Fedora 17

Installation Guide

Installing Fedora 17 on x86, AMD64, and Intel 64 architectures

Fedora Documentation Project
Preface xi
  1. Document Conventions ................................................................. xi
     1.1. Typographic Conventions ...................................................... xi
     1.2. Pull-quote Conventions ......................................................... xii
     1.3. Notes and Warnings .............................................................. xiii
  2. We Need Feedback! ....................................................................... xiii
  3. Acknowledgments ......................................................................... xiv

Introduction xv
  1. Background ................................................................................ xv
     1.1. About Fedora ........................................................................ xv
     1.2. Getting Additional Help ....................................................... xv
  2. About This Document .................................................................... xv
     2.1. Goals ................................................................................... xv
     2.2. Audience ............................................................................. xv

1. Quick Start for Experts 1
  1.1. Overview ................................................................................ 1
  1.2. Download Files ................................................................. 1
  1.3. Prepare for Installation ......................................................... 2
  1.4. Install Fedora ........................................................................ 2
  1.5. Perform Post-installation Steps ............................................. 2

2. Obtaining Fedora 3
  2.1. Downloading Fedora ............................................................. 3
     2.1.1. How Do I Download Installation Files? .......................... 3
     2.1.2. Which Architecture Is My Computer? ............................ 4
     2.1.3. Which Files Do I Download? ........................................... 5
  2.2. Obtaining Fedora on CD or DVD .......................................... 6

3. Making Media 7
  3.1. Making an installation DVD .................................................... 7
  3.2. Preparing a USB flash drive as an installation source .......... 8
     3.2.1. Making Fedora USB Media on a Windows Operating System 9
     3.2.2. Making Fedora USB Media in UNIX, Linux, and Similar Operating Systems 9
  3.3. Making Minimal Boot Media ................................................. 15
     3.3.1. UEFI-based systems ....................................................... 16

I. Installation and Booting 17

4. Planning for Installation on the x86 Architecture 19
  4.1. Upgrade or Install? .............................................................. 19
  4.2. Is Your Hardware Compatible? .............................................. 19
  4.3. RAID and Other Disk Devices .............................................. 19
     4.3.1. Hardware RAID ............................................................ 19
     4.3.2. Software RAID ............................................................ 20
     4.3.3. FireWire and USB Disks ................................................. 20
  4.4. Do You Have Enough Disk Space? ....................................... 20
  4.5. Selecting an Installation Method ........................................... 20
  4.6. Choose a boot method ......................................................... 21

5. Preparing for Installation 23
  5.1. Preparing for a Network Installation .................................... 23
     5.1.1. Preparing for FTP and HTTP installation .................... 24
     5.1.2. Preparing for an NFS installation ................................. 24
  5.2. Preparing for a Hard Drive Installation ............................... 25
Installation Guide

6. System Specifications List 29

7. Booting the Installer 31
  7.1. Starting the Installation Program .......................................................... 32
     7.1.1. Booting the Installation Program on x86, AMD64, and Intel 64 Systems ... 33
     7.1.2. The Boot Menu ............................................................................ 34
     7.1.3. Additional Boot Options .............................................................. 35
  7.2. Booting from the Network using PXE .................................................. 36

8. Configuring Installation Source 39
  8.1. Installation Method ........................................................................... 39
     8.1.1. Installing from DVD .................................................................... 39
     8.1.2. Installing from a Hard Drive ....................................................... 39
     8.1.3. Installing via NFS ....................................................................... 40
     8.1.4. Installing via FTP or HTTP ......................................................... 41

9. Installing using anaconda 43
  9.1. The Text Mode Installation Program User Interface .............................. 43
     9.1.1. Using the Keyboard to Navigate .................................................... 44
  9.2. The Graphical Installation Program User Interface .............................. 44
     9.2.1. Screenshots during installation ...................................................... 45
     9.2.2. A Note about Virtual Consoles .................................................... 45
  9.3. Language Selection .......................................................................... 45
  9.4. Keyboard Configuration .................................................................... 46

9.5. Storage Devices .................................................................................. 47
     9.5.1. The Storage Devices Selection Screen ........................................... 48
  9.6. Setting the Hostname ....................................................................... 61
     9.6.1. Edit Network Connections ............................................................ 62
  9.7. Time Zone Configuration ................................................................... 74
  9.8. Set the Root Password .................................................................... 75
  9.9. Assign Storage Devices .................................................................... 77
  9.10. Initializing the Hard Disk ................................................................. 78
  9.11. Upgrading an Existing System ......................................................... 79
     9.11.1. The Upgrade Dialog ................................................................. 80
     9.11.2. Upgrading Using the Installer ..................................................... 81
     9.11.3. Upgrading Boot Loader Configuration ......................................... 81
  9.12. Disk Partitioning Setup .................................................................... 82
  9.13. Encrypt Partitions .......................................................................... 86
  9.14. Creating a Custom Layout or Modifying the Default Layout ............ 87
     9.14.3. Create Software RAID ............................................................ 93
     9.14.4. Create LVM Logical Volume .................................................... 95
     9.14.5. Recommended Partitioning Scheme ........................................... 98
  9.15. Write changes to disk .................................................................... 102
  9.16. x86, AMD64, and Intel 64 Boot Loader Configuration ...................... 103
     9.16.1. Advanced Boot Loader Configuration ....................................... 106
     9.16.2. Rescue Mode ......................................................................... 108
     9.16.3. Alternative Boot Loaders ......................................................... 108
  9.17. Package Group Selection .................................................................. 108
     9.17.1. Installing from Additional Repositories ................................... 110
     9.17.2. Customizing the Software Selection ......................................... 113
  9.18. Installing Packages ....................................................................... 115
  9.19. Installation Complete ..................................................................... 115

