host alias details

Host Name	Port
*	9511
*	9512
*	9513

e. Return to the Virtual Hosts page, and then select **TPMVirtualHost** > **Host Aliases**.

f. Verify that the following information is displayed for the virtual host:

Table 19. Host alias details

Host Name	Port
*	9045
*	9046
127.0.0.1	9082

5. Check the virtual host mapping to Web modules:
   a. **Applications** > **Enterprise Applications**.
   b. For each application listed in the following table, perform the following actions:
      1) Click on the application name.
      2) Click **Map virtual hosts for Web modules**.
      3) Verify that the Web module for the application is mapped to the correct virtual host.

Table 20. Application mapping

Application Name	Web Module	Virtual host
AgentManager	AgentManager	AgentManageHost
AgentRecoveryService	AgentRecovery	AgentManagerHost
AlphabloxPlatform	IBM DB2 Alphablox Administration Application	TPMVirtualHost
AlphabloxPlatform	IBM DB2 Alphablox	TPMVirtualHost
CDS	DownloadGrid	TPMVirtualHost
CDS	DownloadGridDistribution	TPMVirtualHost
CDS	DownloadGridMonitoring	TPMVirtualHost
CDS	admin	TPMVirtualHost
DMS WebApp	Device Manager Server	TPMVirtualHost
TCEAR	tcWebUI	TPMVirtualHost
TCEAR	WebReplay	TPMVirtualHost
TCEAR	DiscoveryUpload	TPMVirtualHost
TCEAR	SPEWebApplication	TPMVirtualHost
TCEAR	SPEWebStart	TPMVirtualHost

6. Check the SSL configuration repertoires.
   a. Click **Security > SSL**.

b. Select **TPMClientAuthSSL** and verify the following settings:

Table 21. Settings for TPMClientAuthSSL

Setting	Value
Alias	TPMClientAuthSSL
Client authentication	check box is selected
Security level	High
Cipher suites	none selected
Cryptographic token	check box is cleared
Provider	Predefined JSSE Provider, IBMJSSE selected
Protocol	SSLv3
Key file	Ensure that the key file name and password are specified and the format is JKS.
Trust file	Ensure that the trust file name and password are specified, and the format is JKS.

c. From the SSL page, select **TPMServerAuthSSL** and verify the following settings:

Table 22. Settings for TPMServerAuthSSL

Setting	Value
Alias	TPMServerAuthSSL
Client authentication	check box is cleared
Security level	High
Cipher suites	none selected
Cryptographic token	check box is cleared
Provider	Predefined JSSE Provider, IBMJSSE selected
Protocol	SSLv3
Key file	Ensure that the key file name and password are specified and the format is JKS.
Trust file	Ensure that the trust file name and password are specified, and the format is JKS.

7. Verify the mapping of SSL ports to Web container transport chains.
   a. Navigate to the following page: **Servers > Application Servers > server1 > Web Container Settings > Web container transport chains**.
   b. Verify that the following entries:

Table 23. HTTP transport chains

Name	Enabled	Host	Port	SSL Enabled
AgentManagerCientSSL_Chain	Enabled	*	9512	Enabled
AgentManagerSSL_Chain	Enabled	*	9511	Enabled
AgentManager_Chain	Enabled	*	9513	Disabled
TPMClientAuthSSL_Chain	Enabled	*	9046	Enabled
TPMServerAuthSSL_Chain	Enabled	*	9045	Enabled
WCInboundAdmin	Enabled	*	9061	Disabled

Table 23. HTTP transport chains (continued)

Name	Enabled	Host	Port	SSL Enabled
WCInboundAdminSecure	Enabled	*	9044	Enabled
WCInboundDefault	Enabled	*	9080	Disabled
WCInboundDefaultSecure	Enabled	*	9443	Enabled

Chapter 5. Post-installation configuration

After you have verified your installation, you can start setting up the product for your environment. This chapter describes recommended configuration to perform for a production installation. For a default installation, a performing a backup is recommended, but none of the tasks in this chapter are required.

Important: Ensure that you have completed required configuration described in "Installation Step 7: Perform required configuration" on page 49. The configuration described in that section is required for proper operation of Tivoli Provisioning Manager. The configuration described in this chapter is recommended for production installations, but is not required to use the product.

Backing up the database

You should back up your product after it is installed and perform periodic backups based on the backup policies in your organization. Keeping backups of a functional installation ensures that you can recover the product in a working state if required. For backup and restore instructions, see Appendix H, "Backing up the database," on page 147.

Configuring a read-only directory server

The default Tivoli Provisioning Manager installation sets up authentication based on user accounts in the operating system. This type of configuration is for evaluation or demonstration purposes.

Tivoli Provisioning Manager supports a read-only *Lightweight Directory Access Protocol* (LDAP) implementation for user authentication. LDAP is a user registry in which authentication is performed using an LDAP binding. You manage users centrally on the LDAP server and assign user access based on your specific needs. Tivoli Provisioning Manager uses the information in the user registry to authenticate users, but it cannot modify the user registry.

Choosing an authentication method

To determine the type of authentication to use, review the comparison in 63.

Important: Migration of users from operating system authentication to LDAP authentication is not supported. If you want to use a directory server with Tivoli Provisioning Manager, the user accounts must be created on the LDAP server. Before you start using the product, you should decide on the authentication method that you want to use.

Table 24. Comparison of authentication methods

Capability	Operating system	LDAP
Adding users	Users accounts are created in the operating system. You can then add a user to Tivoli Provisioning Manager by specifying the user name for the user account.	Users accounts are created on the LDAP server. You can then add a user to Tivoli Provisioning Manager by specifying the user ID associated with the user account.

Table 24. Comparison of authentication methods (continued)

Capability	Operating system	LDAP
Remove users	You can remove a user from Tivoli Provisioning Manager from the Web interface. The actual user account must be removed from the operating system separately.	You can remove a user from Tivoli Provisioning Manager from the Web interface. The actual user account must be removed from the LDAP server separately.
User information	You can add some basic user profile information such as the email address and phone number.	You cannot edit information in the user profile. If you are storing similar information for users on your LDAP server, you must manually configure the mapping of user account attributes to the appropriate fields in a Tivoli Provisioning Manager user profile.
Data protection	No built-in backup and recovery capability is provided. You must perform your own backups of the operating system to preserve user accounts and backups of the Tivoli Provisioning Manager database to preserve user profile data.	The Tivoli Directory Server database can be configured for high availability disaster recovery.

If you decide to use operating system authentication, no additional authentication configuration is required. Information about adding and managing users is included in the Tivoli Provisioning Manager information center. You can access the information center when you log on to the product.

If you want to configure a read-only directory server, follow the instructions in this section.

Directory server requirements

Before configuring Tivoli Provisioning Manager for supporting read-only LDAP, verify the following requirements:

- Tivoli Directory Server Version 6.1 must be preinstalled on a separate computer. Refer to the Tivoli Directory Server documentation for installation instructions. See “Installing and configuring Tivoli Directory Server” on page 121 for general instructions. Integration with Microsoft Active Directory is only supported on if the provisioning server is installed on Windows.
- Identify the *custom user registry* that specifies how to access information in your directory server. A *user registry* authenticates a user and retrieves information about users and groups to perform security-related functions, including authentication and authorization. A *custom user registry* is a customer-implemented user registry. It can support virtually any type of an account repository and provides considerable flexibility in adapting product security to various environments.

  Tivoli Provisioning Manager provides a sample custom user registry for accessing the general LDAP:

  Tivoli Directory Server:

  com.ibm.tivoli.websphere.customSecurity.sample.IDSCurImplementation

  If the sample does not suit your system requirements, you can implement your own custom user registry. To create your own, see the WebSphere Application Server documentation on custom user registries for more information .
- Identify the LDAP users required for Tivoli Provisioning Manager and ensure that they are defined on the LDAP server.

  WebSphere Application Server administrator
  This user is for accessing the WebSphere Application Server

administrative console. After Tivoli Provisioning Manager installation, the WebSphere Application Server administrator is the `tioadmin` operating system user. The WebSphere Application Server administrator user name in the custom user registry samples is `wasadmin`.

LDAP administrator
For Tivoli Directory Server, this user is the entry owner of the Tivoli Provisioning Manager LDAP suffix. For example `tioldap`.

Tivoli Provisioning Manager administrator
This user is the default administrator that is used to log on to the Tivoli Provisioning Manager Web interface and will be assigned all access privileges in Tivoli Provisioning Manager. For example `webadmin`.

- If you plan to use existing Tivoli Directory Server user accounts with Tivoli Provisioning Manager, user IDs cannot contain double-byte characters.

Configuring Tivoli Provisioning Manager to use the LDAP server

The read-only LDAP script helps you to configure Tivoli Provisioning Manager for authentication with a read-only LDAP.

In some situations, manual configuration of the directory server is required instead of using the read-only LDAP script. If you need to perform the configuration manually, see Appendix F, "Manually configuring read-only LDAP," on page 127.

Note: The script only supports configuration of Tivoli Directory Server. Configuration of Microsoft Active Directory is only supported on if Tivoli Provisioning Manager is installed on Windows.

1. Ensure that the directory server is running.

   To verify the status of Tivoli Directory Server:
   a. Log on to the Tivoli Directory Server computer. If you installed the Tivoli Directory Server client on the Tivoli Provisioning Manager server, you can check the status of Tivoli Directory Server from the Tivoli Provisioning Manager computer instead.
   b. Run the following command:

      ```
      ibmdirctl –D cn=root –w password -h hostname status
      ```

      password
      The password for the base DN (cn=root)

      hostname
      The host name of the Tivoli Directory Server computer. The `-h hostname` part of the command is only required if you are connecting from the Tivoli Provisioning Manager computer.

2. Log on as `tioadmin`.
3. Tivoli Provisioning Manager uses the security name to find groups for users on the directory server. The default security name for Tivoli Directory Server is `cn`. If you want to use a different attribute for Tivoli Directory Server, you must edit the script for configuring Tivoli Provisioning Manager.
   a. Change to the *$TIO_HOME*`/tools/postinstall` directory.
   b. Open the file `readonly-ldap-config.sh` in a text editor.
   c. Find the following line and replace `cn` with the attribute that you want to use for the security name.

      ```
      SECURITYNAME=cn
      ```

   d. Save your changes.

4. Change to the *$TIO_HOME*/tools/postinstall directory.
5. Run the following command to configure Tivoli Provisioning Manager. Ensure that the command and parameters are all entered on a single line.

   Run the following command:

```
readonly-ldap-config.sh ldap_type old_was_user old_was_user_pwd new_was_user
 new_was_user_pwd ldap_fqdn dmport "base_DN" ldap_user ldap_user_pwd "search_filter"
 tpm_admin tpm_admin_pwd search_input
```

ldap_type
The type of LDAP server.

old_was_user
The current WebSphere Application Server administrator user name defined in the operating system. When Tivoli Provisioning Manager is installed, the user name is tioadmin.

old_was_user_pwd
The password for the current WebSphere Application Server administrator user.

new_was_user
The new WebSphere Application Server administrator user name that you defined on the LDAP server.

new_was_user_pwd
The password for the new WebSphere Application Server administrator user.

ldap_fqdn
The fully-qualified domain name of the LDAP server. For example ldap.example.com.

port The port for connections with the LDAP server. The default LDAP port is 389.

base_DN
The base distinguished name (DN) for your directory server, enclosed in quotation marks. Typically, the DN matches the domain name of the directory server computer. For example, if the domain name of the computer is ldap.example.com, then the base DN is dc=example,dc=com for Tivoli Directory Server.

ldap_user
The user you defined on the LDAP server for connections with the LDAP server. For example, tioldap.

ldap_user_pwd
The password for the LDAP user.

search_filter
The LDAP search filter for retrieving user records on the LDAP server, enclosed in quotation marks.

tpm_admin
The Tivoli Provisioning Manager administrator defined on the LDAP server. For example, webadmin.

tpm_admin_pwd
The password for the Tivoli Provisioning Manager administrator.

search_input

Specify a value to use for validation of the search filter you specified for the *search_filter* parameter. The variable %v in your search filter is be replaced by this value.

For example, if your user search filter is "(&(cn=%v)(objectclass=organizationalPerson))" and your search_input value is "tio*", then the search filter becomes "(&(cn=tio*)(objectclass=organizationalPerson))".

Important: Ensure that you select a value that returns at least one user when it is used in the search filter.

Example for Tivoli Directory Server:

```
./readonly-ldap-config.sh ibmds tioadmin tiopas5wd wasadmin waspa5wd myserver.example.com
 389 "dc=example,dc=com" tioldap tioldap "(&(cn=%v)(objectclass=organizationalPerson))"
 webadmin pas5word "tio*"
```

6. If you are using a different security name as explained in step 3 on page 65, you must update user-factory.xml.
   a. Stop Tivoli Provisioning Manager if it is running.
   b. Change to the *$TIO_HOME*/config directory and open the file user-factory.xml in a text editor.
   c. Find the line <userSecurityName>.

      Tivoli Directory Server:

      ```
      <userSecurityName>cn</userSecurityName>
      ```

      Replace cn with the attribute that you want to use for the security name.
7. Encrypt the WebSphere Application Server administrator password:
   a. In a Web browser, open the DB2 Alphablox console:

      ```
      https://hostname:9045/AlphabloxAdmin/home/
      ```

      where *hostname* is the host name of the computer where WebSphere Application Server is installed.
   b. Log on with the new WebSphere Application Server administrator password.
   c. In the console, click **Administration** > **General** > **System**.
   d. Change **Message History Size** from 100 to 101 and save the change. Alphablox automatically encrypts the password in the Server.properties file.
8. Verify that you can log on to the Web interface. For log on instructions, see "Logging on to Tivoli Provisioning Manager" on page 55.
9. Verify the dynamic content delivery management center management center installation:
   a. In a supported Web browser, type the following URL:

      ```
      https://hostname:9045/admin
      ```
   b. Log on with your new Tivoli Provisioning Manager administrator user name and password.

      If you are unable to log on with the new user name and password, try to log on with the old user name and password. If the old user name is working, you must restart the SOAP process for the new user name and password to take effect.

      1) Find the ID for the SOAP process in the file *$TIO_LOGS*/soap/desoap.pid.

2) Kill the SOAP process with the command
   `kill -9 pid`

   Replace *pid* with the ID of the SOAP process.
3) Restart the Tivoli Provisioning Manager server so that the new user name and password take effect. For instructions, see "Starting and stopping Tivoli Provisioning Manager" on page 53.

Tivoli Provisioning Manager is now configured support a read-only LDAP server. See "Importing LDAP users" for information about importing your existing users.

Importing LDAP users

To import the existing user information from your LDAP server to Tivoli Provisioning Manager, complete the following:

1. Create an XML file with the following information, where `testUser1` and `testUser2` are users from your own LDAP:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE datacenter PUBLIC "-//Think Dynamics//DTD XML Import//EN"
    "http://www.thinkdynamics.com/dtd/xmlimport.dtd" [
<!ENTITY resourcepoolconfig SYSTEM "http://www.thinkdynamics.com/dtd/resourcepool.xml">
<!ENTITY dataacquisitionconfig SYSTEM "http://www.thinkdynamics.com/dtd/dataacquisition.xml">
<!ENTITY simulator-cpu '
    <dae-driver device="server" classname="com.thinkdynamics.kanaha.dataacquisitionengine.NullDriver"/>
    <dae-signal name="cpu-utilization"
        device="server" metric="cpu-utilization" aggregation="average"
        filter="low-pass-filter"/>
  '>
]>
<datacenter>
   <user name="<testUser1>" superuser="false" default-access-domain="sample:all-objects">
   <domain-role-assignment domain="sample:all-objects" role="sample:all-permissions"/>
   <tpm-roles>
      <tpm-role>SystemAdministrator</tpm-role>
   </tpm-roles>
   </user>

   <user name="<testUser2>" superuser="false" default-access-domain="sample:all-objects">
   <domain-role-assignment domain="sample:all-objects" role="sample:all-permissions"/>
   <tpm-roles>
      <tpm-role>SoftwareOperator</tpm-role>
   </tpm-roles>
   </user>
</datacenter>
```

2. Import the file into Tivoli Provisioning Manager by running the following command:
   `"$TIO_HOME/tools/xmlimport.sh" "file:file_location"`

The LDAP users are now imported and new user accounts have been created in Tivoli Provisioning Manager. The users will now have access to the applicable features and functions of Tivoli Provisioning Manager.

Optional configuration for a directory server

After you have set up the directory server, you can perform some optional tasks to customize the directory server integration with Tivoli Provisioning Manager.

Group membership: The read-only directory server support is limited to user retrieval only and group information is ignored. You can optionally map your existing groups on the directory server to Tivoli Provisioning Manager user groups.

Group memberships are retrieved differently depending on the LDAP implementation. Tivoli Provisioning Manager provides custom user registry implementation samples. The attribute that is used to retrieve the membership information:

- **ibm-allGroups**: This attribute shows all groups to which an entry belongs. This read-only operational attribute is not allowed in a search filter. This is specified as the value of groupMember attribute in the user-factory-ids-readOnlyLdap.xml file.
- **ibm-allMembers**: This attribute shows all members including groups and users of a group. This read-only operational attribute is not allowed is a search filter. This is specified as the value of user members attribute in the user-factory-ids-readOnlyLdap.xml.

Tivoli Provisioning Manager provides a tool to map these groups. The tool reads an XML file which defines the relationships between the external groups and then Tivoli Provisioning Manager groups and imports it into the data model tables.

The externalRoleMapping.xml file contains the mapping relationships. This is a many-to-many relationship. An external role mapping definition consists of four elements:

name The name of the external role. Tivoli Provisioning Manager returns the set of groups defined in the tpmRoles element when the user belongs to this external group. The method, getGroupsForUser, implemented in the custom user registry, should return the external roles that a user belongs to.

description
The description of the external role.

unique_id
The unique identifier of the external role. This is probably a domain name for an LDAP group entry. This is not currently used in Tivoli Provisioning Manager but is handled to contain this information for later release migration for identify assertion.

tpmRoles
This element contains a set of Tivoli Provisioning Manager groups. These groups must be the permission level groups. They are default groups for Tivoli Provisioning Manager. The groups are not customizable so, users cannot create, update, or remove the groups from Tivoli Provisioning Manager.

In the sample below, there are two external roles being mapped to Tivoli Provisioning Manager by defining the set of Tivoli Provisioning Manager groups that a user should belong to when they log in to Tivoli Provisioning Manager:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE RoleMappings>
<RoleMappings>
<externalRole>
  <name>ExternalRole1</name>
   <description>External Role 1</description>
 <unique_id>ExternalRole1_ID</unique_id>

 <tpmRoles>
  <tpmRole_id>PatchEdit</tpmRole_id>
  <tpmRole_id>uiLogin</tpmRole_id>
  <tpmRole_id>PatchManage</tpmRole_id>
  <tpmRole_id>PatchView</tpmRole_id>
```

```
  <tpmRole_id>ReportGlobalEdit</tpmRole_id>
  <tpmRole_id>ReportGlobalEditSQL</tpmRole_id>
  <tpmRole_id>ReportAuditView</tpmRole_id>
  <tpmRole_id>ReportComplianceView</tpmRole_id>
  <tpmRole_id>ReportCustomView</tpmRole_id>
  <tpmRole_id>ReportDeploymentView</tpmRole_id>
  <tpmRole_id>ReportDiscoveryView</tpmRole_id>
  <tpmRole_id>ReportInventoryView</tpmRole_id>
  <tpmRole_id>ResourceAdminView</tpmRole_id>
  <tpmRole_id>ServiceCatalogManage</tpmRole_id>
  <tpmRole_id>ServiceCatalogEdit</tpmRole_id>
  <tpmRole_id>ServiceCatalogView</tpmRole_id>
  <tpmRole_id>SoftwareEdit</tpmRole_id>
 </tpmRoles>
</externalRole>
<externalRole>
   <name>ExternalRole2</name>
   <description>External Role2 </description>
   <unique_id>ExternalRole2_ID </unique_id>
   <tpmRoles>
   <tpmRole_id>ApplicationsAdminEdit</tpmRole_id>
   <tpmRole_id>ApplicationsAdminView</tpmRole_id>
   <tpmRole_id>CommonAgentManage</tpmRole_id>
   <tpmRole_id>ComplianceEdit</tpmRole_id>
   <tpmRole_id>ComplianceView</tpmRole_id>
   <tpmRole_id>uiLogin</tpmRole_id>
   <tpmRole_id>ComputerEdit</tpmRole_id>
   <tpmRole_id>ComputerView</tpmRole_id>
   <tpmRole_id>ServerTemplateEdit</tpmRole_id>
   </tpmRoles>
 </externalRole>
</RoleMappings>
```

After the xml file is created:

Save the file to the *$TIO_HOME*/tools directory and then run the command importExternalRoleMapping.sh to import the external roles to Tivoli Provisioning Manager.