10. Troubleshooting Installation on an Intel or AMD System 117
11. Boot Options
   11.1. Configuring the Installation System at the Boot Menu
   11.1.1. Specifying the Language
   11.1.2. Configuring the Interface
   11.1.3. Updating anaconda
   11.1.4. Specifying the Installation Method
   11.1.5. Specifying the Network Settings
   11.2. Enabling Remote Access to the Installation System
   11.2.1. Enabling Remote Access with VNC
   11.2.2. Connecting the Installation System to a VNC Listener
   11.2.3. Enabling Remote Access with ssh
   11.3. Logging to a Remote System During the Installation
   11.3.1. Configuring a Log Server
   11.4. Automating the Installation with Kickstart
   11.5. Enhancing Hardware Support
   11.5.1. Overriding Automatic Hardware Detection
   11.6. Using the Maintenance Boot Modes
   11.6.1. Loading the Memory (RAM) Testing Mode
   11.6.2. Verifying boot media
   11.6.3. Booting Your Computer with the Rescue Mode
   11.6.4. Upgrading your computer

12. Installing Without Media
   12.1. Retrieving Boot Files
   12.2. Editing the GRUB Configuration
   12.3. Booting to Installation

13. Setting Up an Installation Server
   13.1. Setting Up cobbler
   13.2. Setting Up the Distribution
   13.3. Mirroring a Network Location
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13.4. Importing the Distribution</td>
<td>145</td>
</tr>
<tr>
<td>13.5. Manually configure a PXE server</td>
<td>146</td>
</tr>
<tr>
<td>13.5.1. Setting up the Network Server</td>
<td>146</td>
</tr>
<tr>
<td>13.5.2. PXE Boot Configuration</td>
<td>147</td>
</tr>
<tr>
<td>13.5.3. Starting the <code>tftp</code> Server</td>
<td>150</td>
</tr>
<tr>
<td>13.5.4. Adding a Custom Boot Message</td>
<td>150</td>
</tr>
<tr>
<td>13.5.5. Performing the PXE Installation</td>
<td>151</td>
</tr>
<tr>
<td>14.1. VNC Viewer</td>
<td>153</td>
</tr>
<tr>
<td>14.2. VNC Modes in Anaconda</td>
<td>154</td>
</tr>
<tr>
<td>14.2.1. Direct Mode</td>
<td>154</td>
</tr>
<tr>
<td>14.2.2. Connect Mode</td>
<td>154</td>
</tr>
<tr>
<td>14.3. Installation Using VNC</td>
<td>155</td>
</tr>
<tr>
<td>14.3.1. Installation Example</td>
<td>155</td>
</tr>
<tr>
<td>14.3.2. Kickstart Considerations</td>
<td>156</td>
</tr>
<tr>
<td>14.3.3. Firewall Considerations</td>
<td>156</td>
</tr>
<tr>
<td>14.4. References</td>
<td>156</td>
</tr>
<tr>
<td>15. Kickstart Installations</td>
<td>157</td>
</tr>
<tr>
<td>15.1. What are Kickstart Installations?</td>
<td>157</td>
</tr>
<tr>
<td>15.2. How Do You Perform a Kickstart Installation?</td>
<td>157</td>
</tr>
<tr>
<td>15.3. Creating the Kickstart File</td>
<td>157</td>
</tr>
<tr>
<td>15.4. Kickstart Options</td>
<td>158</td>
</tr>
<tr>
<td>15.4.1. Advanced Partitioning Example</td>
<td>184</td>
</tr>
<tr>
<td>15.5. Package Selection</td>
<td>185</td>
</tr>
<tr>
<td>15.6. Pre-installation Script</td>
<td>186</td>
</tr>
<tr>
<td>15.6.1. Example</td>
<td>187</td>
</tr>
<tr>
<td>15.7. Post-installation Script</td>
<td>187</td>
</tr>
<tr>
<td>15.7.1. Example</td>
<td>188</td>
</tr>
<tr>
<td>15.8. Making the Kickstart File Available</td>
<td>189</td>
</tr>
<tr>
<td>15.8.1. Creating Kickstart Boot Media</td>
<td>189</td>
</tr>
<tr>
<td>15.8.2. Making the Kickstart File Available on the Network</td>
<td>189</td>
</tr>
<tr>
<td>15.9. Making the Installation Tree Available</td>
<td>190</td>
</tr>
<tr>
<td>15.10. Starting a Kickstart Installation</td>
<td>190</td>
</tr>
<tr>
<td>16. Kickstart Configurator</td>
<td>199</td>
</tr>
<tr>
<td>16.1. Basic Configuration</td>
<td>199</td>
</tr>
<tr>
<td>16.2. Installation Method</td>
<td>200</td>
</tr>
<tr>
<td>16.3. Boot Loader Options</td>
<td>202</td>
</tr>
<tr>
<td>16.4. Partition Information</td>
<td>203</td>
</tr>
<tr>
<td>16.4.1. Creating Partitions</td>
<td>203</td>
</tr>
<tr>
<td>16.5. Network Configuration</td>
<td>206</td>
</tr>
<tr>
<td>16.6. Authentication</td>
<td>207</td>
</tr>
<tr>
<td>16.7. Firewall Configuration</td>
<td>208</td>
</tr>
<tr>
<td>16.7.1. SELinux Configuration</td>
<td>209</td>
</tr>
<tr>
<td>16.8. Display Configuration</td>
<td>209</td>
</tr>
<tr>
<td>16.9. Package Selection</td>
<td>210</td>
</tr>
<tr>
<td>16.10. Pre-Installation Script</td>
<td>211</td>
</tr>
<tr>
<td>16.11. Post-Installation Script</td>
<td>212</td>
</tr>
<tr>
<td>16.11.1. Chroot Environment</td>
<td>213</td>
</tr>
<tr>
<td>16.11.2. Use an Interpreter</td>
<td>213</td>
</tr>
<tr>
<td>16.12. Saving the File</td>
<td>213</td>
</tr>
</tbody>
</table>
C.1. What is block device encryption? ................................................................. 273
C.2. Encrypting block devices using dm-crypt/LUKS ........................................ 273
   C.2.1. Overview of LUKS .................................................................................. 273
   C.2.2. How will I access the encrypted devices after installation? (System Startup) ................................................................. 274
   C.2.3. Choosing a Good Passphrase ................................................................. 274
C.3. Creating Encrypted Block Devices in Anaconda ........................................ 274
   C.3.1. What Kinds of Block Devices Can Be Encrypted? ............................... 275
   C.3.2. Saving Passphrases .............................................................................. 275
   C.3.3. Creating and Saving Backup Passphrases .............................................. 275
C.4. Creating Encrypted Block Devices on the Installed System After Installation ......................................................................................... 275
   C.4.1. Create the block devices .................................................................... 275
   C.4.2. Optional: Fill the device with random data .......................................... 275
   C.4.3. Format the device as a dm-crypt/LUKS encrypted device ................... 276
   C.4.4. Create a mapping to allow access to the device’s decrypted contents ...... 276
   C.4.5. Create filesystems on the mapped device, or continue to build complex storage structures using the mapped device ........................................ 277
   C.4.6. Add the mapping information to /etc/crypttab .................................... 277
   C.4.7. Add an entry to /etc/fstab .................................................................. 278
C.5. Common Post-Installation Tasks .................................................................. 278
   C.5.1. Set a randomly generated key as an additional way to access an encrypted block device ................................................................. 278
   C.5.2. Add a new passphrase to an existing device ........................................... 279
   C.5.3. Remove a passphrase or key from a device ........................................... 279

D. Understanding LVM 281

E. The GRUB Boot Loader 283
   E.1. Boot Loaders and System Architecture .................................................. 283
   E.2. GRUB ........................................................................................................ 283
      E.2.1. GRUB and the boot process on BIOS-based x86 systems ................ 283
      E.2.2. GRUB and the boot process on UEFI-based x86 systems .................. 284
      E.2.3. Features of GRUB ............................................................................ 285
   E.3. Installing GRUB ....................................................................................... 285
   E.4. GRUB Terminology .................................................................................. 286
      E.4.1. Device Names .................................................................................... 286
      E.4.2. File Names and Blocklists ................................................................. 287
      E.4.3. The Root File System and GRUB ....................................................... 288
   E.5. GRUB Interfaces ..................................................................................... 288
      E.5.1. Interfaces Load Order .................................................................... 289
   E.6. GRUB Commands .................................................................................. 290
   E.7. GRUB Menu Configuration File .............................................................. 291
      E.7.2. Configuration File Directives ............................................................. 292
   E.8. Changing Runlevels at Boot Time ............................................................ 293
   E.9. Additional Resources ............................................................................. 293
      E.9.1. Installed Documentation ................................................................. 294
      E.9.2. Useful Websites .............................................................................. 294

F. Boot Process, Init, and Shutdown 295
   F.1. The Boot Process ..................................................................................... 295
   F.2. A Detailed Look at the Boot Process ....................................................... 295
      F.2.1. The firmware interface .................................................................... 295
      F.2.2. The Boot Loader .............................................................................. 296
      F.2.3. The Kernel ....................................................................................... 297
Preface

1. Document Conventions
This manual uses several conventions to highlight certain words and phrases and draw attention to specific pieces of information.

In PDF and paper editions, this manual uses typefaces drawn from the Liberation Fonts\textsuperscript{1} set. The Liberation Fonts set is also used in HTML editions if the set is installed on your system. If not, alternative but equivalent typefaces are displayed. Note: Red Hat Enterprise Linux 5 and later includes the Liberation Fonts set by default.

1.1. Typographic Conventions
Four typographic conventions are used to call attention to specific words and phrases. These conventions, and the circumstances they apply to, are as follows.

**Mono-spaced Bold**

Used to highlight system input, including shell commands, file names and paths. Also used to highlight keycaps and key combinations. For example:

> To see the contents of the file `my_next_bestselling_novel` in your current working directory, enter the `cat my_next_bestselling_novel` command at the shell prompt and press Enter to execute the command.

The above includes a file name, a shell command and a keycap, all presented in mono-spaced bold and all distinguishable thanks to context.

Key combinations can be distinguished from keycaps by the hyphen connecting each part of a key combination. For example:

> Press Enter to execute the command.

> Press **Ctrl+Alt+F2** to switch to the first virtual terminal. Press **Ctrl+Alt+F1** to return to your X-Windows session.