In case a mistake was made and you need to remove all of the relationship mappings, you can run the command:

```
$TIO_HOME/tools/importExternalRoleMapping.sh cleanUpOnly
```

The command will remove all of the relationship entries. To load the data again, run the importExternalRoleMapping command again. The external groups from the customer LDAP have now been mapped to the default Tivoli Provisioning Manager groups.

Defining user attributes: User information is displayed in Tivoli Provisioning Manager on the Manage Users page. The information on this page is retrieved from the directory server based on the user attributes defined in user-factory.xml file. If you want to customize the user attributes that are retrieved, search for the topic "Defining user attributes for read-only LDAP" in the information center. You can access the information center by logging on to the Web interface and clicking **Information Center**.

Authenticating with a client certificate

A self-signed client user certificate can be used to authenticate to Tivoli Provisioning Manager. Using this certificate allows the user to skip the default form based login authentication that would normally prompt them for the user ID and password since the certificate is trusted by Tivoli Provisioning Manager.

Once read-only LDAP is configured, Tivoli Provisioning Manager is defaulted to use form based authentication. If Tivoli Provisioning Manager is installed using the regular installer, it can only be accessed through the secure ports 9045 and 9046 corresponding to the server and mutual authentication ports respectively.

Configuring SSL

Tivoli Provisioning Manager uses virtual host so that it can have its own configuration, security configuration, and keystores. The Web modules contained in Tivoli Provisioning Manager are using the virtual host called TPMVirtualHost.

To configure Tivoli Provisioning Manager for client certificate based authentication, you must change the SSL repertory for the ports that TPMVirtualHost is using, ports 9045 and 9046.

1. Access the WebSphere Application Server administrative console at the following Web address:

   `http://hostname:port/admin`

   where *hostname* is thefully-qualified domain name of theTivoli Provisioning Manager computer and *port* is the WebSphere Application Server **Admin host secure port** that you defined during installation. The default port number is 9044. For example:

   `https://tpmserver.example.com:9044/admin`
2. Enter your user ID and password. Use the WebSphere Application Server user that you set up for the read-only directory server configuration. For example, `wasadmin`.
3. Click **Servers** > **Application servers** > **<server_name>** > **Web Container Settings** > **Web Container** > **HTTP transport** > **9045**.
4. Verify that on port 9045, SSL is set to use **AgentManagerSSL**.
5. Click **Servers** > **Application servers** > **<server_name>** > **Web Container Settings** > **Web Container** > **HTTP transport** > **9046**.
6. Change the SSL repertory to *node_name*`/AgentManagerClientAuthSSL`. Click **Apply**.
7. After the SSL repertory for ports 9045 and 9046 have been identified, verify that the keystore and truststore files are correct for the SSL repertory. Navigate to **SecuritySSL** and then select the *node_name*/**AgentManagerSSL** repertory.
8. The keystore for the Key file should be **agentManagerKeys.jks**. The key file is located inside the `AgentManager/certs` directory. The Trust file should be **agentManagerTrust.jks** and is also located inside the `AgentManager/certs` directory.

Recommended configuration for better performance

Setting the maximum heap size

This configuration change is recommended in order to take advantage of the 64–bit WebSphere Application Server architecture.

1. Log on to the WebSphere Application Server administration console at:

   `https://hostname:port/ibm/console/logon.jsp`

   where *hostname* is the WebSphere Application Server host name and *port* is the secure host port. The default port number is 9044.
2. To change the maximum heap size:

a. Click **Servers** > **Application servers** > *server_name* > **Process Definition** > **Java Virtual Machine**.
b. Change the maximum heap size setting to 2048 MB.

Setting the db-truncation value

This configuration change reduces the size of the result sets returned to the Tivoli Provisioning Manager user. Making this change is beneficial because it generally reduces database workload. However, some users prefer the larger result set size, so the setting can be changed at the discretion of the user based on the Tivoli Provisioning Manager behavior that they prefer.

1. In the Tivoli Provisioning Manager Web user interface, click **Global Settings** > **Variables**.
2. Change the *db-truncation* variable properties from 250 to 60 and save your changes.

Setting the MAXAPPS and MAXCONNECTION parameters

This configuration change is recommended when a large number of concurrent administrators, for example, more than 50 administrators, are using the Tivoli Provisioning Manager user interface. These settings may be more accurately tuned by monitoring the workload of the DB2 instance.

1. Run the command `db2 get db manager configuration` to find the value of `MAX_CONNECTIONS` and `MAXAPPLS`.
2. To increase the value of `MAX_CONNECTIONS`, run the command `db2 update dbm cfg using MAX_CONNECTIONS <value>`. Change the *<value>* to your preferred value, for example, 550.
3. To increase the value of `MAXAPPLS`, run the command `db2 update db cfg for <database name> using MAXAPPLS <value>`. Change the *<value>* to your preferred value, for example, 550.

Setting Ulimit value

This configuration change is generally required when a large number of concurrent administrators, for example, more than 50 administrators, are using the Tivoli Provisioning Manager user interface. Managing `ulimit` is a system administrator activity. The sample method below is one possible way to change this setting.

1. Stop the Tivoli Provisioning Manager server.
2. In a command window, run `ulimit -a` to check the limits. If everything is set to `unlimited`, no further change is required.
3. If the `ulimit` for *open files* is not set to unlimited, complete the following changes:
   a. Open the file,`/etc/security/limit.config`.
   b. Add the line, `* - nofile <value>` at the end of the file, where *<value>* is the value that you want. The value `70000` has been used with success for large scale Tivoli Provisioning Manager testing.
4. Save the file and close the session.
5. Open a new session and start Tivoli Provisioning Manager.

Importing sample data

The data model in Tivoli Provisioning Manager, is a representation of all of the physical and logical that Tivoli Provisioning Manager manages. After you have installed Tivoli Provisioning Manager, you must add the hardware and software that you want to manage from the provisioning server to the data model.

If you want to take an initial look at the product in a test environment, you can import the sample data into the data model.

To import the `venice.xml` file to your data model, follow the steps below:

1. Log in as `tioadmin`.
2. Ensure the database is running.
3. Open a command window and run the following command, which will enable you to import properly formed XML file to populate the data model:

   ```
   "$TIO_HOME/tools/xmlimport.sh" "file://$TIO_HOME/xml/venice.xml"
   ```

You have now populated the data model with sample data.

Note: For more information on `xmlimport` see the information center.

Next steps

When you have completed the necessary post-installation configuration, you can start configuring the product to manage your hardware and software.

1. Log on to the Web interface and click the **Information Center** link to access the product documentation.
2. In the **Contents** pane, expand **Getting Started** > **The basics**. Help topics in this section will provide you with key information for using different features in the product.
   - The **Installation basics** topic contains information for initial setup including security configuration, email notifications, and setting up infrastructure for software distribution.
   - The **Discovery basics** topic describes how to set up discovery of hardware and software.
   - The other basics topics provide information about other features in the product.

Chapter 6. Recovering from installation errors

If you encounter an error during installation, use the information in this chapter to identify the problem and address it.

Recovery first steps

The following list identifies sources of recovery information for key steps in the installation process. Use this list as your starting point to find log files and other information to recover from installation errors.

Note: Log files are encoded in UTF-8 format. When you are viewing log files, ensure that you are using a text editor that supports this format.

For information about exit codes for a silent installation, see "Silent installation exit codes" on page 113.

1. If you performed a default installation, you can review information about the values used for the installation in Appendix A, "Values for a default installation," on page 99. You might need this information to perform some recovery actions. You can also use these values if want to try reinstalling the product using the custom installation option.
2. **Starting the installer**: Before the installation wizard starts, files required to run the installer are installed and configured. If an error occurs before the installer starts, check the following log file:

   `/var/tmp/launchTI.log`

   Check for messages to help you to fix the error and then run the installer again.
3. **Initial preinstallation check**: The installer validates some installation requirements at the beginning of the installation. If you encounter an error, log files are in the user-specified temporary directory (**Temp Location** in the installer). The default location is `/var/tmp`

   preinstall_check_lin.sum
   Contains a summary of all messages.

   preinstall_check_lin.chks
   Contains a description of each preinstallation check and the results of the check.

   For each error or warning message, find the message ID in "Requirement verification by the installer" on page 81 to learn about the error and steps to address it. For most of errors or warnings, you can click **Back** in the installer to go to the panel before the error occurred, and then click **Next** to continue with installation.
4. **Discovery**: The installer uses Common Inventory Technology software to discover software and hardware on your computer. Discovery is run twice by the installer.
   - After the **Configure the Target Server** panel.
   - After the **Specify the location of the images required for installation** panel.

   The results are then displayed on the **Validation summary** panel. If a requirement is not met, you can double-click the requirement for an explanation. If the explanation includes a message ID such as TPM-INST, find the message ID in the section "Requirement verification by the installer" on page 81

page 81 for details about addressing the error.

Table 25. Discovery logs

Type of information	Header
Installation of Common Inventory Technology	If there are installation errors, check `/tmp/cit/cit.log`
Common Inventory Technology scan log	`/tmpCITTrace.log`
The results of discovery	The files are located in: `/tmp` or `/var/tmp` Results are stored in XML files with the fully-qualified domain name in the file name. For example if the fully-qualified domain name is tpmserver.example.com, the file names include: cit_tpmserver.example.com_output.xml tpmserver.example.com_hwoutput.xml tpmserver.example.com_swoutput.xml tpmserver.example.com_vpdoutput.xml

For some discovery errors, you can click **Back** in the installer to go to the panel before the error occurred, and then click **Next** to continue with installation. For example, if there is insufficient disk space, you can make more disk space available without exiting the installer. When the discovery runs again, the available disk space will be validated again.

See "Before prerequisite software is installed" on page 90 for additional recovery steps that you can take before software installation starts.

5. **Software installation**: If an error occurs during installation of a software component, information about the error is contained the log file for that software component.
   a. To identify the component that failed, check the file `.log` file that is created by the installer. This file identifies errors that occur during installation and also contains parameter values that were used by the installer. When the installer is running, the log is in:

      installer_dir`/workspace/.metadata/.log`

      where *installer_dir* is the directory where the installer is located.

      When the installer exits, the following directory is created:

      `var/tmp/tclog_TI_`*timestamp*

      where *timestamp* is the creation date and time of the log file.

      This directory stores the following log files:

      Main installation log file

      `ti_install_`*timestamp*`.log` is the main installation log file. It is a copy of the `.log` file that is created when the installer was running.

      Log files for product configuration

      - `TCConfiguration.SUCCESSFUL.log`
      - `TCConfiguration.FAILED.log`
      - `xmlimport_dcmload.SUCCESSFUL.log`
      - `xmlimport_dcmload.FAILED.log`
      - `xmlimport.log`

b. When you have identified the component, check its log file. Check for references to other components or other log files. For example, the log file for component that failed during installation might point to a WebSphere Application Server log for more information. The WebSphere Application Server might reveal an incorrect WebSphere Application Server setting that caused the component installation to fail.

   Note: In the following table:
   - *$TIO_HOME* is the Tivoli Provisioning Manager installation directory. The default is /opt/ibm/tivoli/tpm.
   - *$WAS_HOME* is the WebSphere Application Server installation directory. The default is /opt/IBM/WebSphere/AppServer.
   - *Tivoli_common_dir* is the Tivoli common directory. The default is /var/ibm/tivoli/common.
   - *$TIO_LOGS* is the location of product runtime logs. The default is /var/ibm/tivoli/common/COP/logs/var/ibm/tivoli/common/COP/logs
   - *AM_HOME* is the agent manager installation directory. The default is /opt/IBM/AgentManager.
   - *temp_dir* is the **Temp Location** directory specified during installation. The default is `/var/tmp`.

Table 26. Log files for product components

Component	Log file
Tivoli Provisioning Manager	**Installation log** The following log file stores information about installing the Tivoli Provisioning Manager application. `/tmp/tclog/tcinstall.log` **Logs for initialization** *$TIO_LOGS*`/reinit.log` **Logs for agent manager registration** *$TIO_LOGS*`/reinit.log` **SSL configuration for agent manager** Located in .log as described in step 5.
WebSphere Application Server	**WebSphere Application Server** `/tmp/was-logs/was-ismp-install.log` **WebSphere Application Server SystemOut log** *$TIO_HOME*`/tioprofile/logs/server1/SystemOut.log` **Logs created by WebSphere Application Server** Logs are stored in the following locations: *$WAS_HOME*`/logs` *user_root*`/logs` where *user_root* is the WebSphere Application Server profile installation path. The default is *$WAS_HOME*`\profiles/`*profile_name*`/logs`

Table 26. Log files for product components (continued)

Component	Log file
DB2™	The main installation log are located is: • \db2install.log is the main installation log. • \db2wi.log contains the log of the most recent installation. Information is written to it as the installation events occur. • \db2trace.log contains installation trace information. • /tmp/db2install.log is the main installation log. • /tmp/db2icrt.log is the database instance creation log. • /var/tmp/db2setuop.his is the installation history log. • /var/tmp/db2trace.log contains installation trace information. Check for other log files that start with db2 for additional information.
agent manager	**agent manager** The main logs can point to other installation logs. *AM_HOME*/logs/AMReturnValues.log *AM_HOME*/logs/am_upgrade.log **agent manager certificate generation** wsadmin.traceout **Logs created by the Tivoli Provisioning Manager installer** This log information is located in *temp_dir*/_amlinux/ and is created even if the other agent manager logs are not created. amisxtrace.log contains installation information
dynamic content delivery management center	**dynamic content delivery management center logs** Logs are in the following location: *Tivoli_common_dir*/ctgde/logs The key log files include: • trace_manager_install.log • trace_isx_install.log • *.out • *.err Ensure that you check the *.out and *.err files, even if they are 0 kb. **Logs created by the Tivoli Provisioning Manager installer** This log information is located in *temp_dir*/_cdslinux/ and is created even if the other dynamic content delivery management center logs are not created. cdsisxtrace.log contains installation information

Table 26. Log files for product components (continued)

Component	Log file
device manager federator	The following log files are in `$TIO_HOME/DeviceManager/log`: **DMS_install.log** Contains information about the device manager federator installation. **dms_config_trace.log** Contains detailed installation information when device manager server and device manager database is configured. It also contains trace information after running the DMSconfig or DMSremoveconfig command with the `-showtrace` option. **dms_config_trace.log** Contains messages after running the DMSconfig or DMSremoveconfig command. Values used for configuration are in: `$TIO_HOME/DeviceManager/config/myDMSconfig` **Logs created by the Tivoli Provisioning Manager installer** This log information is located in *temp_dir*`/_dmslinux/` and is created even if the other device manager federator logs are not created. `dmsisxtrace.log` contains installation information
Tivoli common directory	The Tivoli common directory is a common parent directory that stores log files from multiple Tivoli products. Each product stores logging information in a separate subdirectory within the Tivoli common directory. If you are installing Tivoli Provisioning Manager for the first time as the first Tivoli software product on your system that uses the Tivoli common directory, the directory is created in the location that you specify in the installer. The default location is: `/var/IBM/tivoli/common`

c. Check for messages that might indicate a problem with the configuration of WebSphere Application Server or your database server. For example, if connection with the database server failed, verify that you can connect to the database server with the database client. If the JDBC connection failed, verify that the following information was specified correctly during installation:
   - The host name of the Tivoli Provisioning Manager computer and the database server, if the database server is on a separate computer.
   - All port numbers specified during installation are correct and are available.
   - The value of the environment variable `LD_LIBRARY_PATH` is correct.

d. Check the installation directory that you specified for the software component that failed. Ensure that there are no extra spaces before or after specified path.

e. See "During installation of software" on page 91 for other troubleshooting information for software installation.

f. If the installation fails after several components have been installed successfully, you can leave the successfully installed components so that the next installation is shorter.
   1) Click **Back** in the installer to return to the previous panel.
   2) Uninstall the failed component and any components that installed after the failure. See Appendix B, "Uninstalling and reinstalling Tivoli Provisioning Manager," on page 103 for uninstallation instructions.

3) Click **Next** to continue with installation. The installed components are detected and installation resumes with the remaining components.

6. **Exiting the installer**: When you exit the installer, temporary files for the installer are automatically removed.

   If you clicked **Cancel** to exit the installer before installation completed you should remove applications that were not successfully installed. See Appendix B, "Uninstalling and reinstalling Tivoli Provisioning Manager," on page 103 for uninstallation instructions.

   When the installer exits, the following directory is created:

   `var/tmp/tclog_TI_`*`timestamp`*

   where *timestamp* is the creation date and time of the log file.

   This directory stores the following log files:

   Main installation log file

   `ti_install_`*`timestamp`*`.log` is the main installation log file. It is a copy of the `.log` file that is created when the installer was running.

   Log files for product configuration

   - `TCConfiguration.SUCCESSFUL.log`
   - `TCConfiguration.FAILED.log`
   - `xmlimport_dcmload.SUCCESSFUL.log`
   - `xmlimport_dcmload.FAILED.log`
   - `xmlimport.log`

7. **Starting Tivoli Provisioning Manager**

   When you start Tivoli Provisioning Manager the application creates the file `tio_start.log` under the Tivoli Common Directory. The default location is:

   `/var/ibm/tivoli/common/COP/logs`

8. **Uninstallation**: When you uninstall Tivoli Provisioning Manager, the log files are located in:

   `/tmp/tclog`

If you need contact IBM Tivoli Software Support, gather the following information.

- The installation log files.
- Operating system version, including any service packs.
- The version of the application server, database server, and Java.

WebSphere Application Server

To verify the version of WebSphere Application Server, run the following command from the *$WAS_HOME*`/bin` directory.

`genVersionReport.sh`

The command generates a report called `versionReport.html`. The report identifies the installed version of WebSphere Application Server and all installed maintenance packages.

DB2

To check the version of DB2, run the command, `db2level`.

Java

To verify the Java version installed with WebSphere Application Server, change to the `$WAS_HOME/java/bin` directory and run the command `./java -version`.

The following version is displayed if Java SDK 1.4.2 SR6 is installed:

```
cxia32142ifx-20061121
```

- Hardware description.
- Installation media type (disks or electronic download) and level.
- Whether you are logged on to the computer locally. Running the installation using Remote Desktop is not supported.
- Whether you are logged on as a local administrator or a domain administrator. Cross-domain installation is not supported.

For additional troubleshooting information that is not contained in this guide, refer to the *Tivoli Provisioning Manager Problem Determination Guide*.

Requirement verification by the installer

When you start installation, the installer validates installation requirements. It assumes that you have performed all the preinstallation steps described in Chapter 2, "Preinstallation checklist for Linux on System z," on page 9. If you do not meet a requirement, an error or warning message is displayed.

- An error must be addressed to continue with installation. You must resolve all errors before you can install the product.
- A warning identifies a requirement that can impact the installation, such as insufficient available memory. After reviewing the warning, you can decide if you want to continue with installation.

Each error or warning includes an ID at the beginning of the message. To find out how to address the error or warning, see search for the appropriate message ID in this section.

Existing installation

TPM-INST:

This message appears the Tivoli Provisioning Manager application is found on the computer. This message refers to the Tivoli Provisioning Manager application itself and not the entire set of software components that make up the Tivoli Provisioning Manager installation.

The action that you must take depends on the installed version of the application that is found.

Version 5.1.1 installation

The message is an warning message.

- If a previous installation failed after the Tivoli Provisioning Manager application was successfully installed and you want to try to reinstall the agent manager, the dynamic content delivery management center, or the device manager federator, you can continue with installation.
- If the previous installation failed during installation of the Tivoli Provisioning Manager application, you must uninstall the application and reinstall it. You can click **Back** in the installer, remove the failed application installation, and then click **Next** to rerun the discovery.

See Appendix B, "Uninstalling and reinstalling Tivoli Provisioning Manager," on page 103 for information about uninstalling Tivoli Provisioning Manager.

Previous version

This message is an error message. You must remove the existing installation before installing version 5.1.1. Refer to the uninstallation instructions in the product documentation for the existing version of Tivoli Provisioning Manager.

Operating system and hardware

VER-RHEL

The version of Red Hat you are using is not supported. See "Preinstallation Step 2: Verify operating system requirements" on page 11 for information about the supported operating systems and versions for a Linux on Intel installation.

VER-SLES

The version of SUSE you are using is not supported. See "Preinstallation Step 2: Verify operating system requirements" on page 11 for information about the supported operating systems and versions for a Linux on Intel installation.

LIN-DIST

You must use a supported Linux distribution.

- Red Hat Enterprise Linux Server release 5
- SUSE Linux Enterprise Server 9

For details about the supported Linux distributions and versions, see "Preinstallation Step 2: Verify operating system requirements" on page 11.

LIN-KERN

You must use a supported kernel version. Version 2.6 is supported. Verify the kernel version, using the command, `uname -r`.

THR-MODE

The JDK used by Tivoli Provisioning Manager does not support the Native POSIX Thread Library (NPTL), the default thread mode used by SUSE Linux Server 9, Enterprise Edition. You must force the Linux threads to be used instead on all SUSE Linux Server 9, Enterprise Edition.

To determine the current thread mode, run the following commands:

```
getconf GNU_LIBPTHREAD_VERSION
2>&1 | grep NPTL
```

For NPTL, you should get an output similar to the following example:

```
NPTL 0.61
```

To force Linux threads be used instead, run the following commands:

```
export LD_ASSUME_KERNEL=2.4.19
export RPM_FORCE_NPTL=1
```

Note: For System z, the LD_ASSUME_KERNEL is enabled by the Tivoli Provisioning Manager installer. However, it is not required after the installation, so it is recommended that it be disabled. See the following technote for instructions on managing the LD_ASSUME_KERNEL: http://www-1.ibm.com/support/docview.wss?uid=swg21308563.

CPU-SPD (warning)

The following processor speed is recommended for Tivoli Provisioning Manager. The installation for most components is single-threaded and does not take full advantage of dual processors.

Table 27. Minimum processor speed

Server type	Processor speed
64 bit IBM zSeries®	1 GHz CPU

CPU-TYPE

A regular installation is only supported on a 64-bit s390x processor.

DSK-FREE

Ensure that you have 15 GB free disk space to run the installer.

RAM-SIZE (warning)

A minimum of 4 GB of available RAM is recommended. If you proceed with less memory available, installation time will be affected.

Networking

The preinstallation checks in this section are for required ports and host name resolution. The following general host name requirements apply:

- A fully-qualified domain name is configured. For example, if the host name is `river` and the domain name is `example.com`, the fully-qualified domain name is `river.example.com`. Some computers might be configured to return a short host name only, such as `river`.
- A static IP address is configured. A dynamic IP is not supported for the provisioning server.
- If you are using a DNS server, ensure that the host name configured in the operating system matches the host name configured on the DNS server.

Using a hosts file for IP address resolution:

If you are not using a DNS server to resolve the host name of your computer, you must use a `hosts` file to resolve the host name. The file `/etc/hosts` must be properly configured with the following information:

- The IP address, fully-qualified domain name, and host name of the computer where you are running the installer as the first entry.
- The IP address `127.0.0.1`, the fully-qualified domain name `localhost.localdomain`, and the host name `localhost`

The following example shows settings for a computer with the host name `provision`.

```
#IP address  Fully Qualified Domain Name   Short Name
10.0.0.12    provision.example.com         provision
127.0.0.1    localhost.localdomain         localhost
```

PRT-FREE

Ensure that required ports are unused. The following table summarizes all communication ports used by Tivoli Provisioning Manager. The installer verifies that the following ports are available: 9080 9061 9443 9511 9512 9513 9082 9043 9045 9046 8881 1527.

Table 28. Communication ports used by Tivoli Provisioning Manager. In the **Direction** column the arrow points from the source port to the destination port.

Usage	Protocol	Provisioning server port	Direction	Managed computer port
DHCP REQUEST	UDP (broadcast)	67	←	any
DCHP REPLY	UDP	67	→	68
PROXY DHCP	UDP	4011	←	any
TFTP	UDP	69	←	any
BootDiscovery	UDP (multicast)	4011 IP:233.1.0.1	←	any
MTFTPPort	UDP	4015	←	any
MTFTPClients	UDP (multicast)	any	→	8500 IP:233.1.0.1
NBPServer	UDP	4012	←	any
FileServerPort	UDP	4013	←	any
FileMCAST-Address	UDP	any	→	10000
FASTPort	UDP	4025	←	any
SSH	TCP	any	→	22
Telnet	TCP	23	←	any
TS	TCP	any	→	3389
SNMP	UDP	any	→	161
SNMP-TRAP	UDP	162	←	any
SMB / NetBIOS	TCP	any	→	139
agent manager	TCP	9511, 9512, 9513	→	any
WebSphere Application Server	TCP	8881, 9080, 9082, 9061, 9043, 9045, 9046, 9443	→	any
Eclipse embedded database	TCP	1527	←	any

Use the following command to check port availability:

```
netstat -a | grep port
```

where *port* is the port number you want to check. If no results are returned, the port is available.

A list of connections and listening ports is displayed. Ensure that the required ports are not listed.

NET-IF

The network interface name could not be obtained.

DNS-NAME and DNS-EQIP

If you are using a DNS server to resolve host names, the host name must be defined on the DNS server. The preinstallation script uses the **nslookup** command to verify that the host name of the computer is defined on the DNS server. It also compares the host name defined on the DNS server with the local host name defined in the operating system to ensure that they match.

- If you receive the **DNS-NAME** error, the host name could not be found on the DNS server. Verify the connection to your DNS server and verify that the host name is correctly defined on the DNS server.
- If you receive the **DNS-EQIP** error, check the configuration of the host name in the operating system of the computer and on the DNS server and ensure that they match.

To verify the host name information:

1. To check the host name configured in the operating system, run the command:

   ```
   hostname
   ```

   The command returns the host name and domain name.
2. To check the host name configured on the DNS server, run the command:

   ```
   nslookup hostname
   ```

   where *hostname* is the value returned in the previous step. The command returns the fully-qualified domain name registered on the DNS server.
3. If the host names do not match, use the **hostname** command to change the value configured in the operating system.

   ```
   hostname new_name
   ```

   where *new_name* is the new host name.

The default domain name search order is as follows:

1. Domain Name System (DNS) server
2. Network Information Service (NIS)
3. Local `/etc/hosts` file

If the `/etc/resolv.conf` file does not exist, the `/etc/hosts` file is used. If only the `/etc/hosts` file is used, the fully qualified computer name must be the first one that is listed after the IP address.

Verify that the `/etc/resolv.conf` file exists and contains the appropriate information, such as:

```
domain mydivision.mycompany.com
nameserver 123.123.123.123
```

If NIS is installed, the `/etc/irs.conf` file overrides the system default. It contains the following information:

```
hosts = bind,local
```

The `/etc/netsvc.conf` file, if it exists, overrides the `/etc/irs.conf` file and the system default. It contains the following information:

```
hosts = bind,local
```

If the NSORDER environment variable is set, it overrides all of the preceding files. It contains the following information:

```
export NSORDER=bind,local
```

Run this command to display the fully qualified domain name of the computer:

```
more /etc/hosts
```

An example of the output is displayed:

```
123.123.123.123 mydivision.mycompany.com mydivision
```

The IP address is displayed followed by the fully qualified domain name and the short name.

HST-FRMT

The **HST-FRMT** message appears when the format of the file `/etc/hosts` is incorrect.

If you are using the `hosts` file to resolve IP addresses, the file must be configured correctly. The file must include:

- The IP address, fully-qualified domain name, and host name of the computer where you are running the installer as the first entry.
- The IP address `127.0.0.1`, the fully-qualified domain name `localhost.localdomain`, and the host name `localhost`

The following example shows settings for a computer with the host name `river`.

```
#IP address  Fully Qualified Domain Name   Short Name
10.0.0.12    river.example.com             river
127.0.0.1    localhost.localdomain         localhost
```

Note: Linux installations differentiate between the IP address for the `localhost` host name and the actual host name of the computer. Ensure that your `/etc/hosts` file includes the static IP address for both `localhost` and the actual host name of the computer.

HST-FQDN

This message is generated if the `host` command does not return a fully-qualified domain name for the computer. For example, if the host name of the computer is `tpmserver` and the domain name suffix is `example.com`, the fully-qualified domain name is `tpmserver.example.com`. The command requires name resolution using a DNS server, so this error message does not apply if you are using a HOSTS file for name resolution.

If you are using a DNS server for name resolution, run the `host` and check the results of the command. Ensure that the computer is correctly set up on your DNS server.

NET-LOIP

The IP address of `localhost` is not correctly defined. If you are using a `hosts` file to resolve IP addresses, ensure that the IP address for the `localhost` is configured correctly. See “HST-FRMT” for more information.

NET-PING

The installer verifies that it can run the command `ping localhost` successfully. If you receive this error, run the command manually and review any error messages generated by the command to determine the cause of the problem.

If you are using a `hosts` file to resolve IP addresses, ensure that it is configured correctly. See “HST-FRMT” for more information.

Connectivity

SSH-CFG

The file `/etc/ssh/sshd_config` does not exist for validating SSH configuration. If SSH is installed, verify that this file exists. The file contains SSH configuration settings that are used to validate other SSH requirements for installation.

SSH-INST
SSH must be installed to perform installation. Install SSH if it is not installed.

SSH-RUN
SSH is not running.

SSH must be running to perform installation. You can run the following command to check the status:

```
/etc/init.d/sshd status
```

The command returns ″sshd is running...″ if SSH is started. If it is not started, run the following command:

```
/etc/init.d/sshd
```

SSH-ROOT
The root user must have permissions to login over SSH. Ensure that root access is permitted by the SSH daemon (sshd). In the `/etc/ssh/sshd_config`, ensure that `PermitRootLogin` is set to `yes`.

```
PermitRootLogin yes
```

X11-FWD
If you are using X11 forwarding, disable it before you perform installation. If you leave X11 forwarding enabled, the installation will take a significantly longer time.

Required packages

PKG-INST
The package identified in the error message is not installed. Verify that you have installed all the required packages.

See “Required packages” on page 11 for details.

PKG-VER and PKG-NVER
The package identified in the message is not at the required version level. There are two types of messages:

PKG-VER
: This error is generated if the package is not installed or if the package is an older version than the required version. Verify that the package is installed and verify that you are using the correct version level or a newer version.

PKG-NVER
: This warning is generated if the package is a newer version than the required version. You can continue installation with the newer package version, but the installation or operation of the product might fail if the newer package is incompatible with Tivoli Provisioning Manager.

See “Required packages” on page 11 for details and package requirements.

PKG-PATH
This error indicates that paths for required packages are not set correctly. See “Required packages” on page 11 for information about required packages and package paths.

User management and permissions

GRP-TIV

This error is displayed if you have not created the required `tivoli` user group and assigned the user `tioadmin` as a member of the group. See "Preinstallation Step 5: Set up required users" on page 18 for a list of required users and groups.

SH-ROOT

You must be logged on as `root` to perform installation.

NIS-USR and NIS-GRP

Network Information Service (NIS) is not supported for managing user accounts or groups. Disable NIS user management.

NIS-USRC and NIS-GRPC

Network Information Service (NIS) is not supported for managing user accounts or groups. These warning messages are generated when NIS in compatibility mode is detected. It is recommended that you disable NIS.

MSK-SET

The umask must be set to `002` for the `root` user. The `umask` setting determines the default permissions for a user when new files are created. The setting of `0002` gives read, write, and execute permissions to a file owner and the owner's primary group, and grants other users read and execute permissions.

Make the following changes:

Table 29. Setting umask for root

Shell used by `root`	Required setting
Korn	In home directory for `root`, add the following line to the file `.profile` `umask 002`
Bash	In home directory for `root`, add the following line to the files `.bash_profile` and `.bashrc` `umask 002`

You can return existing umask settings to their original values after installation.

TMP-PERM

Permissions on the `/tmp` directory must be set to 1777 (drwxrwxrwt). The 777 means that any user can read or write to the directory. The initial 1 means that only the owner of a file in the directory can modify or delete the file. This is the default permission setting for the directory.

USR-ULMT

Required user limits must be set as described in "User limits" on page 20.

Prerequisite applications

If you want to use an existing installation of WebSphere Application Server or a preinstalled database server, ensure that you meet the requirements in this section. For the prerequisite applications, you must use the correct version, including the correct fix pack level. Use the installation media provided with Tivoli Provisioning Manager to ensure that you get the right version. Installing from other sources can lead to installation or operational problems that are hard to debug.

Table 30. Supported prerequisite software

Application	Supported version
Database	DB2 Enterprise Server Edition 8.1, Fix Pack 11 **Note:** If the installer installs DB2 for you, it creates a 64-bit instance for the DB2 database.
Application server	WebSphere Application Server 6.0.2.11 (Version 6.0 with refresh pack 2 and fix pack 11) **Note:** Only the 64-bit version of WebSphere Application Server is supported.

DB2-VER

This warning message is displayed if an unsupported version of DB2 is found. If you want to use existing installation of DB2 with Tivoli Provisioning Manager, it must be at the supported version level: DB2 Enterprise Server Edition 8.1, Fix Pack 11.

To check the version of DB2, run the command, `db2level`.

Important: Installation on with a different version of DB2 is not supported and might affect the installation or operation of Tivoli Provisioning Manager.

WAS-SEC

This warning message appears if security is enabled in WebSphere Application Server. When security is enabled, the status of WebSphere Application Server cannot be verified. Ensure that WebSphere Application Server is stopped before you continue with installation. See "WAS-STOP" for instructions to stop WebSphere Application Server.

WAS-STOP

WebSphere Application Server must be stopped before you run the installer.

1. Change to the `bin` subdirectory of the WebSphere Application Server installation, the default is /opt/IBM/WebSphere/AppServer/`bin`.
2. Run the command:

   `./stopServer.sh` *app_server* `-username` *was_adminID* `-password` *password*

   app_server
   : The name of the application server. The default is `server1`.

   was_adminID
   : The WebSphere Application Server administrator user name. After a new installation of Tivoli Provisioning Manager, the user name is `tioadmin`.

   password
   : The WebSphere Application Server administrator password for the specified user name.

Some Java processes might still be running and can cause installation to fail. Ensure that the processes are stopped.

1. Run the following command:

   ```
   ps -ef | grep java
   ```

2. If processes are still running, stop them with the command:

   ```
   pkill -9 java
   ```

WAS-VER

This warning is displayed if an unsupported version of WebSphere Application Server is found. If you are using an existing installation of WebSphere Application Server, it must be at the supported version level: 6.0.2.11 (Version 6.0 with refresh pack 2 and fix pack 11) is required.

To verify the version of WebSphere Application Server, run the following command from the *$WAS_HOME*/bin directory.

```
genVersionReport.sh
```

The command generates a report called versionReport.html. The report identifies the installed version of WebSphere Application Server and all installed maintenance packages.

Important: Installation on with a different version of WebSphere Application Server is not supported and might affect the installation or operation of Tivoli Provisioning Manager.

Other requirements

PKG-GUID

A Global Unique Identifier (GUID) exists on the computer. A GUID is used to identify a Tivoli common agent on a computer. The agent ID is the name of the installation directory of the common agent. If you are uninstalling the Tivoli GUID tool or the Tivoli Common Agent, the agent ID is not automatically removed from the system. You must remove existing agent IDs from the computer before you install Tivoli Provisioning Manager

To remove the GUID:

1. Check if the GUID still exists:
   ```
   rpm -qa | grep TIVguid
   ```
2. If the GUID exists, run the following command to remove it.
   ```
   rpm -evv TIVguid-1.3.0-0
   ```

TMP-CLN

On RedHat Advanced Server 4.0, the yeahch utility is installed. By default, the /etc/cron.daily/tmpwatch script runs daily and removes files in /tmp that have not been accessed in 10 days. By default, the Tivoli Provisioning Manager installer is installed under /tmp. See "Preinstallation Step 6: Verifying the environment" on page 21 for instructions to temporarily disable the script.

Recovering from other errors

This section lists recovery steps for some errors that might occur.

Before prerequisite software is installed

This section describes recovery actions for errors that might occur after the installer starts and before any prerequisite software is actually installed or configured by the installer. This part of the installation process includes:

- Validation of credentials.
- Specifying the installation topology.
- Validation of prerequisite hardware and software.
- Specifying installation options for components that will be installed.

The following subsections describe possible errors during this stage of the installation.

Display problems while using Exceed X window server

If DISPLAY is exported to an Exceed X window server, to install Tivoli Provisioning Manager, the label and the progress bar of the first product being installed, disappears, when the installation is started. After the first product is installed, the progress bar is displayed again, but the label will not appear.

During installation of software

This section describes recovery actions for errors that might occur when the installer performs installation of software components.

Preinstalled software not detected

If you preinstalled the prerequisite software but it was not identified by the installer, verify that you are using the correct version, including any fix packs or other software updates that are required for Tivoli Provisioning Manager installation. Previous product levels or multiple installations of the same application with different product levels is not supported.

See Appendix D, “Preinstalling required software,” on page 115 for details about requirements for preinstalled software.

Installer unable to copy from disks

Error:

The installer is unable to copy the installation files from Tivoli Provisioning Manager disks or complete the installer.

Resolution:

You must download SUN’s JVM 1.4.2.11 and then start installer again. To download the JVM, go tohttp://java.sun.com/j2se/1.4.2/download.html

To workaround this problem:

1. Run the installer.
2. Click **Cancel** at the Welcome panel.
3. Install the SUN’s JRE 1.4.2.x into the `$TIL_HOME/eclipse/jre` folder.
4. Launch `$TIL_HOME/eclipse/eclipse` again.