The first paragraph highlights the particular keycap to press. The second highlights two key combinations (each a set of three keycaps with each set pressed simultaneously).

If source code is discussed, class names, methods, functions, variable names and returned values mentioned within a paragraph will be presented as above, in **mono-spaced bold**. For example:

> File-related classes include **filesystem** for file systems, **file** for files, and **dir** for directories. Each class has its own associated set of permissions.

**Proportional Bold**

This denotes words or phrases encountered on a system, including application names; dialog box text; labeled buttons; check-box and radio button labels; menu titles and sub-menu titles. For example:

> Choose **System → Preferences → Mouse** from the main menu bar to launch **Mouse Preferences**. In the **Buttons** tab, click the **Left-handed mouse** check box and click

\textsuperscript{1} \url{https://fedorahosted.org/liberation-fonts/}
Close to switch the primary mouse button from the left to the right (making the mouse suitable for use in the left hand).

To insert a special character into a gedit file, choose Applications → Accessories → Character Map from the main menu bar. Next, choose Search → Find… from the Character Map menu bar, type the name of the character in the Search field and click Next. The character you sought will be highlighted in the Character Table. Double-click this highlighted character to place it in the Text to copy field and then click the Copy button. Now switch back to your document and choose Edit → Paste from the gedit menu bar.

The above text includes application names; system-wide menu names and items; application-specific menu names; and buttons and text found within a GUI interface, all presented in proportional bold and all distinguishable by context.

Mono-spaced Bold Italic or Proportional Bold Italic

Whether mono-spaced bold or proportional bold, the addition of italics indicates replaceable or variable text. Italics denotes text you do not input literally or displayed text that changes depending on circumstance. For example:

To connect to a remote machine using ssh, type ssh username@domain.name at a shell prompt. If the remote machine is example.com and your username on that machine is john, type ssh john@example.com.

The mount -o remount file-system command remounts the named file system. For example, to remount the /home file system, the command is mount -o remount /home.

To see the version of a currently installed package, use the rpm -q package command. It will return a result as follows: package-version-release.

Note the words in bold italics above — username, domain.name, file-system, package, version and release. Each word is a placeholder, either for text you enter when issuing a command or for text displayed by the system.

Aside from standard usage for presenting the title of a work, italics denotes the first use of a new and important term. For example:

Publican is a DocBook publishing system.

1.2. Pull-quote Conventions

Terminal output and source code listings are set off visually from the surrounding text.

Output sent to a terminal is set in mono-spaced roman and presented thus:

<table>
<thead>
<tr>
<th>books</th>
<th>Desktop</th>
<th>documentation</th>
<th>drafts</th>
<th>mss</th>
<th>photos</th>
<th>stuff</th>
<th>svn</th>
</tr>
</thead>
<tbody>
<tr>
<td>books_tests</td>
<td>Desktop1</td>
<td>downloads</td>
<td>images</td>
<td>notes</td>
<td>scripts</td>
<td>svgs</td>
<td></td>
</tr>
</tbody>
</table>

Source-code listings are also set in mono-spaced roman but add syntax highlighting as follows:

```java
package org.jboss.book.jca.ex1;
import javax.naming.InitialContext;
```
public class ExClient
{
    public static void main(String args[])
        throws Exception
    {
        InitialContext iniCtx = new InitialContext();
        Object ref = iniCtx.lookup("EchoBean");
        EchoHome home = (EchoHome) ref;
        Echo echo = home.create();

        System.out.println("Created Echo");
        System.out.println("Echo.echo('Hello') = " + echo.echo("Hello"));
    }
}
3. Acknowledgments

Introduction

This guide covers installation of Fedora, a Linux distribution built on free and open source software. This manual helps you install Fedora on desktops, laptops, and servers. The installation system is easy to use even if you lack previous knowledge of Linux or computer networks. If you select default options, Fedora provides a complete desktop operating system, including productivity applications, Internet utilities, and desktop tools.

This document details the full range of installation options, including those that apply only in limited or unusual circumstances. The Fedora 17 Installation Quick Start Guide provides a much-abbreviated set of instructions for downloading Fedora, creating an installation disc, and installing Fedora on a typical desktop or laptop computer. The Fedora 17 Installation Quick Start Guide is available from http://docs.fedoraproject.org/installation-quick-start-guide/.

1. Background

1.1. About Fedora

To find out more about Fedora, refer to http://fedoraproject.org/. To read other documentation on Fedora related topics, refer to http://docs.fedoraproject.org/.

1.2. Getting Additional Help

For information on additional help resources for Fedora, visit http://fedoraproject.org/wiki/Communicate.

2. About This Document

2.1. Goals

This guide helps a reader:

1. Understand how to locate the Fedora distribution online
2. Create configuration data that allows a computer to boot Fedora
3. Understand and interact with the Fedora installation program
4. Complete basic post-installation configuration of a Fedora system

Other Sources of Documentation

This guide does not cover use of Fedora. To learn how to use an installed Fedora system, refer to http://docs.fedoraproject.org/ for other documentation.

2.2. Audience

This guide is intended for Fedora users of all levels of experience. However, it treats the installation process and its many options in far greater detail than most novice users are likely to require. You do
not need to read and understand this entire document to install Fedora on a computer. This document is most likely to help experienced users perform advanced and unusual installations.
Quick Start for Experts

This section offers a very brief overview of installation tasks for experienced readers who are eager to get started. Note that many explanatory notes and helpful hints appear in the following chapters of this guide. If an issue arises during the installation process, consult the appropriate chapters in the full guide for help.