Installation of DB2 fails when node name is different than host name

Error:

DB2 installation stops before it is complete. On the computer where you are performing the installation, the configured node name is different than the configured host name.

Explanation:

The DB2 installation uses the **uname -n** command to obtain the node name of the computer. Typically, the node name is the same as the host name that is returned with the **hostname** command. Tivoli Provisioning Manager installation requires that the host name and the node name of the computer are identical.

Resolution:

Check the value of the host name and node name. You must change the node name if it does not match the host name.

1. Run the command `hostname` to obtain the host name.
2. Run the command `uname -n` to obtain the node name.
3. If the node name is different than the host name:
   a. Log on as root.
   b. Change the node name to match the host name. For example, to change the node name to **myserver**, run the following command:

      ```
      uname -S myserver
      ```

After DB2 installation

This section lists recovery steps for some errors that might occur after the DB2 installation.

DB2 connection fails with a password incorrect error for the DB2 instance

Fix pack install after the DB2 base image install updates only DB2 libraries in the installation directory but not the instance libraries in /home/db2inst1, so there will be a mismatch between the libraries. An error can occur while starting DB2.

Resolution

Complete the following steps:

1. Navigate to /opt/IBM/db2/v8.1/instance as a root user.
2. Stop the DB2 instance using the `db2istop db2inst1` command.
3. Update the instance using the `db2iupdt db2inst1` command.
4. Start the instance using the `db2istart db2inst1` command.

Missing WebSphere Application Server installation causes Tivoli Provisioning Manager installation to fail

If WebSphere Application Server was previously installed on the computer, check for the following message in `tcinstall.log`

```
WebSphere Application Server does not appear to be installed on the system.
ACTION: Install WebSphere Application Server
```

If WebSphere Application Server was uninstalled but the WebSphere Application Server installation directory was not removed, the installer might initially identify WebSphere Application Server as installed, and then fail during Tivoli Provisioning Manager installation.

If WebSphere Application Server was uninstalled on the computer, perform the following steps:

- Ensure that the WebSphere Application Server installation directory is removed. The default location is /opt/IBM/WebSphere/AppServer.
- Click **Back** in the installer until you reach the **Configure the target servers** panel. Click **Next** so that the installer can check again for installed components.

On the **Validation Summary** panel, the **Found** column displays **No** if WebSphere Application Server is fully uninstalled. You can now continue with installation.

The device manager federator installation fails

- If the device manager federator installation failed, check for these additional items:
  1. Verify that all the device classes and job types are registered. Type the following command:

     ```
     DMS_HOME/bin/deviceclass.sh -list
     ```

     The command lists all device classes that are registered.
  2. Test auto-enrollment for a device. You can install and start a Windows 32-bit agent to test the auto-enrollment. Test submitting a job using the console to an enrolled device. Test running a job on an enrolled device. You can connect to the server with a Windows 32-bit agent to test if a job runs on a device.
- If device manager federator configuration failed, check these items:
  1. Verify the configuration parameters. Configuration parameters used by the installer are in *$TIO_HOME*/DeviceManager/config/DMSconfig.properties.
  2. Ensure that the dmsadmin user ID was successfully created on the database server.
     - Ensure that the password is not set to expire at the next login.
     - Verify that the passwords provided to the device manager database installation are correct by connecting to DB2 with the user name and password specified. Run the following DB2 command;

       ```
       db2 connect to dms user dmsadmin USING password
       ```

       Note: This command only works if the device manager database was created when the database configuration was completed.
     - Ensure that the DB2 instance specified is correct. To list the valid DB2 instances, type db2ilist from a DB2 command environment.
     - Ensure the DB2 port is correct. Open the file /etc/services and locate the following line:

       ```
       db2c<instance> <port>/tcp #Connection
       port for DB2 instance <instance>
       ```
  3. Ensure that the Oracle port is correct. Find the correct Oracle port by using the /lsnrctl status command. Use this port everywhere.

     Note: You might have to find the exact port on which the Oracle server is listening.
- If there are problems starting device manager federator, check the following items:
  - If you receive the message DYM2794E: Failed to create the database connection pool in the WebSphere Application Server SystemOut.log file, ensure that DB2 is started and that the DB2 client is configured correctly.
  - If you receive a message about no protocol found in the WebSphere Application Server SystemOut.log file, verify the values for the proxy settings that are used to construct the Device Manager server URL (DMS_PROXY_PROTOCOL and DMS_PROXY_HOSTNAME have not been changed. Restart the DMS_AppServer after making any changes to the WebSphere environment variables.

– If you receive an AccessControlException error that references a JDBC driver for the database, check your security settings in WebSphere Application Server.
  - If Global Security was enabled, which, Java 2 Security is enabled by default.
  - If Java 2 Security is enabled, the device manager server servlet gets an AccessControlException when it starts. The servlet calls the JDBC driver to access a system resource for which it does not have permission. To eliminate the AccessControlException message and start Device Manager, follow the steps for enabling security as described in your WebSphere Application Server documentation.

Installation using a Reflection X connection fails

During installation, the installation fails with the following error:

```
An error has occurred. See the log file
/var/tmp/TopologyInstaller/workspace/.metadata/.log
```

The log file also contains an error that starts with ″org.eclipse.swt.SWTError: Font not valid″.

This error occurs if a recognized font cannot be resolved at startup time. This error has been observed when accessing a remote computer with Reflection X.

You can fix the problem by changing font settings in Reflection X.

1. In Reflection X Client Manager, click **Settings > Fonts**. change **Sub directories and font servers** to `100dpi 75dpi misc hp sun ibm dec`.
2. Reconnect to the computer where you are performing the installation and run the installer again.

After Tivoli Provisioning Manager installation

This section describes recovery actions for errors that might occur after Tivoli Provisioning Manager installation.

SOAP services fail to start

SOAP services should start automatically after Tivoli Provisioning Manager installation. If the message `The specified username or password is incorrect` is displayed when you try to log on to the dynamic content delivery management center console and SOAP services do not start successfully, check *$TIO_LOGS*`/soap/desoap_start.log` for either of the following exceptions:

```
Caused by: java.lang.NoClassDefFoundError: com/ibm/pvcws/proxy/Logger
   at java.lang.ClassLoader.defineClass0(Native Method)
   at java.lang.ClassLoader.defineClass(ClassLoader.java:810)
   at org.eclipse.osgi.framework.adaptor.core.DefaultClassLoader.defineClass
(DefaultClassLoader.java:370)
   at org.eclipse.core.runtime.adaptor.EclipseClassLoader.defineClass
(EclipseClassLoader.java:233)
```

or

```
Caused by: java.util.MissingResourceException: Can't find bundle for base name
com.ibm.pvcws.proxy.wsosgimessages, locale en_US
   at java.util.ResourceBundle.throwMissingResourceException(ResourceBundle.
java:825)
```

```
at java.util.ResourceBundle.getBundleImpl(ResourceBundle.java:794)
at java.util.ResourceBundle.getBundle(ResourceBundle.java:532)
at com.ibm.pvcws.proxy.WsosgiMessages.<clinit>(WsosgiMessages.java:32)
... 39 more
```

To manually start the SOAP services:

1. Stop Tivoli Provisioning Manager. For instructions, see "Starting and stopping Tivoli Provisioning Manager" on page 53.
2. Open the file called *$TIO_HOME*/tools/run-desoap.sh and edit the following lines:

   Original: -Xbootclasspath/a:$TIO_HOME/lib/jaasmodule.jar \
   New: -Xbootclasspath/a:$TIO_HOME/lib/jaasmodule.jar:$TIO_HOME/eclipse/plugins/com.ibm.pvcws.osgi/com.ibm.pvcws.osgi.props.jar \

   Original: -noSplash -application launcher.CliLauncher \
   New: -noSplash -clean -application launcher.CliLauncher \

   Important: Ensure that the \ character is the final character in each line.
3. Start Tivoli Provisioning Manager. For instructions, see "Starting and stopping Tivoli Provisioning Manager" on page 53.
4. Verify that the SOAP services started by checking the *$TIO_LOGS*/soap/desoap_start.log.

Installation of dynamic content delivery management center fails

Description

Installation of the dynamic content delivery service fails because the location of Java cannot be found by the installer. In the log file /opt/ibm/tivoli/ctgde/logs/cds_upgrade.txt, the error description looks like the following example:

```
INSTALLER_PATH=/extra/ibm/tivoli/tio/CDS/scripts/./setup.binChecking the environment
variables specifed in the JVM files to find the JVM...
Verifying... /bin/java -cp /tmp/istemp7613004171417/Verify.jarVerify java.vendor
java.versionVerification passed for / using the JVM file /tmp/istemp7613004171417/
relative_to_upgrade.jvm.
JavaHome is not resolved correctly in the jvm file /tmp/istemp7613004171417/
relative_to_upgrade.jvm.
Failed to launch the application.
```

Resolution

This error occurs when Java is installed in /bin/java and /bin is in the path listed in the PATH variable. To fix the error, update the PATH variable so that the **java** command does not resolve to the /bin directory.

1. To confirm the location of Java, run the command

   ```
   which java
   ```

   If this command is not available on your system, run the following command instead

   ```
   type java
   ```
2. If the returned value is /bin/java, run the following command to display the contents of the PATH variable:

   ```
   echo $PATH
   ```
3. If the first part of the path is /bin, update the PATH variable so that /bin does not resolve the **java** command. There are several options for making this change:

- Move /bin to the end of the list of paths in the PATH variable. Normally the **java** command will resolve to /usr/bin/java.
- Create a symbolic link for /bin/java under another directory and add that path to the front of the PATH variable. For example, if you have a link in /usr/bin to the **java** command, ensure that /usr/bin is at the front of the PATH variable or place /usr/bin before /bin in the list of paths.

Out Of Memory error

Registration of device manager endpoints causes an OutOfMemory error. The error appears in the WebSphere Application Server log file *$TIO_HOME*/tioprofile/logs/server1/SystemOut.log.

Workaround

Change the heap size.

1. Log on to the WebSphere Application Server administration console at:

   https://*hostname*:*port*/ibm/console/logon.jsp

   where *hostname* is the WebSphere Application Server host name and *port* is the secure host port. The default port number is 9043.
2. Change the maximum heap size:
   a. Click **Servers** > **Application servers** > *server_name* > **Process Definition** > **Java Virtual Machine**.
   b. Change the **Maximum Heap Size** setting to 2048 MB.

Chapter 7. Upgrading Tivoli Provisioning Manager to Tivoli Intelligent Orchestrator

You can upgrade and existing Tivoli Provisioning Manager Version 5.1.1 installation to Tivoli Intelligent Orchestrator Version 5.1.1. Before you begin to upgrade ensure that the following requirements are met:

- Tivoli Provisioning Manager is stopped. See "Stopping Tivoli Provisioning Manager" on page 56.
- You have located the *Tivoli Intelligent Orchestrator Version 5.1.1* CD.
- Ensure that the directory server and the database servers are started.

To upgrade to Tivoli Intelligent Orchestrator:

1. Log on as `root`.
2. Unzip Tivoli Intelligent Orchestrator Version 5.1.1 Disk 2 into a folder, then run **unixInstall.sh**
3. On the **Welcome** panel, read the information and then click **Next** to continue with the installation.
4. On the **Software License Agreement** panel, Review the terms of the license agreement. You must accept the license agreement to proceed with installation. You must accept the terms of the license agreement to continue with the installation.
5. The installer indicates that Tivoli Provisioning Manager is detected and will be upgraded to Tivoli Intelligent Orchestrator. Review the information about ensuring that all Tivoli Provisioning Manager processes have been completed. Click **Next** to continue.

   Note: The upgrade will take some time to finish. The installation is complete when the Installation Summary panel is displayed.
6. When the Installation Summary panel is displayed, click **Finish**. You have completed the upgrade to Tivoli Intelligent Orchestrator.

Note: If you want to uninstall Tivoli Provisioning Manager after the upgrade, you must first uninstall Tivoli Intelligent Orchestrator before you can uninstall Tivoli Provisioning Manager.

Appendix A. Values for a default installation

The following tables summarize the settings that are used during a default installation. When you choose a default installation, default values are used for the settings that you would need to specify during a custom installation.

Tivoli Provisioning Manager default settings

The following settings are used to configure Tivoli Provisioning Manager. They correspond to settings described in "Tivoli Provisioning Manager tab" on page 36. The tables in this section point to the corresponding step in a custom installation so that you can learn more about the settings.

Table 31. Tivoli Provisioning Manager. Settings for "Tivoli Provisioning Manager settings" on page 37.

Setting	Value
Installation directory	/opt/ibm/tivoli/tpm
Local file repository	/opt/ibm/tivoli/tpm/repository
Management IP address:	The IP address specified on the **Configure the target servers** panel. See Figure 5 on page 30.

Table 32. Tivoli Provisioning Manager: WebSphere Application Server. Settings for "WebSphere Application Server settings" on page 38.

Setting	Value
Domain Name Suffix	The domain name portion of the fully-qualified domain name specified on the **Configure the target servers** panel. See Figure 5 on page 30. For example, if your fully-qualified domain name is `tpmserver.admin.example.com`, the domain name suffix is `admin.example.com`. This information is used by WebSphere Application Server.
Installation directory:	/opt/IBM/WebSphere/AppServer
Default host port	9082
SSL server authentication port	9045
SSL mutual authentication port:	9046
Cell Name	*hostname*Node01Cell The value *hostname* is host name of the Tivoli Provisioning Manager computer. For example, if the host name is admin, the cell name is adminNode01Cell.
Node Name	*hostname*Node01
Settings in the Advanced section	
Admin host port	9061
Admin host secure port	9044
Bootstrap port	2810
SOAP connector port	8881
SAS SSL server authentication listener port	9402

Table 32. Tivoli Provisioning Manager: WebSphere Application Server (continued). Settings for "WebSphere Application Server settings" on page 38.

Setting	Value
CSIV2 SSL server authentication listener port	9404
CSIV2 SSL mutual authentication listener port:	9403
ORB listener port:	9101
DCS unicast port:	9354
SIB endpoint port:	7277
SIB endpoint secure port	7287
SIB MQ endpoint port:	5559
SIB MQ endpoint secure port:	5579

Table 33. DB2. Settings for "DB2 settings" on page 40.

Setting	Value
Database Server Connection Port:	50001
Database name	tc
Local Instance owner group name	tioadmin
Database Server Instance owner user name:	tioadmin
Database Server Instance owner password	[tioadmin user password]
DB2 not installed - Instance owner home directory:	/home/tioadmin
DB2 installed - Existing local DB2 instance location	/home/tioadmin/sqllib

Core component default settings

The following settings are used to configure core components. They correspond to the settings described in "Tivoli Provisioning Manager Components Configuration tab" on page 41.

Table 34. Core components

Setting	Value
Installation directory	/opt/IBM/AgentManager
Registration port:	9511
Secure port	9512
Public port:	9513
Agent registration password	The password that you specified for the user **tioadmin** on the **Default installation** panel. See Figure 8 on page 35.
Agent Manager password:	The password that you specified for the user **tioadmin** on the **Default installation** panel. See Figure 8 on page 35.
Management center administrator	The value that you specified for **Tivoli Provisioning Manager administrator user name** in "Tivoli Provisioning Manager tab" on page 36.

WebSphere Application Server default settings

The following settings are used to configure core WebSphere Application Server. They correspond to the settings described in “WebSphere Application Server tab” on page 43.

Table 35. WebSphere Application Server

Setting	Value
Installation directory	/opt/IBM/WebSphere/AppServer

DB2 default settings

The following settings are used to configure core DB2. They correspond to the settings described in “DB2 tab” on page 45.

Table 36. DB2

Setting	Value
Installation directory	/opt/IBM/db2/V8.1
Language pack	System locale or English if the language is not supported.
Instance port	50001
Instance owner user name	tioadmin
Instance owner password	The password that you specified for the user **tioadmin** on the **Default installation** panel. See Figure 8 on page 35.
Instance owner group name	tioadmin
Fenced user name:	tioadmin
Fenced user password	The password that you specified for the user **tioadmin** on the **Default installation** panel. See Figure 8 on page 35.
Fenced user group name	tioadmin

Appendix B. Uninstalling and reinstalling Tivoli Provisioning Manager

The Tivoli Provisioning Manager uninstaller removes Tivoli Provisioning Manager only. To properly and completely remove Tivoli Provisioning Manager, you must remove components in the following order:

1. "Uninstall core components"
2. "Uninstalling Tivoli Provisioning Manager" on page 105
3. "Remove or unconfigure prerequisite applications" on page 107
4. "Remove items remaining after uninstallation" on page 108

Uninstall core components

Core components must be uninstalled in the following order:

1. "Uninstall the device manager federator"
2. "Uninstall the dynamic content delivery management center" on page 104
3. "Uninstall the agent manager" on page 105

Note: If you want to continue to use any of these components with other products, Tivoli Provisioning Manager must remain installed. These component might not work if you uninstall Tivoli Provisioning Manager.

Uninstall the device manager federator

1. Close all database command windows and device manager consoles.
2. Log on as `tioadmin`
3. Ensure that:
   - Tivoli Provisioning Manager is stopped.
   - The database is running.
4. Remove the device manager federator database tables:
   a. Change to the `$TIO_HOME/tools/DMS` directory.
   b. Run the following command:

      `./DMS_DB2_uninstall.sh` *db_name db_owner db_owner_pwd dm_dir*

      db_name
      The name of the Tivoli Provisioning Manager database.

      db_owner
      The database instance owner. For a default installation, the Tivoli Provisioning Manager database owner is `tioadmin`. For a custom installation, the default Tivoli Provisioning Manager database owner is `db2inst1`.

      db_owner_pwd
      The password for the database instance owner.

      dm_dir
      The full path of the device manager federator installation directory. By default the files are installed in the `DeviceManager` subdirectory of the Tivoli Provisioning Manager installation directory.

      The following example uses `db2inst1` as the instance owner.

```
./DMS_DB2_uninstall.sh tc db2inst1 pas5word /opt/ibm/tivoli/tpm/DeviceManger
```

5. Log out `tioadmin` and log on as `root` to continue with uninstallation.
6. Change to the directory *$TIO_HOME*/DeviceManager/config.
7. In *$TIO_HOME*/DeviceManager/config, find the device manager federator configuration file that starts with DMSconfig100. You will need this file name to remove the device manager federator configuration.
8. If you configured a read-only directory server for use with Tivoli Provisioning Manager and you changed the administrator user for WebSphere Application Server to another user name, perform the following steps:
   a. Open the file that you identified in step 7 in a text editor.
   b. In the following line, change `tioadmin` to the current WebSphere Application Server administrator user name.
      ```
      instWASUsername=tioadmin
      ```
      For example, if the current WebSphere Application Server administrator is `wasadmin`, change the line to:
      ```
      instWASUsername=wasadmin
      ```
   c. In the next line, change the value of `instWASPassword` to the password for the current WebSphere Application Server administrator. For example, if the current password is `pass5word`, change the line to:
      ```
      instWASPassword=pass5word
      ```
9. Remove device manager federator configuration with the following command:
   ```
   ./DMSremoveconfig.sh -server -file ./DMSconfig_file -showtrace
   ```
   Replace *DMSconfig_file* with the name of the file that you identified in step 7.
10. Change to the directory $TIO_HOME/DeviceManager/_uninst.
11. Run the uninstaller.
    ```
    uninstaller.bin
    ```
12. Remove the device manager federator installation directory $TIO_HOME/DeviceManager.