Experts Only

This section is intended only for experts. Other readers may not be familiar with some of the terms in this section, and should move on to Chapter 2, Obtaining Fedora instead.

1.1. Overview

The installation procedure is fairly simple, and consists of only a few steps:

1. Download files to make media or another bootable configuration.

2. Prepare system for installation.

3. Boot the computer and run the installation process.

4. Reboot and perform post-installation configuration.

1.2. Download Files

Do any one of the following:

Verify your downloads

Downloads may fail for any number of reasons. Always verify the sha256sum of the downloaded files.

1. Download the ISO image for a Live image. Create CD media from the ISO file using your preferred application. You may also use the livecd-tools package to write the image to other bootable media such as a USB flash disk. To install the distribution to your hard disk, use the shortcut on the desktop after you log in.

2. Download the ISO images for the full distribution on DVD. Create DVD media from the ISO files using your preferred application, or put the images on a Windows FAT32 or Linux ext2, ext3, or ext4 partition.

3. Download the boot.iso image for a minimal boot CD or USB flash drive. Write the image to the appropriate physical media to create bootable media. The boot media contains no packages but must be pointed at a hard disk or online repository to complete the installation.

4. Download the vmlinuz kernel file and the initrd.img ramdisk image from the distribution's isolinux/ directory. Configure your operating system to boot the kernel and load the ramdisk
Chapter 1. Quick Start for Experts

image. For further information on installation without media, refer to Chapter 12, Installing Without Media.

For information on setting up a network boot server from which you can install Fedora, refer to Chapter 13, Setting Up an Installation Server.

To learn how to turn ISO images into CD or DVD media, refer to Making Fedora Discs available from http://docs.fedoraproject.org/readme-burning-isos/.

1.3. Prepare for Installation

Back up any user data you need to preserve.

Resizing Partitions

The installation program provides functions for resizing ext2, ext3, ext4, and NTFS formatted partitions. Refer to Section 9.14, "Creating a Custom Layout or Modifying the Default Layout" for more information.

1.4. Install Fedora

Boot from the desired media, with any options appropriate for your hardware and installation mode. Refer to Chapter 11, Boot Options for more information about boot options. If you boot from the Live CD, select the Install to Hard Disk option from the desktop to run the installation program. (Alternatively, the option can be found in Applications → System Tools.) If you boot from minimal media or a downloaded kernel, select a network or hard disk resource from which to install.

Proceed through all the steps of the installation program. The installation program does not change your system until you make a final confirmation to proceed. When installation is finished, reboot your system.

1.5. Perform Post-installation Steps

After the system reboots, it displays additional configuration options. Make appropriate changes to your system and proceed to the login prompt.

Refer to Chapter 17, Firstboot or the Firstboot page on the Fedora wiki: http://fedoraproject.org/wiki/FirstBoot for more detail.
Chapter 2.

Obtaining Fedora

This chapter explains how to get the files you need to install and run Fedora on your computer. Concepts in this chapter may be new, especially if this is your first free and open source operating system. If you have any trouble with this chapter, find help by visiting the Fedora Forums at http://www.fedoraforum.org/.

The Fedora Project distributes Fedora in many ways, mostly free of cost and downloaded over the Internet. The most common distribution method is CD and DVD media. There are several types of CD and DVD media available, including:

- A full set of the software on DVD media
- Live images you can use to try Fedora, and then install to your system if you so choose
- Reduced-size bootable CD and USB flash disk images you can use to install over an Internet connection
- Source code on DVD media

Most users want the Fedora Live image or the full set of installable software on DVD. The reduced bootable images are suitable for use with a fast Internet connection and install Fedora on one computer. Source code discs are not used for installing Fedora, but are resources for experienced users and software developers.

Users with a broadband Internet connection can download ISO images of CD and DVD media or images of USB flash disks. An ISO image is a copy of an entire disc in a format suitable for writing directly to a CD or DVD. A USB flash disk image is a copy of an entire disk in a format suitable for writing directly to a USB flash disk.

For more information on burning CDs and DVDs, refer to Chapter 3, Making Media.

If downloading the Fedora ISO images and burning them to CD or DVD is impossible or impractical for you, refer to Section 2.2, “Obtaining Fedora on CD or DVD” to learn about other ways that you can obtain Fedora.

2.1. Downloading Fedora

2.1.1. How Do I Download Installation Files?

To follow a Web-based guide to downloading, visit http://get.fedoraproject.org/. For guidance on which architecture to download, refer to Section 2.1.2, “Which Architecture Is My Computer?”.

Fedora software is available for download at no cost in a variety of ways.

2.1.1.1. From a Mirror
Chapter 2. Obtaining Fedora

The Fedora installation files are freely available from web servers located in many parts of the world. These servers mirror the files available from the Fedora Project. If you visit http://download.fedoraproject.org/, you are redirected to a mirror, based on a calculation of which mirror is likely to offer you the best download speed. Alternatively, you can choose a mirror from the list maintained at http://mirrors.fedoraproject.org/publiclist. This page lists mirrors according to geographic location. The mirrors geographically closest to you are likely to provide you with the fastest downloads. If the company or organization that provides your internet access maintains a mirror, this mirror is likely to provide you with the fastest downloads of all.

Mirrors publish Fedora software under a well-organized hierarchy of folders. For example, the Fedora 17 distribution normally appears in the directory fedora/linux/releases/17/. This directory contains a folder for each architecture supported inside that folder, in a folder called iso/. For example, you can find the file for the DVD distribution of Fedora 17 for x86_64 at fedora/linux/releases/17/Fedora/x86_64/iso/Fedora-17-x86_64-DVD.iso.

2.1.1.2. From BitTorrent

BitTorrent is a way to download information in cooperation with other computers. Each computer cooperating in the group downloads pieces of the information in a particular torrent from other peers in the group. Computers that have finished downloading all the data in a torrent remain in the swarm to seed, or provide data to other peers. If you download using BitTorrent, as a courtesy you should seed the torrent at least until you have uploaded the same amount of data you downloaded.

If your computer does not have software installed for BitTorrent, visit the BitTorrent home page at http://www.bittorrent.com/download/ to download it. BitTorrent client software is available for Windows, Mac OS, Linux, and many other operating systems.

You do not need to find a special mirror for BitTorrent files. The BitTorrent protocol ensures that your computer participates in a nearby group. To download and use the Fedora BitTorrent files, visit http://torrent.fedoraproject.org/.

Minimal Boot Images

Minimal boot CD and USB flash disk images are not available through BitTorrent.

Verify your download

Once you have downloaded an ISO, verify it for security and integrity. To follow a web-based guide, visit https://fedoraproject.org/en/verify.

2.1.2. Which Architecture Is My Computer?

Releases are separated by architecture, or type of computer processor. Use the following table to determine the architecture of your computer according to the type of processor. Consult your manufacturer's documentation for details on your processor, if necessary.
Which Files Do I Download?

Table 2.1. Processor and architecture types

<table>
<thead>
<tr>
<th>Processor manufacturer and model</th>
<th>Architecture type for Fedora</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intel Atom (see note below,) Core series, Pentium 4, and recent vintage Xeon; AMD Athlon, Duron, some Semprons; and older; VIA C3, C7</td>
<td>i386</td>
</tr>
<tr>
<td>Intel Atom (See note below), Core 2 series, Core i series and Xeon; AMD: Athlon 64, Athlon II, Sempron64, Phenom series, Fusion series, Bulldozer series and Opteron; Apple MacBook, MacBook Pro, and MacBook Air</td>
<td>x86_64</td>
</tr>
</tbody>
</table>

1386 Works for Most Windows Compatible Computers

If you are unsure what type of processor your computer uses, choose 1386.

The exception is if your computer is a non-Intel based Apple Macintosh. Refer to http://fedoraproject.org/wiki/Architectures/PowerPC for more information on using Fedora on these systems.

Intel Atom Processor Architectures Vary

The Z Series and N200 Series Atom processors are based on the i386 architecture. The 230 and 330 Series and the rest of the N Series Atom processors are based on the x86_64 architecture. Refer to http://ark.intel.com/products/family/29035 for more details.

2.1.3. Which Files Do I Download?

You have several options to download Fedora. Read the options below to decide the best one for you.

Each file available for download in a Fedora distribution includes the architecture type in the file name. For example, the file for the DVD distribution of Fedora 17 for x86_64 is named Fedora-17-x86_64-DVD.iso. Refer to Section 2.1.2, “Which Architecture Is My Computer?” if you are unsure of your computer’s architecture.

Full Distribution on DVD

If you have plenty of time, a fast Internet connection, and wish a broader choice of software on the install media, download the full DVD version. Once burned to DVD, the media is bootable and includes an installation program. The DVD version contains a mode to perform rescue operations on your Fedora system in an emergency. You can download the DVD version directly from a mirror, or via BitTorrent.

Live Image

If you want to try Fedora before you install it on your computer, download the Live image version. If your computer supports booting from CD or USB, you can boot the operating system without making any changes to your hard disk. The Live image also provides an Install to Hard Disk desktop shortcut (alternatively, the shortcut can be found in Applications → System Tools). If you decide you like what you see, and want to install it, simply activate the selection to copy Fedora to your hard disk. You can download the Live image directly from a mirror, or using BitTorrent.
Chapter 2. Obtaining Fedora

For more detailed instructions on setting up a Live image installation, including selecting a language for the installation process, refer to the *Fedora Installation Quick Start Guide*.

**Minimal Boot Media**

If you have a fast Internet connection but do not want to download the entire distribution, you can download a small boot image. Fedora offers images for a minimal boot environment on CD. Once you boot your system with the minimal media, you can install Fedora directly over the Internet. Although this method still involves downloading a significant amount of data over the Internet, it is almost always much less than the size of the full distribution media. Once you have finished installation, you can add or remove software to your system as desired.

<table>
<thead>
<tr>
<th>Media type</th>
<th>File locations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full distribution on DVD</td>
<td>fedora/linux/releases/17/Fedora/arch/iso/Fedora-17-arch-DVD.iso</td>
</tr>
<tr>
<td>Live image</td>
<td>fedora/linux/releases/17/Live/arch/iso/ Fedora-17-arch-Live.iso, fedora/linux/releases/17/Live/ arch/iso/Fedora-17-KDE-arch-Live.iso</td>
</tr>
<tr>
<td>Minimal CD boot media</td>
<td>fedora/linux/releases/17/Fedora/arch/os/images/boot.iso</td>
</tr>
</tbody>
</table>

The following table explains where to find the desired files on a mirror site. Replace *arch* with the architecture of the computer being installed.