Uninstall the dynamic content delivery management center

Perform the following steps to remove the dynamic content delivery management center.

1. Log on as `root`.
2. Ensure that Tivoli Provisioning Manager is stopped.
3. Ensure that the device manager federator is uninstalled. See "Uninstall the device manager federator" on page 103.
4. Change to the *$TIO_HOME*/CDS/_uninst directory.
5. Run the uninstaller with the command
   ```
   ./uninstaller.bin -silent
   ```
   The uninstallation process runs in the background and you are returned to the command prompt.
6. When the uninstallation is complete, remove the dynamic content delivery management center installation directory *$TIO_HOME*/CDS.
7. Ensure that the registry entries for the dynamic content delivery management center are removed. The entries are stored in the following file.
   ```
   /root/InstallShield/Universal/cds_manager/Gen1/_vpddb/vpd.script
   ```
   If the `cds_manager` directory is empty, the files have been removed automatically. If the `Gen1` directory still exists, delete it.

Uninstall the agent manager

Uninstalling the agent manager removes the agent manager servlets from WebSphere Application Server. The uninstallation wizard does not drop the registry database or delete the agent manager objects from the database.

1. Log on as `tioadmin`.
2. Ensure that Tivoli Provisioning Manager is stopped.
3. Ensure that the device manager federator and the dynamic content delivery management center are uninstalled. See "Uninstall the device manager federator" on page 103 and "Uninstall the dynamic content delivery management center" on page 104.
4. Remove the database tables.
   a. Change to the *$TIO_HOME*`/tools/CAS` directory.
   b. Run the following command:

      `./CAS_DB2_uninstall.sh` *db_name db_owner db_owner_pwd*

      db_name
      The name of theTivoli Provisioning Manager database.

      db_owner
      The database instance owner. For a default installation, the Tivoli Provisioning Manager database owner is `tioadmin`. For a custom installation, the default Tivoli Provisioning Manager database owner is `db2inst1`.

      db_owner_pwd
      The password for the database instance owner.

      The following example uses `db2inst1` as the instance owner.

      ```
      ./CAS_DB2_uninstall.sh tc db2inst1 mypassword
      ```

   c. Log out as `tioadmin` and log on as `root` to continue with uninstallation.
5. Run the uninstaller and follow the instructions in the wizard.

   AM_HOME`/_uninst/uninstall.bin`

   where *AM_HOME* is the agent manager installation directory. The default location is `/opt/IBM/AgentManager`.
6. Delete the agent manager installation directory.

Uninstalling Tivoli Provisioning Manager

Running the uninstallation program only removes Tivoli Provisioning Manager. It does not remove:

- Core components. Core components must be removed before you uninstall Tivoli Provisioning Manager.
- The database and application server
- Log files.

You must uninstall Tivoli Provisioning Manager and the installer if you want to reinstall it.

To uninstall Tivoli Provisioning Manager:

1. Log on as `root`.
2. Ensure that you have removed core components. See "Uninstall core components" on page 103.

3. Stop Tivoli Provisioning Manager and ensure that any running Java processes are stopped. See "Stopping Tivoli Provisioning Manager" on page 56 for instructions.
4. Ensure that the database is still running.

   To verify that DB2 is running:
   a. Switch to the DB2 instance owner. For a default installation, the Tivoli Provisioning Manager database owner is `tioadmin`. For a custom installation, the default Tivoli Provisioning Manager database owner is `db2inst1`.

      For example, if the instance owner is `db2inst1`, run the command.

      ```
      su - db2inst1
      ```
   b. Run the command to start DB2:

      ```
      db2start
      ```

      DB2 is started if it is not running already. If DB2 is already running, the following message is displayed.

      ```
      SQL1026N  The database manager is already active
      ```

   To verify the status of the Oracle database (supported by SLES 9 only) and listener:
   a. Log on to SQL*Plus. The status of the database is displayed when you log on.
   b. Run the following command to verify the status of the listener:

      ```
      lsnrctl status
      ```
5. If you want to run the uninstaller from a Gnome terminal window, configure the terminal window to run as a login shell.
   a. Open the terminal window.
   b. Click **Edit** > **Current® Profile**.
   c. Click the **Title and Command** tab.
   d. Under **Command** select the **Run command as login shell** check box.
   e. Close the Edit window.
   f. Close the terminal window.
   g. Open a new terminal window.
6. Change to the directory with the uninstaller. The default location is:

   ```
   /opt/ibm/tivoli/tpm/_uninst/_uninstTPM
   ```
7. Run the following command:

   ```
   ./uninstaller.bin
   ```
8. If you want to reinstall Tivoli Provisioning Manager, you must remove the database. When prompted, select the option to remove the database and specify your database administrator user name and password. For DB2, use your database instance administrator user name and password.
9. Specify your WebSphere Application Server administrator user name and password when prompted. If you are using the default operating system authentication for Tivoli Provisioning Manager, the user name is `tioadmin`. If you configured a directory server to authenticate users, specify the new user name and password that you set up with the instructions in "Configuring a read-only directory server" on page 63. The default user name is `wasadmin`.

   The uninstaller checks if WebSphere Application Server is running. If WebSphere Application Server is running, the uninstaller stops it and then continues with uninstallation.
10. Remove the `/var/tmp/install/TPMinstall` directory if it exists.

11. If you will be reinstalling Tivoli Provisioning Manager, perform the following steps:
    a. Remove the Tivoli Provisioning Manager installation directory.
    b. Keep the user `tioadmin` so that it is ready for the reinstallation.
    c. Keep the user directory `/home/tioadmin`.

Remove or unconfigure prerequisite applications

This section describes how to remove DB2 and WebSphere Application Server.

- If you no longer require these applications or if you want to reinstall them, use the information in this section to remove the applications.
- If your existing prerequisite software is properly installed, you can reuse them for a reinstallation of Tivoli Provisioning Manager. The installer will automatically discover the existing installations.

Uninstalling DB2

1. Log on as `root`.
2. Ensure that you have removed the following items if they are already installed:
   - Core components. See "Uninstall core components" on page 103.
   - Tivoli Provisioning Manager. See "Uninstalling Tivoli Provisioning Manager" on page 105.
3. Drop all databases. with the command `drop database`.
4. Remove the DB2 Administration Server if it still exists. If you removed the database during uninstallation of Tivoli Provisioning Manager, this step is not required.
   a. Log in as the DB2 administration server owner. For a default installation, the Tivoli Provisioning Manager database owner is `tioadmin`. For a custom installation, the default Tivoli Provisioning Manager database owner is `db2inst1`.
   b. Stop the DB2 administration server with the command `db2admin stop`.
   c. Remove the Administration Server. Run the following command as `root`.
      `DB2_HOME``/instance/dasdrop`

      where *`DB2_HOME`* is the DB2 installation directory. The default location is `/opt/IBM/db2/V8.1`.
5. Remove DB2 instances if they exist.
   a. Log in as the owner of the DB2 instance. For a default installation, the Tivoli Provisioning Manager database owner is `tioadmin`. For a custom installation, the default Tivoli Provisioning Manager database owner is `db2inst1`.
   b. Run the startup script:
      `instance_home``/sqllib/db2profile`

      where *`instance_home`* is the home directory of the instance owner. For a default installation, the default is `/home/tioadmin`. For a custom installation, the default is `/home/db2inst1`.
   c. Stop all database applications with the command `db2 force application all`.
   d. Stop the DB2 database manager with the command `db2stop`.
   e. Confirm that the instance is stopped with the command `db2 terminate`.

f. Remove the instance by running the following command as root:
   DB2_HOME/instance/db2idrop *instance_name*

6. Uninstall DB2:
   a. Extract the contents of the DB2 installation image, if the installation image is not currently on the computer.
   b. Change to the ese directory of the installation image.
   c. Run the command ./db2_deinstall.
   d. If you will be reinstalling Tivoli Provisioning Manager, keep all the DB2 users, groups, and home directories that were created in Chapter 2, "Preinstallation checklist for Linux on System z," on page 9.
7. If you want to reinstall Tivoli Provisioning Manager after uninstalling DB2, remove registered DB2 instance entries in /etc/services. The default port number is 50001. It can be changed in a custom installation, but it cannot be changed for a default installation. Installation will fail if the port number used to reinstall DB2 conflicts with a port that is already registered.

Uninstalling WebSphere Application Server

1. Log on as root.
2. Ensure that you have removed the following items if they are already installed:
   - Core components. See "Uninstall core components" on page 103.
   - Tivoli Provisioning Manager. See "Uninstalling Tivoli Provisioning Manager" on page 105.
3. Change to the WebSphere Application Server installation directory. The default is /opt/IBM/WebSphere/AppServer.
4. In the _uninst subdirectory, run the command ./uninstall.
5. Remove the WebSphere Application Server installation directory.
6. In the /root directory, verify that all WebSphere Application Server entries are removed from vpd.properties.
7. You can optionally remove temporary files and log files in the following locations.

   ```
   /tmp/was
   /tmp/was-logs
   ```

   If you plan to reinstall WebSphere Application Server, these files will be removed automatically.

Remove items remaining after uninstallation

After uninstalling Tivoli Provisioning Manager there are a number of items that are not removed by the installer. You must remove these items to ensure that Tivoli Provisioning Manager is completely removed from your system.

Some files, such as log files, might remain in the directory where Tivoli Provisioning Manager was installed. Uninstallation only removes files created during the installation process.

The following section provides more details about some files that remain after installation. Some of these items must be removed if you plan to reinstall Tivoli Provisioning Manager.

Application files and configuration settings

Files and configuration settings that remain after some applications are uninstalled can cause an installation of Tivoli Provisioning Manager to fail. Ensure that you check for files and settings that need to be removed.

DB2 If DB2 was previously installed, ensure that registered DB2 instances are removed from `/etc/services`. The default DB2 port number is `50001`. If this port is registered from a previous DB2 installation or used by another service, a default installation. A custom installation will fail if the port that you specify conflicts with port that is registered in `/etc/services`.

Tivoli Provisioning Manager
If you uninstalled Tivoli Provisioning Manager, ensure that the Tivoli Provisioning Manager installation directory has been deleted. The default location is /opt/ibm/tivoli/tpm. If this directory remains after uninstallation, reinstallation of the product will fail.

WebSphere Application Server
If WebSphere Application Server was previously installed on the computer, verify the following items:

- Ensure that the WebSphere Application Server installation directory is deleted. The default location is /opt/IBM/WebSphere/AppServer. If this directory remains after uninstallation, reinstallation of the product will fail.
- The `vpd.properties` file lists program components that are currently installed. It helps installers to recognize previous installations of WebSphere Application Server. When WebSphere Application Server is uninstalled, entries in `vpd.properties` are normally removed automatically. In some situations, however, the entries are not removed properly when WebSphere Application Server is uninstalled. If these entries remain when you start a Tivoli Provisioning Manager installation, the installer cannot properly validate whether WebSphere Application Server is installed and if WebSphere Application Server is currently running and installation will fail.

  Check the `vpd.properties` for entries that must be removed. The file is located the `root` directory.

  For more information about the file, see the following topic in the WebSphere Application Server information center: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.base.doc/info/aes/ae/rins_vpd.html

Global Unique Identifier

A Global Unique Identifier is used to identify a Tivoli common agent on a computer. The agent ID is the name of the installation directory of the common agent. If you are uninstalling the Tivoli GUID tool or the Tivoli Common Agent, the agent ID is not automatically removed from the system. You must remove existing agent IDs from the computer before you install Tivoli Provisioning Manager.

To remove the GUID:

1. Check if the GUID still exists:
   ```
   rpm -qa | grep TIVguid
   ```
2. If the GUID exists, run the following command to remove it.
   ```
   rpm -evv TIVguid-1.3.0-0
   ```

Reinstalling Tivoli Provisioning Manager

Before you reinstall Tivoli Provisioning Manager, you must uninstall it first. See "Uninstalling Tivoli Provisioning Manager" on page 105.

The following considerations apply to a reinstallation:

- If you did not remove your database, application server, or directory server, these products will be discovered when you run the installer.
- If you did remove some of the prerequisite applications, ensure that they are completely removed. For more information, see "Remove items remaining after uninstallation" on page 108.
- If discovered prerequisite applications are still configured for Tivoli Provisioning Manager, you do not need to reinstall or reconfigure them with the installer in most cases.

  For DB2, however, you must select the **Configure** option in the installer during reinstallation. If the database from the previous installation still exists, you must also specify a new database name.

After you have checked all reinstallation considerations, you can run the installer to reinstall Tivoli Provisioning Manager.

Appendix C. Performing a silent installation

Silent installation provides you with the ability to predefine installation options in a template *response file*. You can then run the installation without being prompted to specify additional information. Silent installation is also useful for installing the same configuration on multiple computers.

A response file is an XML file with predefined settings for the installation. During a silent installation the installer reads the necessary input from the response file at run time while performing a silent installation.

You can run the installer in record mode to save your installation options, and then use the response file to perform the installation.

Creating a response file

To create the response file, you must run the installer in record mode. The installer saves your installation options instead of performing the installation.

1. Run the following command:

   `./install.sh -record filename`

   where *filename* is the full path and name of the response file.

   Additional parameters:

   The following optional parameters can be used to run the installer

   -locale

   The installer attempts to detect the language configured for the computer. If the locale cannot be detected correctly, use the command `install.sh -locale`. For example, if the locale is Japanese and you want to start the installer in Japanese, run the following command:

   `./install.sh -locale ja_JP`

   -tiLocation *directory*

   Specifies a different temporary directory for installer files. Use this option if the default user temporary directory does not have sufficient disk space or if you want to use an alternate user temporary directory.

2. When the installer starts, select the options that you want to use for the installation.

The response file is created with the specified file name. If you ran the installer on Windows, a response file for a UNIX® installation is also created with the specified file name and a `.unix` extension. You can use the appropriate response file to perform the installation.

Important: If you need to change values in the response file, run the installer in record mode again and create a new response file. Some values in the response file are not available from the installer interface because they cannot be changed. If you change these values directly in the response file, installation might fail.

Running a silent installation

After you have created the response file, you are ready to run the silent installation.

1. Log on as `root`.

   Note: If you are using the `su` command to change to root, ensure that you use `su -`. Note the hyphen after `su`.

2. If you preinstalled WebSphere Application Server, ensure that it is stopped.
   a. Change to the `bin` subdirectory of the WebSphere Application Server installation, the default is `/opt/IBM/WebSphere/AppServer/bin`.
   b. Run the command:

      `./stopServer.sh` *`app_server`* `-username` *`was_adminID`* `-password` *`password`*

      `app_server`
      The name of the application server. The default is `server1`.

      `was_adminID`
      The WebSphere Application Server administrator user name. After a new installation of Tivoli Provisioning Manager, the user name is `tioadmin`.

      `password`
      The WebSphere Application Server administrator password for the specified user name.

3. If you preinstalled the database, ensure that it is running.

   DB2

   To verify that DB2 is running:
   a. Switch to the DB2 instance owner. For a default installation, the Tivoli Provisioning Manager database owner is `tioadmin`. For a custom installation, the default Tivoli Provisioning Manager database owner is `db2inst1`.

      For example, if the instance owner is `db2inst1`, run the command.

      ```
      su - db2inst1
      ```

   b. Run the command to start DB2:

      ```
      db2start
      ```

      DB2 is started if it is not running already. If DB2 is already running, the following message is displayed.

      ```
      SQL1026N  The database manager is already active
      ```

4. Start the installation with the following commands at the command prompt. Replace the variable *`file_name`* with the file name.

   Note: Provide the fully qualified path of the directory in which the file is located.

   `./install.sh -silent` *`filename`*

   where *`filename`* is the full path and name of the response file.

5. The installer begins to install all the options that were selected in the response file. This will take a few minutes. The cursor will keep blinking on the command prompt. This indicates that the installation is in progress. The command prompt is displayed again. The Tivoli Provisioning Manager has now been installed successfully.
6. Restart the Tivoli Provisioning Manager server.
7. After installation, see the log files to determine if the silent installation was successful.

- The main installation logs are located in the directory `/tmp/tclog_TI_timestamp`, where *timestamp* is the creation date and time of the directory. For recovery information and information about other log files, see "Recovery first steps" on page 75.
- If you encountered an error during installation.
  - See "Silent installation exit codes" for a description of silent installation exit codes.
  - See Chapter 6, "Recovering from installation errors," on page 75 for other recovery information.

8. Installation of the product is now complete. Before you begin using the product, some additional steps are required.
   - See Chapter 4, "Verifying installation," on page 53 to verify your installation.
   - Some product configuration is required after the product is installed. See Chapter 5, "Post-installation configuration," on page 63 for information about required and recommended post-installation tasks.

Silent installation exit codes

The following tables describe installation exit codes for a silent installation.

Table 37. Exit codes for the database server

Error code	Description
201	Invalid number of arguments
205	DB2 profile not found
206	Error sourcing-in DB2 profile
210	Cannot connect to database server. Ensure that DB2 is running. This error might be due to factors such as an invalid port number, incorrect user name or password, or an incorrect host name or IP address.
211	Cannot connect to database. Ensure that DB2 is running. This error might be due to factors such an incorrect user name or password or an incorrect database name.
212	Import Failed
213	Export failed
214	Create database table failed
215	Database user does not have sufficient permissions (not used)
216	Bind Failed (not used)
217	Failed to drop table
218	Failed to drop database
220	DB2 configuration failed
225	DB2 unconfiguration failed
230	DB2 client not found

Table 38. Exit codes for WebSphere Application Server

Error code	Description
120	Unable to configure WebSphere Application Server (trouble running `was_config.jacl`).
121	Unable to unconfigure WebSphere Application Server (trouble running `was_unconfig.jacl`).
122	Unexpected error when configuring WebSphere Application Server properties files.
130	Failed to enable security for WebSphere Application Server.

Table 38. Exit codes for WebSphere Application Server (continued)

Error code	Description
131	Failed to disable security for WebSphere Application Server.
140	Failed to deploy application for WebSphere Application Server.
141	Failed to undeploy application for WebSphere Application Server.
145	Incorrect WebSphere Application Server installation directory.
147	WebSphere Application Server security is on.
148	WebSphere Application Server failed to start.
149	WebSphere Application Server check for ports failed.
150	Unexpected MQ error (71 or 20 return code from MQ control commands, other MQ errors should not happen)
160	WebSphere Application Server incorrect version or not installed.

Table 39. Exit codes for core components

Error code	Description
155	Failed to install agent manager
156	Failed to uninstall agent manager

Table 40. Other exit codes

Error code	Description
110	Failed to install GUID
117	Bash location is not `/bin/bash`
118	Expect location is not `/usr/bin`
252	Installation user does not have root permissions
253	Tivoli Provisioning Manager is already installed.
254	Software downgrade
255	License downgrade

Appendix D. Preinstalling required software

Depending on the installation topology that you are using, you might need to preinstall some required software before you begin Tivoli Provisioning Manager installation.

Note: You cannot install any of the software listed below using a mapped network drive. Mapped network drives are not supported.

Table 41. Applications to preinstall

Application	Preinstallation required?	
WebSphere Application Server 6.0.2.11 (64-bit version only)	**No**	
DB2 Enterprise Server Edition 8.1, Fix Pack 11	**Yes**	Preinstallation is required if you want DB2 to be installed on a separate computer. You must preinstall the database server on the second computer and preinstall the database client on the Tivoli Provisioning Manager computer.
	No	Preinstallation is not required if you want DB2 installed on the Tivoli Provisioning Manager computer.

Refer the information in the following sections for details about preinstalling the software and performing any required configuration.