**2.2. Obtaining Fedora on CD or DVD**

If you do not have a fast Internet connection, or if you have a problem creating boot media, downloading may not be an option. Fedora DVD and CD distribution media is available from a number of online sources around the world at a minimal cost. Use your favorite Web search engine to locate a vendor, or refer to [http://fedoraproject.org/wiki/Distribution](http://fedoraproject.org/wiki/Distribution).
Making Media

Use the methods described in this section to create the following types of installation and boot media:

- an installation DVD
- a USB flash drive to use as an installation source
- a minimal boot CD or DVD that can boot the installer
- a USB flash drive to boot the installer

The following table indicates the types of boot and installation media available for different architectures and notes the image file that you need to produce the media.

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Installation DVD</th>
<th>Installation USB flash drive</th>
<th>Boot CD or boot DVD</th>
<th>Boot USB flash drive</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS-based 32-bit x86</td>
<td>x86 DVD ISO image file</td>
<td>x86 DVD ISO image file</td>
<td>boot.iso</td>
<td>boot.iso</td>
</tr>
<tr>
<td>BIOS-based AMD64 and Intel 64</td>
<td>x86_64 DVD ISO image file (to install 64-bit operating system)</td>
<td>x86_64 DVD ISO image file (to install 64-bit operating system)</td>
<td>boot.iso</td>
<td>boot.iso</td>
</tr>
<tr>
<td>UEFI-based 32-bit x86</td>
<td>Not available</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UEFI-based AMD64 and Intel 64</td>
<td>x86_64 DVD ISO image file</td>
<td>Not available</td>
<td>Not available</td>
<td>efiboot.img (from x86_64 DVD ISO image file)</td>
</tr>
</tbody>
</table>

3.1. Making an installation DVD

You can make an installation DVD using the disc burning software on your computer.

The exact series of steps that produces a DVD from an ISO image file varies greatly from computer to computer, depending on the operating system and disc burning software installed. Use this procedure as a general guide. You might be able to omit certain steps on your computer, or might have to perform some of the steps in a different order from the order described here.

Make sure that your disc burning software is capable of burning discs from image files. Although this is true of most disc burning software, exceptions exist.

In particular, note that the disc burning feature built into Windows XP and Windows Vista cannot burn DVDs; and that earlier Windows operating systems did not have any disc burning capability installed by default at all. Therefore, if your computer has a Windows operating system prior to Windows 7 installed on it, you need a separate piece of software for this task. Examples of popular disc burning software for Windows that you might already have on your computer include Nero Burning ROM and Roxio Creator.
Chapter 3. Making Media

The **Disk Utility** software installed by default with Mac OS X on Apple computers has the capability to burn discs from images built into it already. Most widely-used DVD burning software for Linux, such as **Brasero** and **K3b**, also includes this capability.

1. Download an ISO image file of a Fedora 17 disc as described in Chapter 2, Obtaining Fedora.

2. Insert a blank, writeable disc into your computer’s disc burner. On some computers, a window opens and displays various options when you insert the disc. If you see a window like this, look for an option to launch your chosen disc burning program. If you do not see an option like this, close the window and launch the program manually.

3. Launch your disc burning program. On some computers, you can do this by right-clicking (or control-clicking) on the image file and selecting a menu option with a label like **Copy image to DVD**, or **Copy CD or DVD image**. Other computers might provide you with a menu option to launch your chosen disc burning program, either directly or with an option like **Open With**. If none of these options are available on your computer, launch the program from an icon on your desktop, in a menu of applications such as the **Start** menu on Windows operating systems, or in the Mac **Applications** folder.

4. In your disc burning program, select the option to burn a DVD from an image file. For example, in **Nero Burning ROM**, this option is called **Burn Image** and is located on the **File** menu.

   Note that you can skip this step when using certain DVD burning software; for example, **Disk Utility** on Mac OS X does not require it.

5. Browse to the ISO image file that you downloaded previously and select it for burning.

6. Click the button that starts the burning process.

   On some computers, the option to burn a disc from an ISO file is integrated into a **context menu** in the file browser. For example, when you right-click an ISO file on a computer with a Linux or UNIX operating system that runs the GNOME desktop, the **Nautilus** file browser presents you with the option to **Write to disk**.

### 3.2. Preparing a USB flash drive as an installation source

**Unusual USB Media**

In a few cases with oddly formatted or partitioned USB media, image writing may fail.

You can install Fedora on 32-bit x86 systems and BIOS-based AMD64 and Intel 64 systems using a USB flash drive, provided that your hardware supports booting from this type of device. Note that you cannot install Fedora on UEFI-based AMD64 and Intel 64 systems from a USB flash drive, although you can use a USB flash drive to boot the Fedora installer on UEFI-based AMD64 and Intel 64 systems — refer to Section 3.3, “Making Minimal Boot Media”.

---

[Image]
3.2.1. Making Fedora USB Media on a Windows Operating System

This method is not destructive, so existing data on the media is not harmed. Nevertheless, it is always a good idea to back up important data before performing sensitive disk operations.

The most straightforward way to place a Fedora image on USB media using a Windows operating system is to transfer the Fedora live image to the USB device with the LiveUSB Creator tool.

Note that the dd tool discussed in Section 3.2.2, “Making Fedora USB Media in UNIX, Linux, and Similar Operating Systems” is also available for Windows. Follow the instructions in that section to use an implementation of dd for Windows operating systems. The instructions in this section assume that you will use LiveUSB Creator.