Preinstalling WebSphere Application Server

The following requirements apply to the installation. Refer to theWebSphere Application Server documentation for installation instructions.

1. WebSphere Application Server must be installed on the same computer as Tivoli Provisioning Manager.
2. The WebSphere Application Server cell name and node name must be in the format *hostname*`Node01Cell` and *hostname*`Node01` respectively, where *hostname* is the host name of theWebSphere Application Server computer.
3. Stop existing WebSphere Application Server profiles before you begin the installation. Stopping the profiles allow the agent manager to configure SSL on WebSphere Application Server. For more information, on stopping and starting the profiles, see the section, "WebSphere Application Server tasks" on page 144.
4. **Application server**. Tivoli Provisioning Manager can use a WebSphere Application Server installation with existing deployed applications in the default WebSphere Application Server profile.

Preinstalling DB2

You can preinstall DB2 on the Tivoli Provisioning Manager node or on a separate node. If you want to use DB2 on a separate node, it must be preinstalled. If you are using DB2 on the Tivoli Provisioning Manager node, you can preinstall the application or Tivoli Provisioning Manager can install it for you.

This section provides basic installation instructions for a typical installation of DB2. If you require more information, see the installation information in the DB2 information center at http://publib.boulder.ibm.com/infocenter/db2luw/v8/topic/com.ibm.db2.udb.doc/welcome.htm.

Use the DB2 installation media provided with Tivoli Provisioning Manager to ensure that you are using the correct version.

Note: A DB2 9.x database client is not compatible with the DB2 Enterprise Server Edition 8.1, Fix Pack 11 database server.

Installing the DB2 server

Prerequisites:

- Ensure that your system meets installation, memory, and disk requirements. For information about the DB2 requirements, and security issues to consider when installing DB2, see the DB2 documentation. The DB2 installer will automatically calculate required disk space and determine if you have sufficient space. Also ensure that you allocate sufficient disk space for growth of the database. For more information, see "Disk space for database growth" on page 18.
- You must have root authority to perform the installation.
- The DB2 Setup wizard is a graphical installer. You must have X window software capable of rendering a graphical user interface for the DB2 Setup wizard to run on your machine.
- Ensure that Asynchronous I/O (AIO) has been enabled. It must be enabled before DB2 can be successfully installed. To use AIO on Linux, you must install libaio-0.3.96 or later, have a kernel that supports AIO (for example, version 2.6).

To install the DB2 server:

1. Log on as `root`.
2. If you are using CDs, find the correct DB2 CD for your language. Mount the CD-ROM, and then change to the directory where the CD-ROM is mounted by entering the following command:

   ```
   cd /cdrom
   ```

   where */cdrom* represents the mount point of the CD-ROM.
3. If you are using installation images, copy the archive file that starts with **DB2_ESE_V82FP11** to the directory you want to install DB2. Select the file for the language that you want to install. Extract the contents of the archive file.
4. Change to the folder that starts with the letters **ese** and type `./db2setup` to start the DB2 Setup wizard.
5. The IBM DB2 Setup Launchpad opens. From this window, review installation prerequisites and the release notes for the latest information and then proceed with the installation.
6. Click **Install Products**.
7. Select **DB2 UDB Enterprise Server Edition** and click **Next**.
8. In the Welcome screen, click **Next**.
9. Accept the licence agreement and click **Next**.
10. Accept the default value (**Typical**) and click **Next**.
11. Select the **Install DB2 UDB Enterprise Server Edition on this computer** check box and click **Next**.

12. Continue with the installation and use the default values suggested by the installer.
    - Specify the DB2 Administration Server user name and password.

      Note: Setup of the administration contact list is optional.
    - In the Instance setup window, select **Create a DB2 instance**. If prompted in the **Select how this instance will be used** panel, select **Single-partition instance**. A partitioned instance is not supported.
    - Accept the default fenced user name and specify a password. The fenced user is responsible for running fenced, user-defined functions, such as stored procedures.
    - For the DB2 tools catalog, select **Prepare the DB2 tools catalog on this computer**.
    - In the DB2 summary panel called **Start copying files**, review the settings for the installation. Consider copying these to a text file so that you can refer to them when you start Tivoli Provisioning Manager installation. Settings you will need for the database server include:
      – user names and passwords
      – group names
      – instance owner home directory
      – database name
      – DB2 server connection port
13. After the installation completes, a status page opens. Click the **Status report** tab to ensure your installation was successful.

Post-installation steps

1. Ensure that the `db2inst1` user is configured so that the user has unlimited file system and memory resources available. The user limits are validated by the preinstallation script. For details about requirements, see "User limits" on page 20.
2. Log on as the instance owner.

   For example, if the instance owner is `db2inst1`, run the following command from the `root` account:

   ```
   su - db2inst1
   ```
3. Ensure that the DB2 database installation directory matches the database instance owner home directory.
4. Stop and then restart DB2:

   ```
   db2stop
   db2start
   ```
5. Run the following commands:

   ```
   db2set DB2COMM=TCPIP
   db2set DB2BQTRY=120
   db2set DB2BQTIME=2
   db2set DB2AUTOSTART=YES
   ```
6. Stop and then restart DB2:

   ```
   db2stop
   db2start
   ```
7. Verify that the database instance is listening on the DB2 connection port. The default port number is `50001`.

   Use the following command to check the port status.

   ```
   netstat -a | grep port
   ```

where *port* is the DB2 port number.

A list of connections and listening ports is displayed. Ensure that the DB2 connection port is displayed. You can also check the port in the DB2 Control Center.

a. Start the DB2 Control Center. **Start** > **Programs** > **IBM DB2** > **General Administration Tools** > **Control Center**.
b. Navigate to the DB2 instance.
c. Right-click the instance and click **Setup Communications**.
d. Click **Properties** for the TCP/IP protocol to check the port.

Installing the DB2 client

If you are using DB2 on a separate node, the DB2 client must be preinstalled on the Tivoli Provisioning Manager computer. During Tivoli Provisioning Manager installation, the database client is used to connect to the DB2 server and configure it for use with Tivoli Provisioning Manager.

1. Log on as `root`.
2. If you are using CDs, mount the CD-ROM, and then change to the directory where the CD-ROM is mounted by entering the following command:

   ```
   cd /cdrom
   ```

   where */cdrom* represents the mount point of the CD-ROM.
3. If you are using images, copy the archive file that starts with **DB2_ADMCL_V82FP11** to the directory you want to install DB2.
4. Change to the folder that starts with the letters **admcl** and type `./db2setup` to start the DB2 Setup wizard.
5. The IBM DB2 Setup Launchpad opens. From this window, review installation prerequisites and the release notes for the latest information and then proceed with the installation.
6. Click **Install Products**.
7. Select **DB2 Administration Client** and click **Next**.
8. In the Welcome screen, click **Next**.
9. Accept the licence agreement and click **Next**.
10. Accept the default value (**Typical**) and click **Next**.
11. Select **Create a DB2 instance**.
12. Specify the DB2 instance owner. If you created the user manually, specify the user name that you created. If you did not create the user manually, the installer will create it for you.

    For example, specify `db2inst1` for the database owner and `db2grp1` as the user's primary group.

    Note:

    - The DB2 user name and password must match the instance owner name and password on the DB2 server.
    - Ensure that the database client directory is the `sqllib` directory under the instance owner home directory. For example, if the home directory is `/home/db2inst1`, then the client location is `/home/db2inst1/sqllib`,
13. Accept the default values for the remaining panels.
14. On the summary panel, review your settings. Note the following information:
    - Name of the database instance owner

- The group name for the database instance owner
- The DB2 client installation directory.

You will need this information for Tivoli Provisioning Manager installation.

15. Click **Finish** to start the installation.

Appendix E. Installing the directory server

If you want to use a read-only directory server, you must install it before you configure Tivoli Provisioning Manager to use the directory server.

Installing and configuring Tivoli Directory Server

This chapter provides instructions to install Tivoli Directory Server and then configure a sample instance with the users required by Tivoli Provisioning Manager. If you are not familiar with installing and configuring a directory server, you can use the sample instance and sample users to set up a test directory server.

After you have set up Tivoli Directory Server, you must follow the steps in "Configuring a read-only directory server" on page 63 to set it up as a read-only directory server for Tivoli Provisioning Manager.

Requirements

- Tivoli Directory Server must be installed on a separate computer.
- Tivoli Directory Server Version 6.1 is the required version. The installation media is provided with Tivoli Provisioning Manager.
- Create an operating system user that will own the database instance for the directory server.

  For the instructions for the sample instance, the group name **idsldap** and user name **ldapinst** are used.

  1. Log on as a user with `root` privileges.
  2. Create the group with the command:

     ```
     groupadd idsldap
     ```
  3. Create the database instance owner and add the user to the group.

     ```
     useradd -g idsldap -d /home/ldapinst -m -s /bin/ksh ldapinst
     ```
  4. Set the user password for the ldapinst user.

     ```
     passwd ldapinst
     ```
  5. Verify that you can log on with the user name and password before continuing.
  6. Add the root user to the group idsldap with the following commands:

     ```
     usermod -G idsldap,root_secondary_group root
     ```

     Replace *root_secondary_group* with any other secondary groups for the root user. You can obtain a list of groups for the root user with the command `groups root`.

Operating system requirements

This section summarizes operating system requirements. For details, see the Tivoli Directory Server information center for details http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc_6.0/install.htm.

For the client:

Memory
A minimum of 128 MB RAM is required. For better results, use 256 MB or more.

For the server:

These recommendations are based on a directory with 100,000 inetOrgPerson objects, where each entry is approximately 10 KB. Requirements will vary based on your directory and performance responsiveness requirements:

Memory

The following amounts of RAM are recommended for each directory server instance:

- At least 512 MB for each directory server instance. This includes both proxy servers and full servers.
- At least 256 MB for each database instance. (This is not required for a proxy server.)
- At least 256 MB for running the Web Administration Tool and the embedded version of WebSphere Application Server - Express on the same computer.

Add these memory requirements together if you have a full server, the Web Administration Tool, and the embedded version of WebSphere Application Server - Express on the same computer.

Disk space

For a full server, Tivoli Directory Server (including the client, the server, and the database) requires about 2 GB of disk space. This might increase based on the number of entries and the size of each entry for your installation.

Be sure that you have at least 100 MB of free space in the /var directory and one of the following:

- At least 100 MB in the /tmp directory (or the directory you want to use as a temporary directory) if installing only the client
- At least 400 MB in the /tmp directory (or the directory you want to use as a temporary directory) if installing a server

Packages

- The Korn shell is required.
- GSKit 7.0.3.3 is provided and is the only supported version of GSKit.

DB2 requirements

Before you run the command to install Tivoli Directory Server, a supported version of DB2 must be installed. for a list of supported versions, see the section for your operating system in the Tivoli Directory Server information center: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc_6.0/install.htm.

If you want to use the version of DB2 provided with Tivoli Directory Server, you must use the **db2_install** utility to install it. (If you do not use this utility, the DB2 license file is not added correctly.) The db2_install utility is in the db2 directory of the Tivoli Directory Server installation media.

Notes:

1. The db2_install utility can install only in a C or en_US locale. If you are installing on a computer with a different locale, set the locale in a shell to C or en_US before you use the db2_install utility.
2. After you start the db2_install utility, you are prompted for a keyword. In response to this prompt, type DB2.ESE.
3. After you install DB2, you can check the following two files to verify that the installation was successful:
   - /tmp/db2_install.rc.99999
   - /tmp/db2_instal_log.99999

   99999 is a random number associated with the installation.

Ensure that you meeting requirements for the version of DB2 that you are using with Tivoli Directory Server. See the DB2 information center for details: http://publib.boulder.ibm.com/infocenter/db2luw/v8/topic/com.ibm.db2.udb.doc/welcome.htm

Java runtime environment

You must have the Java runtime environment 1.4.2 installed. It is provided in the `/java` subdirectory of the Tivoli Directory Server installation media.

Additional requirements

See the requirements information in the Tivoli Directory Server for additional requirements that apply to your operating system. http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc_6.0/install12.htm

Installing Tivoli Directory Server

To install IBM Tivoli Directory Server 6.1:

1. Log in as **root**.
2. Mount the CD that contains the Tivoli Directory Server files.
   a. Log in as a user with root authority.
   b. Insert the disk and mount the CD-ROM drive.
3. Copy the file to a temporary directory.
4. At a command prompt, untar the tar file using the tar –xvf *package name*.
5. Change directory to tdsV6.1/tds and run ./install_tds.sh
6. Select the language you want to use during IBM Tivoli Directory Server installation. Click **OK**.
7. On the Welcome window, click **Next**.
8. After reading the Software license, select **I accept the terms in the license agreement**. Click **Next**.
9. Any preinstalled components and corresponding version levels are displayed. Click **Next**.
10. In the installation type, select **Typical**. Click **Next**.
11. A window opens with the following components:
    - Client SDK
    - Java Client
    - Web Administration Tool

- Proxy Server
- Server
- Embedded version of WebSphere Application Server - Express
- DB2
- GSKit

The components that are not yet installed are preselected. This window also indicates the amount of disk space required and available. Verify that the components you want to install are selected, and click **Next**. A summary panel displays the components you selected and the locations where the selected components will be installed.

12. Click **Back** to change any of your selections. Click **Install** to begin the installation.
13. By default, links are set automatically for client and server utilities. However, in case of a conflict, a window opens asking if you want to override the previous links. In such a case, if you want the installation program to override the links, click **Yes**.
14. When the completion window is displayed, click **Finish**. When prompted to, type in a new password and confirm it. After the installation is complete, the Instance Administration Tool automatically runs. Click **Cancel** to close the tool.

Configuring Tivoli Directory Server

You must create a database instance for Tivoli Directory Server. You can then configure the LDAP suffix for the Tivoli Provisioning Manager users and import the sample users

Creating a directory server instance

1. Log on as `root`.
2. Change to the `sbin` subdirectory in the Tivoli Directory Server installation directory. For example, `/opt/ibm/ldap/V6.0/sbin`.
3. Create a new instance:

   ```
   idsicrt -I ldapinst –p 389 –s 636 –e mysecretkey! -l /home/ldapinst
   ```

   where *mysecretkey!* is a string of characters that will be used as an encryption seed. The encryption seed must contain only printable ISO-8859-1 ASCII characters with values in the range of 33 to 126, and must be a minimum of 12 and a maximum of 1016 characters in length. This encryption seed is used to generate a set of Advanced Encryption Standard (AES) secret key values. These values are stored in a directory key stash file for the directory server instance, and are used to encrypt and decrypt directory stored password and secret key attributes.
4. Configure the primary administrator DN:

   ```
   idsdnpw -I ldapinst -u cn=root -p password
   ```

   where *password* is the password for the `cn=root`.
5. Configure the database:

   ```
   idscfgdb -I ldapinst -a ldapinst -w password -t ldapdb -l /home/ldapinst
   ```

   where *password* is the password for the user `ldapinst`.

Configuring the LDAP suffix and importing data

The LDAP suffix, or base DN, defines the location where the user information is held.

All of the Tivoli Provisioning Manager data resides in a suffix. The default value for Tivoli Provisioning Manager is `dc=ibm,dc=com`.

There are three required users for Tivoli Provisioning Manager. The following users are configured in the sample data that you will import:

wasadmin
The WebSphere Application Server administrator user. This user will replace `tioadmin` as the WebSphere Application Server administrator when you configure Tivoli Provisioning Manager to use the directory server.

tioldap
This user is the entry owner of the Tivoli Provisioning Manager LDAP suffix. An entry owner has all of the required permissions to the data under the domain that they are the owner of. For Tivoli Provisioning Manager, tioldap is the owner of the domain `dc=ibm,dc=com`. When the user logs in as tioldap, they can create, delete, and edit the existing data in that domain.

tioappadmin
The administrator for the Tivoli Provisioning Manager Web interface. This user will replace the currently configured Web interface administrator. The default user name after a fresh installation is `admin`.

For the sample data, the passwords for each user are the same as the user name.

1. Log in as root, as the directory server instance owner, or with a user ID that is in the primary group of the directory server instance owner.
2. Start the Tivoli Directory Server Configuration Tool at a command prompt with the following command:
   ```
   idsxcfg
   ```
3. Configure the base DN.
   a. Click **Manage Suffixes** in the navigation pane.
   b. In the Suffixes pane, type the base DN. For the sample instance, use `dc=ibm,dc=com`. This is the base DN that is used in the example data that you will import.
   c. Click **Add** and then click **OK**.
4. Change to the `sbin` subdirectory in the Tivoli Directory Server installation directory. For example, `/opt/ibm/ldap/V6.0/sbin`.
5. Start the directory server database instance. At the command prompt run the following command:
   ```
   idsslapd -I instance_name
   ```
   Replace *instance_name* with the instance name. For example,
   ```
   idsslapd -I ldapinst
   ```

   Note:

   If you receive the following error message, you might have a problem with your electronic DB2 license.

```
GLPCTL010E Failed to start database manager for database instance: <instance_name>.
```

   To check your license, run the command `db2start`. If your license is correct, you see the message:
   ```
   SQL1063N DB2START processing was successful.
   ```

Otherwise, you see a message indicating that your license has expired or will expire in some number of days.

To upgrade your DB2 product from a demonstration license to a product license:

a. Log on as `ldapinst`.
b. Copy the license file from the DB2 CD to the system where DB2 is installed. You do not need to reinstall DB2. The file is located in:

   path`/itdsv60/db2/license/ldap-custom-db2ese.lic`

   where *path* is the location where you extracted the Tivoli Directory Server installation media. Your Proof of Entitlement and License Information booklets identify the products for which you are licensed.
c. After you have a valid license file on the system, run the following command to activate the license:

   `db2licm -a` *license_filename*
d. Log on as root. You can now start the database instance.

6. Extract the contents of Tivoli Provisioning Manager Disk 2 to a temporary directory. In these instructions, the directory `/tmp/disk2` is used.
7. Change to the `/tmp/disk2/tools/ldap` directory.
8. Import the database schema. At the command prompt, run the following command to import the LDAP schema:

   install_dir`/bin/ldapmodify -a -h` *fqdn* `-D cn=root -w` *password* `-i schema.ldif`

   install_dir
   The full path of the Tivoli Directory Server installation directory.

   fqdn The fully-qualified domain name of the computer. For example, `idsserver.example.com`

   password
   The password that you set during installation for `cn=root`, the administrator DN.
9. Import the sample data with the following command:

   install_dir`/bin/ldapmodify -a -h` *fqdn* `-D cn=root -w` *password* `-i ldap.ldif`
10. When the data is imported, you must provide the passwords for the imported users. For each of the three sample users, the password is the same as the user name. The passwords are encrypted in `ldap.ldif`, but you must provide them in plain text.

Note: If you want to see the details for the users that are imported, open the file `/tmp/tpmdisk2/tools/ldap/ldap.ldif` and find the heading that starts with `## Users`. It is the last section of the file.

Appendix F. Manually configuring read-only LDAP

In some situations, it might be necessary to configure the LDAP server manually instead of using the read-only LDAP script. To perform the manual configuration, you must complete the following steps:

1. "Disable WebSphere Application Server security settings"
2. "Configure WebSphere Application Server to use custom user registry"
3. "Replace the user-factory.xml file" on page 130
4. "Restart Tivoli Provisioning Manager" on page 132
5. "Enable WebSphere Application Server security" on page 132
6. "Import the Tivoli Provisioning Manager administrator user" on page 132
7. "Update user password information" on page 132

Disable WebSphere Application Server security settings

1. Ensure that Tivoli Provisioning Manager is running.
2. Log on to the WebSphere Application Server administrative console at the following URL

   `http://hostname:port/admin`

   Where *hostname* is the host name and *port* is the WebSphere Application Server Admin host port that was defined during installation.
3. Log on as the WebSphere Application Server administrator user ID `tioadmin`.
4. Select **Security > Global Security**.
5. Disable security by clearing **Enable Global Security**.
6. Save your changes and restart Tivoli Provisioning Manager.

Configure WebSphere Application Server to use custom user registry

A custom user registry is a customer-implemented user registry that authenticates a user and retrieves information about users and groups to perform security-related functions, including authentication and authorization. For details about creating a custom user registry, see the WebSphere Application Server documentation at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r0/topic/com.ibm.websphere.base.doc/info/aes/ae/xsec_customuser.html. For information about the provided samples, see "Read-only LDAP sample information" on page 128.

To configure WebSphere Application Server to globally use the custom user registry:

1. Click **Security > Global Security > Active User Registry** and select **Custom User Registry**.
2. Click **Security > Global Security > User Registry > Custom** and enter the following information:
   - **Server User ID**: Enter a new user name. This user name is used in the custom user registry for accessing WebSphere Application Server.
   - **Server User Password**: Enter a new password for accessing WebSphere Application Server.

- **Custom Registry Class Name**: Enter the custom user registry class implementation name. In the provided custom user registry sample, the class name is

  Tivoli Directory Server:

  com.ibm.tivoli.websphere.customSecurity.sample.IDSCurImplementation
- **Ignore Case for Authorization**: Ensure that this option is selected.

3. Save your changes and restart Tivoli Provisioning Manager.

Read-only LDAP sample information

The read-only Lightweight Directory Access Protocol (LDAP) documentation provides samples for Tivoli Directory Server and Microsoft Active Directory. Integration with Microsoft Active Directory is only supported with a provisioning server on Windows. The sample supports various functions, including multiple LDAP registries, external role mapping to Tivoli Provisioning Manager internal roles, custom user filer, and custom user login attributes.

Read-only LDAP support consists of the following functions:

External role mapping
: You will generally have your own external security roles defined in your LDAP registry. Tivoli Provisioning Manager supports mapping these external roles in to the Tivoli Provisioning Manager internal roles.

Custom user filter
: A user can specify their own filter to find the Tivoli Provisioning Manager user. So, users can be from different objectclasses. Tivoli Provisioning Manager does not require users to be of specific objectclasses defined by Tivoli Provisioning Manager.

Custom user login attribute
: Users can specify their own attributes for user login to Tivoli Provisioning Manager

Tivoli Directory Server sample

The configuration settings are specified in the `user-factory.xml` file. This is a sample `user-factory.xml` file:

```
<?xml version="1.0"?>

<user-database>
    <ws-security>false</ws-security>
    <custom-user-registry>com.ibm.tivoli.tpm.cur.IDSWriteAndTPMRoles</custom-user-registry>
    <user-factory>com.ibm.tivoli.tpm.userAndRoleFactory.UserAndDBGroupFactory</user-factory>
    <authentication-realm>com.ibm.tivoli.tpm.security.realm.authentication.FakeSecurityRealm
</authentication-realm>


    <read-only>LDAP</read-only>
    <update-password>true</update-password>
    <ldapRegistries>
        <ldapRegistry>
                <initial-context-factory>com.sun.jndi.ldap.LdapCtxFactory</initial-context-factory>
                <server>hikari.torolab.ibm.com</server>
                <ldap-port>389</ldap-port>
                <ldaps-port>636</ldaps-port>
                <ssl-for-binding>false</ssl-for-binding>
                <baseDN>dc=ibm,dc=com</baseDN>
                <subtree></subtree>
                <bindingUserName>tioldap</bindingUserName>
                <bindingPassword>wJgxYQRYgak=</bindingPassword>
                <userSecurityName>cn</userSecurityName>
```

```
                <userUniqueId>dn</userUniqueId>
                <userDisplayNameAttr>cn</userDisplayNameAttr>
                    <userFilter>(&amp;(cn=%v)(objectclass=organizationalPerson))</userFilter>
                <groupS>cn</groupSecurityName>
                <groupUniqueId>dn</groupUniqueId>
                <groupDisplayNameAttr>cn</groupDisplayNameAttr>
               <groupFilter>(&amp;(cn=%v)(|(objectclass=groupOfURLs)(|(objectclass=groupOfNames)
(objectclass=groupOfUniqueNames))))</groupFilter>
                <groupMember>ibm-allGroups</groupMember>
                <userMember>ibm-allMembers</userMember>

        </ldapRegistry>
    </ldapRegistries>
</user-database>
```

The information that is required for the Tivoli Directory Server read-only LDAP sample implementation is specified in the `ldapRegistries` element in the `user-factory.xml` file. The following tables provide the information on how the `ldapRegistry` is constructed and configured for Tivoli Directory Server support:

Table 42. General LDAP server configuration

Attribute	Description
`initial-context-factory`	Specifies the initial context factory to be used for the Java Naming and Directory Interface (JNDI). It should have the value `com.sun.jndi.ldap.LdapCtxFactory`.
`server`	The hostname of the Tivoli Directory Server. It should be a fully qualified hostname.
`ldap-port`	The non-secure socket layer (SSL) port for the LDAP protocol. This port is usually 389.
`ldaps-port`	The SSL port for the LDAP protocol. This port is usually 636.
`ssl-for-binding`	Specifies if the SSL is used for communication between Tivoli Provisioning Manager and Tivoli Directory Server. Additional configuration is required when you use the LDAPs protocol. Refer to the related documentation for how the LDAPs is enabled in the Tivoli Directory Server.
`baseDN`	The base DN that Tivoli Provisioning Manager will search for in the user and group information. In Tivoli Directory Server, the base DN could be the suffix that the user and group information resides in.
`subtree`	An additional way to specify the name of the context or object to search. For example, if the user information resides in an `OU-TIO` under the suffix specified in the `baseDN` element, you can specify `OU=TIO` under `subtree` to refine the search to the organization unit, `TIO`.
`bindingUserName`	The user name that is used to bind to Tivoli Directory Server.
`bindingPassword`	The encrypted password that is used together with the `bindingUserName` to bind to Tivoli Directory Server.

Table 43. User specific LDAP server configuration information

Attribute	Description
`userSecurityName`	This is used for user authentication and authorization in WebSphere Application Server. The value of the attribute in Tivoli Directory Server is used to validate the user login name when accessing Tivoli Provisioning Manager.
`userUniqueId`	The unique identifier for the user. The value has to be unique across all registered Tivoli Directory Server directories. It usually has a value of `dn`.
`userDisplayNameAttr`	This is used to specify the attribute to store the display name of the user that is shown in the Web interface.
`userFilter`	This filter is used for searching for the user in the registry. It should contain information such as the `objectclass` that the user belongs to. For example, `(&(cn=%v)(objectclass=organizationalPerson)` . The parameter `%v` is necessary because during the search, the `%v` will be replaced with real user name.

Table 44. Group specific LDAP server configuration information

Attribute	Description
`groupSecurityName`	This attribute is returned from a group search.
`groupUniqueId`	The unique identifier for the group. The value has to be unique across all registered Tivoli Directory Server directories. It usually has a value of `dn`.
`groupDisplayNameAttr`	This is used to specify the attribute to store the display name of the group that is shown in the Web interface.
`groupFilter`	This filter searches for the group in the registry.
`groupMember`	This attribute returns a set of groups, including ancestor groups, to which a user has member. In Tivoli Directory Server it should be `ibm-allGroups`.
`userMember`	This attribute returns a set of group membership, including static, dynamic, and nested group members as described by the nested group hierarchy. In Tivoli Directory Server, the `ibm-allMembers` attribute should be used.

These attributes show one instance of Tivoli Directory Server user registry. Multiple registries can be defined and registered in multiple `ldapRegistry` elements in the in the `user-factory.xml` file.

The search for a user is completed sequentially according to the order of the LDAP registries being registered file. If the first LDAP registry does not find the user, it will go to the next LDAP registry in the list and continue until either the user is found or the end of the list is reached.

Replace the user-factory.xml file

A user-factory.xml file is provided for each custom user registry sample:

Tivoli Directory Server: user-factory-ids-readOnlyLdap.xml

The read-only LDAP user-factory.xml contains the following important configuration items:

custom-user-registry:

This is the implementation class of the custom user registry. The class has to implement the interface UserRegistry provided by WebSphere Application Server. Tivoli Provisioning Manager provides the following sample:

Tivoli Directory Server
com.ibm.tivoli.websphere.customSecurity.sample.IDSCurImplementation

authentication-realm:

This configuration item is used for Web service authentication. This class is responsible for authenticating credentials against a user repository. There are different security realm implementations for different user repositories

- Tivoli Directory Server
- The operating system.

You can also define your own.

The authentication realm must match the implementation class of the interface BaseSecurityRealm in the package com.ibm.tivoli.tpm.security.realm.authentication.

If you are configuring a custom user registry for read-only LDAP, the user-factory.xml should use the following as the value for the authentication-realm: com.ibm.tivoli.tpm.security.realm.authentication.CustomLdapRegistryRealm

The complete set of possible values for the authentication-realm are:

- com.ibm.tivoli.tpm.security.realm.authentication.CustomLdapRegistryRealm: Use for read-only LDAP with a custom user registry.
- com.ibm.tivoli.tpm.security.realm.authentication.OSSecurityRealm: Use if the users are at the operating system level and you want to authenticate against the operating system user.
- com.ibm.tivoli.tpm.security.realm.authentication.ActiveDirectorySecurityRealm: Use if you are authenticating against users in Microsoft Active Directory

  Note: Microsoft Active Directory is only supported for Tivoli Provisioning Manager installations on Windows.
- com.ibm.tivoli.tpm.security.realm.authentication.IBMDSSecurityRealm: Use to authenticate against users in Tivoli Directory Server.
- com.ibm.tivoli.tpm.security.realm.authentication.CustomLdapRegistryRealm: Usually reserved for testing only. It is hardcoded to authenticate to the username/password: tioappadmin/tioappadmin.

To replace the user-factory.xml:

1. In the *$TIO_HOME*/config directory, rename the file that you are using to user-factory.xml.

   If you have created your own custom user registry, a user-factory.xml file is still required, however, use only the following section from the file:

```
<?xml version="1.0"?>

<!-- User database setup -->
<user-database>
  <ws-security>true</ws-security>
  <custom-user-registry>com.ibm.tivoli.websphere.customSecurity.sample.IDSCurImplementation
</custom-user-registry>
  <user-factory>com.ibm.tivoli.tpm.userAndRoleFactory.IDSReadOnlyUserAndDBGroupFactory
</user-factory>
  <authentication-realm>com.ibm.tivoli.tpm.security.realm.authentication.CustomLdapRegistryRealm
</authentication-realm>

  <read-only>true</read-only>
  <update-password>true</update-password>
</user-database>
```

Figure 17. Tivoli Directory Server

2. When you prepare your user-factory.xml file you might need to encrypt the user password. To encrypt the user password, change to the *$TIO_HOME*/tools directory and run the following command at a command prompt:

   ```
   encrypt.cmd <plain_password_text>
   encrypt.sh <plain_password_text>
   ```

Restart Tivoli Provisioning Manager

Stop and then restart Tivoli Provisioning Manager. For instructions on starting and stopping Tivoli Provisioning Manager, see "Starting and stopping Tivoli Provisioning Manager" on page 53.

Enable WebSphere Application Server security

After all the configuration settings are changed, you can re-enable the WebSphere Application Server security settings.

1. Navigate to **Security > Global Security > Enable Global Security**
2. Select **Enable Global Security** and clear **Enforce Java 2 Security**.
3. Save your changes.
4. Stop and then restart Tivoli Provisioning Manager. For instructions on starting and stopping Tivoli Provisioning Manager, see "Starting and stopping Tivoli Provisioning Manager" on page 53.

Import the Tivoli Provisioning Manager administrator user

Import the Tivoli Provisioning Manager administrator user by following the instructions in "Importing LDAP users" on page 68.

Update user password information

Perform the following steps to ensure that administrator passwords are updated in all required locations:

1. Update DB2 Alphablox:
   a. Change to the *$TIO_HOME*/db2alphablox/repository/servers/AlphabloxAnalytics directory.
   b. In the Server.properties file, locate the line that starts with:

      ```
      ws.admin.username=
      ```

Change the value to the new WebSphere Application Server administrator user name.

c. locate the line that starts with:

```
ws.admin.password.protected=
```

Change the value to the password for the WebSphere Application Server administrator in plain text.

2. Grant the new Tivoli Provisioning Manager administrator with privileges to log on to the dynamic content delivery management center administration console:
   a. Change to the *$TIO_HOME*/tools/postinstall\ directory.
   b. Run the following command:

```
changeCDSAdminUserName.sh username CDSSCHEMA cdsschema_pwd
```

username
The Tivoli Provisioning Manager administrator user name.

3. Update dynamic content delivery management center repository service access point with new Tivoli Provisioning Manager administrator user name and password.
4. Start Tivoli Provisioning Manager. For instructions, see "Starting Tivoli Provisioning Manager" on page 53.
5. Add the **Alphablox** administrator role to the new WebSphere Application Server user.
   a. Log on to the WebSphere Application Server console with the new administrator user name and password.
   b. Click **Enterprise Applications > AlphabloxPlatform > Map security roles to users/groups**.
   c. Select the **AlphabloxAdministrator** role, then click **Look up users**.
   d. Click **Search**.
   e. In the **Available** list, find the new administrator user name and move it to the **Selected** list.
   f. Save your changes.
6. Encrypt the WebSphere Application Server administrator password:
   a. In a Web browser, open the DB2 Alphablox console:

```
https://hostname:9045/AlphabloxAdmin/home/
```

where *hostname* is the host name of the computer where WebSphere Application Server is installed.

   b. Log on with the new WebSphere Application Server administrator password.
   c. In the console, click **Alphablox Admin Pages** > **Administration** > **General** > **System**.
   d. Change **Message History Size** from 100 to 101 and save the change. Alphablox automatically encrypts the password in the `Server.properties` file.

Appendix G. Common tasks for Tivoli Provisioning Manager installation

The following sections describe how to perform some common tasks in applications that support Tivoli Provisioning Manager.

Creating users and groups

If you are unfamiliar with creating users and groups, use the information in this appendix to learn the basic commands for creating required users and groups. For more detailed instructions, see your operating system documentation.

Creating a group

Create a group with the command:

`groupadd group_name`

Example::

To create a group called `tivoli`, run the following command:

```
groupadd tivoli
```

Creating a user

The command to create a user can also create the home directory for the user, assign the user to groups, and set the default shell. To create a user, run the following command:

```
useradd -g primary_group -G group1,group2,... -d /home/user_name -m -s shell user_name
```

primary_group
The name of the primary group for the user.

group1,group2,...
The names of secondary groups for the user. If there is more than one group, separate the group names with commas.

user_name
The user name that you are creating.

shell The path to the default shell program for the user. For the Bash shell, the location is `/bin/bash`.

Examples:

The following table shows some example commands for creating users.

Table 45. Example user creation commands

User	Groups and shell	Command
tioadmin	**Primary:** tioadmin **Secondary:** tivoli and db2grp1 **Shell:** Bash	`useradd -g tioadmin -G tivoli,db2grp1 -d /home/tioadmin -m -s /bin/bash tioadmin`
admin	No required groups **Shell:** Bash	`useradd -d /home/admin -m -s /bin/bash admin`
db2inst1	**Primary:** db2grp1 **Shell:** Bash	`useradd -g db2grp1 -d /home/db2inst1 -m -s /bin/bash db2inst1`

Setting user passwords

To set the user password run the following command:

```
passwd user_name
```

For example, to set the password for the user `tioadmin`, run the following command:

```
passwd tioadmin
```

Verify that you can log on with the user name and password before performing installation or configuration tasks that involve the user.

Other user commands

Table 46. Other user commands

Header	Header

Manual create a home directory	`mkdir -p /home/user_name`
	
	Example:
	
	The following example creates the directory `/home/tioadmin` for the user `tioadmin`.
	`mkdir -p /home/tioadmin`

Assign a home directory to a user	`usermod -d /home/user_name user_name`
	Example:
	The following example assigns the home directory `/home/tioadmin` to the user `tioadmin`.
	`usermod -d /home/tioadmin tioadmin`

Assign a user to a primary group	`usermod -g primary_group user_name`
	Example:
	The following example assigns sets `db2grp1` as the primary group for `db2inst1`.
	`usermod -g db2grp1 db2inst1`

Assign a user to secondary groups	`usermod -G group1,group2,... user_name`
	Example:
	The following example adds the user `tioadmin` to the groups `tivoli` and `db2grp1`. Group names are separated by a comma.
	`usermod -G tivoli,db2grp1 tioadmin`

Change the default shell	`usermod -s shell user_name`
	Example:
	The following example sets the Bash shell as the default shell for `tioadmin`.
	`usermod -s /bin/bash tioadmin`

Changing default passwords

After Tivoli Provisioning Manager installation, you can use the **changePassword** tool to change the password for administrator accounts associated withTivoli Provisioning Manager. You can only change a password for one user at a time.

Requirements::

- The environment variables are defined: *$WAS_HOME*, *$TIO_HOME*, and *$JAVA_HOME* (Java runtime environment installation directory). These variables are typically defined whenTivoli Provisioning Manager is installed.
- WebSphere Application Server is running.
- The **changePassword** tool only changes passwords stored in Tivoli Provisioning Manager. The following password changes must be performed separately.
  - If you are changing the password for the following operating system users, you must change the passwords in the operating system first before running **changePassword**.
    - `tioadmin`
    - The database instance owner. For a default installation, the Tivoli Provisioning Manager database owner is `tioadmin`. For a custom installation, the default Tivoli Provisioning Manager database owner is `db2inst1`.
  - If you configured a read-only directory server, you must run **changePassword** after making a change to the following administrator users:

- `tioadmin`
- The Tivoli Provisioning Manager administrator in the Web interface. The default is `admin`.
- The WebSphere Application Server administrator. After a new installation, the user name is `tioadmin`. If you configured a read-only directory server, use the password for the WebSphere Application Server administrator that is configured on the directory server.

To change a user password:

1. Log on as `tioadmin`.
2. Change to the *$TIO_HOME* directory.
3. Run the following command:

```
changePassword.sh -c component_name -n new_password -u wasadmin_user -p current_wasadmin_password
```

component_name
The component for the user whose password you want to change.

Table 47. Components for password change

Component	Description of the user
tioadmin	• The Tivoli Provisioning Manager system administrator • Defined is in the operating system • Used to log on to the operating system • Used to install Tivoli Provisioning Manager
admin	• The Tivoli Provisioning Manager administrator in the Web interface. • The default user name is `admin`.
database	• The database instance owner. • For a default installation, the DB2 database owner is `tioadmin`. For a custom installation, the default DB2 database owner is `db2inst1`.
wasadmin	• The WebSphere Application Server administrator. • After a new installation, the user name is `tioadmin`. If you configured a read-only directory server after installation, use the password for the WebSphere Application Server administrator that is configured on the directory server.
agent	• The user name that the common agent uses to register with the agent manager. • Defined during installation in Defined during installation in “Tivoli Provisioning Manager Components Configuration tab” on page 41 and stored in `agentmanager.xml`.
resourcemgr	• The user name that Tivoli Provisioning Manager uses to register with the agent manager • Defined during installation in Defined during installation in “Tivoli Provisioning Manager Components Configuration tab” on page 41 and stored in `agentmanager.xml`.
cdscli	• The management center administrator for logging on to the dynamic content delivery management center console. • Defined during installation in “Tivoli Provisioning Manager Components Configuration tab” on page 41.

new_password
The new password for the user.

wasadmin_user
The WebSphere Application Server administrator. After a new installation, the user name is `tioadmin`. If you configured a read-only

directory server after installation, use the password for theWebSphere Application Server administrator that is configured on the directory server.

current_wasadmin_password
The current password for the WebSphere Application Server administrator user.

Important: User passwords should be unique.

4. For all users except the Tivoli Provisioning Manager administrator in the Web interface (`admin`), you must restart Tivoli Provisioning Manager for changes to take effect.

   Important: Stopping and starting Tivoli Provisioning Manager requires you to enter the WebSphere Application Server administrator user name and password. If you have changed the WebSphere Application Server administrator password, stop WebSphere Application Server with the old password.

DB2 tasks

This section provides tips on running with DB2. For more information, see the DB2 documentation.

Checking the status of DB2

To verify that DB2 is running:

1. Switch to the DB2 instance owner. For a default installation, the Tivoli Provisioning Manager database owner is `tioadmin`. For a custom installation, the default Tivoli Provisioning Manager database owner is `db2inst1`.

   For example, if the instance owner is `db2inst1`, run the command.

   ```
   su - db2inst1
   ```

2. Run the command to start DB2:

   ```
   db2start
   ```

   DB2 is started if it is not running already. If DB2 is already running, the following message is displayed.

   ```
   SQL1026N  The database manager is already active
   ```

Starting DB2

To start a DB2 instance:

1. Log on as the instance owner. For a default installation, the DB2 database owner is `tioadmin`. For a custom installation, the default DB2 database owner is `db2inst1`.
2. Run the following command from the command line:

   ```
   db2start
   ```

Stopping DB2

To stop DB2:

1. Stop Tivoli Provisioning Manager. For instructions, see “Stopping Tivoli Provisioning Manager” on page 56.
2. Log on as the instance owner. For a default installation, the DB2 database owner is `tioadmin`. For a custom installation, the default DB2 database owner is `db2inst1`.

3. Display all applications and users that are connected to the specific database that you want to stop. To ensure that no vital or critical applications are running, list applications. You need SYSADM, SYSCTRL, or SYSMAINT authority for this.
4. Force all applications and users off the database. You require SYSADM or SYSCTRL authority to force users.
5. To stop the instance type using the command line, enter:

   ```
   db2stop
   ```

Note: The db2stop command can only be run at the server. No database connections are allowed when running this command; however, if there are any instance attachments, they are forced off before the instance is stopped.

Reorganizing DB2 tables

The performance of SQL statements that use indexes can be impaired after many updates, deletions, or insertions of data into the database. Generally, newly inserted rows cannot be placed in a physical sequence that is the same as the logical sequence defined by the index (unless you use clustered indexes). This means that the Database Manager must perform additional read operations to access the data, because logically sequential data might be on different physical data pages that are not sequential. This in turn causes the performance to deteriorate. Some data files in the DB2 database that Tivoli Provisioning Manager uses can grow significantly larger than any other data files. To determine if you need to reorganize your DB2 tables, follow this procedure:

1. Get database configuration information (see "Get database configuration information" on page 140).
2. Get a DB2 database report (see "Get a DB2 database report" on page 141).
3. Reclaim DB2 space and update statistics (see "Reclaim DB2 space and update statistics" on page 141).

Get database configuration information

To get database configuration information, follow this procedure:

1. Start the DB2 environment.

   From the command prompt, run the db2profile of your DB2 instance owner. For a default installation, the DB2 database owner is tioadmin. For a custom installation, the default DB2 database owner is db2inst1. The following example uses the user name db2inst1.

   ```
   $ . ~db2inst1/sqllib/db2profile
   ```

2. Issue the following command. This example uses the database name of **TIODB**. If you use a different database name, enter your database name.

   ```
   db2 get db cfg for TIODB
   ```

3. A list of your database configuration is displayed. Look for the value "Path to log files". The following example shows where the database files are located which is SQL000xx.

   ```
   Path to log files =C:\DB2\NODE0000\SQL000xx\SQLOGDIR\
   ```

4. Change the directory to C:\DB2\NODE0000\SQL000xx\TIODB1. Look at the directory listing of the files. If you see some files which are significantly larger than the rest, then you should continue with the following procedures (see "Get a DB2 database report" on page 141 and "Reclaim DB2 space and update statistics" on page 141).

Get a DB2 database report

To get a DB2 report, follow this procedure:

1. From the DB2 command window, connect to the database using the following command:

   ```
   db2 connect to <database_name> user <db2_admin> using
   <db2_admin_password>
   ```

   For example, if your database name is **TIODB**, your DB2 administrator user ID is `db2admin`, and your DB2 administrator user password is `db2adminpswd`, this is the command to use:

   ```
   db2 connect to TIODB user db2admin using db2adminpswd
   ```

2. From the same command window run the
3. Issue the following **reorgchk**. The command calculates statistics on the database to determine if tables need to be reorganized.

   ```
   db2 reorgchk
   ```

   Search for asterisks (*) in the REORG column of the report. This indicates that the table or index needs to be reorganized. For more information about how to read the output from the **reorgchk** command, see **reorgchk** command in DB2 information center. For more information about reorganizing tables, see ″Table reorganization″ in the DB2 information center.

Reclaim DB2 space and update statistics

To reclaim DB2 space and update statistics, follow this procedure:

1. From the DB2 command window, issue the **reorg** command on the problem tables:

   ```
   db2 reorg
   ```

   It might take time to reorganize large tables and indexes. Therefore, you should reorganize the tables when the system has low usage. You can specify a particular table to organize in the command.

   ```
   db2 reorg table table_name
   ```

   After the reorganization, the free space in fragmented data will be removed. The file size of the problem tables will be reduced. This can provide faster access to the data thereby improving performance.

2. Issue the **runstats** command on the problem tables:

   ```
   db2 runstats on table table_name
   ```

   You should issue the **runstats** command after you issue the **reorg** command. This will update the statistics for the table. It might take time to collect the statistics for a large table. The statistics from the **runstats** command can provide better information for better performance.

Configuring the DB2 database

Database log files are key to the operation of the database. The primary database log files are allocated upon database activation. If there are indicators of running out of log space, or insufficient secondary log space, it is recommended that you ensure the disk volume has sufficient space. In addition, you can increase the log configuration to ensure the primary log space allocation is sufficient. To achieve this, follow these steps:

1. Stop Tivoli Provisioning Manager. For more information, see the section “Stopping Tivoli Provisioning Manager” on page 56.
2. Start a DB2 environment.

From the command prompt, run the db2profile of your DB2 instance owner. For a default installation, the DB2 database owner is tioadmin. For a custom installation, the default DB2 database owner is db2inst1. The following example uses the db2inst1 user name:

```
$ . ~/db2inst1/sqllib/db2profile
```

3. Run the following commands. These examples use the default database name of TIODB. If your database name is different, use your database name.

```
db2 update db cfg for TIODB using LOGFILSIZ 10240
db2 update db cfg for TIODB using LOGPRIMARY 120
db2 update db cfg for TIODB using LOGSECOND 120
```

Note: You must disable all of the connections associated with the database. Then, the next connection will start using the new database configuration.

4. Restart Tivoli Provisioning Manager. For more information, see the section "Starting Tivoli Provisioning Manager" on page 53.

Managing the transaction logs

The database that is used by the manager has the database recovery option turned on by default. This allows the recovery of the database in case of a system crash. By turning the recovery option on, DB2 will generate transaction logs and save them in a DB2 system directory. Over time, these logs will grow in size. The recommended way to free up the space is to use the DB2 **userexit** function as described in the *DB2 Administration Guide*. Another way to free up the file system space is to move the inactive logs to another file system. This method is described below. To move the inactive logs to another file system, follow the steps below.

Follow these steps:

1. Start a DB2 environment.

   From the command prompt, run the db2profile of your DB2 instance owner. For a default installation, the DB2 database owner is tioadmin. For a custom installation, the default DB2 database owner is db2inst1. The following example uses the db2inst1 user name.

   ```
   $ . ~/db2inst1/sqllib/db2profile
   ```

2. Issue the following command. This example uses the database name of TIODB. If you use a different database name, use your database name.

   ```
   db2 get db cfg for TIODB
   ```

3. A list is displayed of your database configuration. Look for the values for **Path to log files** and **First active log file**. The **Path to log files** is where the log files are located. The **First active log file** indicates the current active log.

   The path will be: DB2/NODE0000/SQL000nn/SQLOGDIR/. You can move the files, S0000001.LOG to S0000013.LOG, to another file system or back up and remove the log files to free up the log space. (Do not move the active log file.)

Note: This method is provided to you as a quick way to manage your transaction logs. However, the recommended way to free up space is to use the DB2 **userexit** program.

Dropping a DB2 database

To drop a DB2 database (**TIODB**), follow these steps:

1. Open a DB2 command window.
2. Enter this command:

```
db2 connect to TIODB user db2admin using <password>
```

This connects to the database named **TIODB** with a user ID of **db2admin**.

The output is shown as follows:

```
Database Connection Information

 Database server        = DB2/NT 7.2.6
 SQL authorization ID   = RCHIANG
 Local database alias   = TIODB
```

3. Issue this command to list the DB2 applications:

   ```
   db2 list application
   ```

   You will see this output:

   ```
   Auth Id  Application    Appl.      Application Id               DB       # of
            Name           Handle                                  Name    Agents

   -------- -------------- ---------- --------------------------- -------- -----

   RCHIANG  db2bp.exe      11         *LOCAL.DB2.031024215710      SAMPLE   1

   RCHIANG  db2bp.exe      10         *LOCAL.DB2.031024215537      TIODB 1
   ```

4. Issue this command to stop the application:

   ```
   db2 force application (10)
   ```

5. You can then drop the DB2 database with this command:

   ```
   db2 drop database TIODB
   ```

Tivoli Directory Server tasks

This describes common tasks for Tivoli Directory Server. For more information, see the Tivoli Directory Server documentation.

Starting the directory administration daemon:

By default, the administration daemon is running when you install the Tivoli Directory Server. The daemon must be started to use the command line commands for starting and stopping the server and checking server status. To start the administration daemon run the command:

```
ibmdiradm
```

Checking Tivoli Directory Server status:

To verify the status of Tivoli Directory Server:

1. Log on to the Tivoli Directory Server computer. If you installed the Tivoli Directory Server client on the Tivoli Provisioning Manager server, you can check the status of Tivoli Directory Server from the Tivoli Provisioning Manager computer instead.
2. Run the following command:

   ```
   ibmdirctl –D cn=root –w password -h hostname status
   ```

   password
   The password for the base DN (cn=root)

   hostname
   The host name of the Tivoli Directory Server computer. The `-h` *hostname* part of the command is only required if you are connecting from the Tivoli Provisioning Manager computer.

Starting or stopping Tivoli Directory Server:

1. Log on to theTivoli Directory Server server. If you installed the Tivoli Directory Server client on the Tivoli Provisioning Manager server, you can check the status of Tivoli Directory Server from the Tivoli Provisioning Manager computer instead.
2. Run the appropriate command:

   Start Tivoli Directory Server

   Run the following command:

   ```
   ibmdirctl –D cn=root –w password -h hostname start
   ```

   Stop Tivoli Directory Server

   ```
   ibmdirctl –D cn=root –w password -h hostname stop
   ```

   password

   The password for the base DN (cn=root)

   hostname

   The host name of the Tivoli Directory Server computer. The `-h hostname` part of the command is only required if you are connecting from the Tivoli Provisioning Manager computer.

WebSphere Application Server tasks

This section provides tips on running with WebSphere Application Server. For more information, see the WebSphere Application Server documentation.

Checking WebSphere Application Server status

To check the status of WebSphere Application Server:

1. Change to the directory *$TIO_HOME*/tioprofile/bin.
2. Run the command:

   ```
   ./serverStatus.sh server1 -username admin_user -password admin_pwd
   ```

   where *admin_user* is the WebSphere Application Server administrator user name and *admin_pwd* is the password for the administrator. After a new installation of Tivoli Provisioning Manager, the administrator user name is `tioadmin`.

Starting and stopping the WebSphere Application Server

The following steps describe tasks for the WebSphere Application Server profile for Tivoli Provisioning Manager, **tioprofile**.

Start WebSphere Application Server

1. Change to the `$TIO_HOME/tioprofile/bin` directory.
2. Run the following command:

   ```
   ./startServer.sh server1
   ```

Stop WebSphere Application Server

1. Change to the `$TIO_HOME/tioprofile/bin` directory.
2. Run the following command:

   ```
   ./startServer.sh server1
   ```

   Stop the profile **tioprofile**:

   ```
   ./stopServer.sh server1 -username admin_user -password admin_pwd
   ```

For these commands, *admin_user* is the WebSphere Application Server administrator user name and *admin_pwd* is the password for the administrator. After a new installation of Tivoli Provisioning Manager, the administrator user name is `tioadmin`.

Logging on to the WebSphere Application Server administrative console

The administrative console is a graphical interface for performing deployment and system administration tasks. It runs in your Web browser. Your actions in the console modify a set of XML configuration files. You use the administrative console to manually deploy content integration server on WebSphere Application Server.

To use the administrative console:

1. Ensure that WebSphere Application Server is started. It is started automatically when you start Tivoli Provisioning Manager. If you want to start WebSphere Application Server only, see "Checking WebSphere Application Server status" on page 144 for instructions.
2. Ensure that cookies are enabled in the Web browser. Enablement of JavaScript™ is also recommended so that all the features of the administrative console are available to you.
3. Access the WebSphere Application Server administrative console at the following Web address:

   `http://`*`hostname`*`:`*`port`*`/admin`

   where *hostname* is thefully-qualified domain name of theTivoli Provisioning Manager computer and *port* is the WebSphere Application Server **Admin host secure port** that you defined during installation. The default port number is 9044. For example:

   `https://tpmserver.example.com:9044/admin`

   Note:

   When the administrative console is on the local machine, the value of *hostname* can be `localhost`.
4. Wait for the console to load into the browser. A Login page appears after the console starts.
5. Log on with your WebSphere Application Server administrator user ID and password. If you are using operating system authentication, log on as `tioadmin`. If you configured a read-only directory server after installation, the default user name is `wasadmin`. A user ID lasts for the duration of the session for which it was used to log in. If you enter an ID that is already in use (and in session), you are prompted to do one of the following:
   - Force the existing user ID out of session.
   - The configuration file used by the existing user ID is saved in the `temp` area.
   - Wait for the existing user ID to log out or time out of the session.
   - Specify a different user ID
6. Click **OK**.
7. When you are finished using the console, click **Save** on the console taskbar to save work that you have done and then click **Logout** to exit the console.

   Note: If you close the browser before saving your work, when you next log in under the same user ID, you can recover any unsaved changes

Appendix H. Backing up the database

You should back up your product after it is installed and perform periodic backups based on the backup policies in your organization.

Before backing up or restoring the database

Before you begin back up or restore the database, ensure that all running workflows are stopped, and then stop Tivoli Provisioning Manager.

1. Log on as `tioadmin`.
2. Ensure that Tivoli Provisioning Manager is running. You can verify the status of Tivoli Provisioning Manager by running the following command from *$TIO_HOME*/`tools`:

   `./tioStatus.sh` *`wasadmin_username wasadmin_password`*

   wasadmin_username
   The WebSphere Application Server administrator user name. After a new installation, the default is `tioadmin`.

   wasadmin_password
   The password for the specified user name. After a new installation, the default is `tioadmin`
3. Stop all running workflows.
   a. Change to the *$TIO_HOME*/`tools` directory.
   b. From the command prompt, run the following commands:

   ```
   ./cancel-all-in-progress.sh
   ./clean-up-deployment-requests.sh
   ```
4. Stop Tivoli Provisioning Manager.
5. Stop all running applications on the Tivoli Provisioning Manager computer: "Starting and stopping Tivoli Provisioning Manager" on page 53

Backing up a DB2 database

To back up the database:

1. Ensure that you followed the steps in "Before backing up or restoring the database."
2. Change the user to your DB2 instance owner. For a default installation, the DB2 database owner is `tioadmin`. For a custom installation, the default DB2 database owner is `db2inst1`. The following example uses the `db2inst1` user name:

   ```
   su - db2inst1
   ```
3. Run the following command to check for running applications:

   ```
   db2 list applications
   ```
4. If the command lists any applications, run the following command to disconnect them:

   ```
   db2 force applications all
   ```
5. If you are not connected to the database, use the `db2 connect` command to connect to the database. For example,`db2 connect to tc` where `tc` is the default database name.
6. Back up the database with the following command:

   `db2 backup` *`db_name`* `user` *`user_name`* `using` *`password`* `to` *`location`*

db_name
The name of the database.

user_name
The user name of the user performing the backup. This must be the Administrator.

password
The password used to authenticate the user name.

location
The location that the database backup will be stored.

- The full path of the location is required. The specified directory must already exist.
- The instance owner user must have write permissions to the specified path.
- Consider saving the backup in a location that is accessible from the Tivoli Provisioning Manager computer so that you do not need to transfer the backup to a second location when you are performing backup and restore operations.

7. If you did not select a target directory that is accessible to the Tivoli Provisioning Manager computer, transfer the backup to an accessible location.

A backup has been created and can be used to restore the Tivoli Provisioning Manager database when it is required.

Restoring a DB2 database

To restore the database:

1. Ensure that you followed the steps in "Before backing up or restoring the database" on page 147.
2. Open the file *$TIO_HOME*/config/dcm.xml to verify the database name and user name. The name element contains an alias for the database name, and the username element contains the user name. This information is specified Tivoli Provisioning Manager installation.
3. Change the user to your DB2 instance owner. For a default installation, the DB2 database owner is tioadmin. For a custom installation, the default DB2 database owner is db2inst1. The following example uses the db2inst1 user name:
   ```
   su - db2inst1
   ```
4. Run the following command to check for other running applications:
   ```
   db2 list applications
   ```
5. If the command lists other applications, run the following command to disconnect them:
   ```
   db2 force applications all
   ```
6. End the DB2 session with the command db2 terminate.
7. Stop DB2 with the command: db2stop.
8. Stop all DB2 interprocess communication with the command ipclean.
9. Start DB2 with the command: db2start.
10. Delete and uncatalog the existing database with the following command
    ```
    db2 drop db db_name
    ```

    where *db_name* is the name of the database.

11. Attach to the local host alias with the command:
    `db2 attach to LHOST0 user user_name using password`
12. Restore the backed up database with the following command:
    `db2 restore db db_name user user_name using password from location`

    db_name
    The name of the database.

    user_name
    The user name of the user restoring the database.

    password
    The password used to authenticate the user name.

    location
    The location where the backup is stored. The full path of the location is required.

The Tivoli Provisioning Manager database has been restored. The database backup remains in place so that you can restore the database whenever it is required.

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement might not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
2Z4A/101
11400 Burnet Road
Austin, TX 78758 U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Trademarks

AIX, DB2, IBM, System i™, System p™, System z, the IBM logo, Passport Advantage, Tivoli, and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Intel and Pentium® are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States, other countries, or both.

Linux is a trademark of Linus Torvalds in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

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

Adobe is a registered trademark of Adobe Systems Incorporated in the United States, other countries, or both.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.

Program Number:

Printed in USA

GC23-9723-00