2. LiveUSB Creator can create live USB media either from an image file that you downloaded previously, as described in Section 2.1.3, “Which Files Do I Download?”, or it can download an image file from the Internet. Either:

   • click the Browse button under the Use existing LiveCD label, browse to the location where you previously downloaded a Fedora Live ISO file, and select that file.

   • select a Fedora Live ISO file from the drop-down menu that LiveUSB Creator presents under the Download Fedora label. Note that image files are large and that it is probably impractical to use LiveUSB Creator to download an image file if you do not have a broadband connection to the Internet.

3. Click Create Live USB.

3.2.2. Making Fedora USB Media in UNIX, Linux, and Similar Operating Systems

A graphical tool is available to create Fedora USB media on systems that run Fedora or operating systems derived from Fedora. To create Fedora USB media on other UNIX or Linux operating systems (including Mac OS X), use the command-line method described in Section 3.2.2.1.3, "Making Fedora USB Media with dd".

3.2.2.1. Creating Fedora USB Media in Fedora and similar Linux distributions

Graphical and command-line tools are available to create Fedora USB media on computers that run Fedora and Linux distributions derived from Fedora. The command line tools work with both Fedora DVD and live images, but the graphical tool works only with live images. To create Fedora USB media from the distribution image or minimal boot media image, use one of the command line methods described in Section 3.2.2.1.2, “Making Fedora USB Media with livecd-tools” and Section 3.2.2.1.3, “Making Fedora USB Media with dd”.

3.2.2.1.1. Making Fedora USB Media with a graphical tool

**Important — Enable Extra Packages for Enterprise Linux**

To perform this procedure on Linux distributions derived from Fedora, enable the *Extra Packages for Enterprise Linux* (EPEL) repository. Refer to [http://fedoraproject.org/wiki/EPEL/FAQ#howto](http://fedoraproject.org/wiki/EPEL/FAQ#howto) for instructions.

**Note — This Method Is Not Destructive**

This method is not destructive, so existing data on the media is not harmed. Nevertheless, it is always a good idea to back up important data before performing sensitive disk operations.

1. Install the `liveusb-creator` on your system with your graphical package manager, or the following command:

   ```bash
   su -c 'yum -y install liveusb-creator'
   ```

2. Plug in your USB media.

3. Launch `LiveUSB Creator`, either from a menu or by entering `liveusb-creator` on the command line. Enter the root password for your system when `LiveUSB Creator` prompts you for it.

4. `LiveUSB Creator` can create live USB media either from an image file that you downloaded previously, as described in Section 2.1.3, "Which Files Do I Download?", or it can download an image file from the Internet. Either:
   - click the **Browse** button under the **Use existing LiveCD** label, browse to the location where you previously downloaded a Fedora Live ISO file, and select that file.
   - select a Fedora Live ISO file from the drop-down menu that `LiveUSB Creator` presents under the **Download Fedora** label. Note that image files are large and that it is probably impractical to use `LiveUSB Creator` to download an image file if you do not have a broadband connection to the Internet.

5. Click **Create Live USB**.
3.2.2.1.2. Making Fedora USB Media with livecd-tools

**Important — Enable Extra Packages for Enterprise Linux**

To perform this procedure on Linux distributions derived from Fedora, enable the Extra Packages for Enterprise Linux (EPEL) repository. Refer to [http://fedoraproject.org/wiki/EPEL/FAQ#howtouse](http://fedoraproject.org/wiki/EPEL/FAQ#howtouse) for instructions.

**Note — This Method Is Not Destructive**

This method is not destructive, so existing data on the media is not harmed. Nevertheless, it is always a good idea to back up important data before performing sensitive disk operations.

1. Install the `livecd-tools` package on your system with your graphical package manager, or the following command:

   ```bash
   su -c 'yum -y install livecd-tools'
   ```

2. Plug in your USB media.

3. Find the device name for your USB media. If the media has a volume name, use it to look up the device name in `/dev/disk/by-label`, or use the `findfs`:

   ```bash
   su -c 'findfs LABEL="MyLabel"'
   ```

   If the media does not have a volume name, or you do not know it, consult the `/var/log/messages` log for details:

   ```bash
   su -c 'less /var/log/messages'
   ```

4. Use the `livecd-iso-to-disk` command to write the ISO image to the media:

   ```bash
   su -c 'livecd-iso-to-disk the_image.iso /dev/sdX1'
   ```

   Replace `sdX1` with the device name for the partition on the USB media. Most flash drives and external hard disks use only one partition. If you have changed this behavior or have oddly partitioned media, you may need to consult other sources of help.
3.2.2.1.3. Making Fedora USB Media with dd

**Warning — These instructions could destroy data**

When you perform this procedure any data on the USB flash drive is destroyed with no warning. Make sure that you specify the correct USB flash drive, and make sure that this flash drive does not contain any data that you want to keep.

1. Plug in your USB flash drive.

2. Become root:

   ```
   su -
   ```

3. Your flash drive must have a single partition with a vfat file system. To determine how it is formatted, find the name of this partition and the device itself by running `dmesg` shortly after connecting the drive. The device name (similar to `/dev/sdc`) and the partition name (similar to `/dev/sdc1`) both appear in several lines towards the end of the output.

4. Use the partition name to ensure that the file system type of the USB flash drive is vfat.

   ```
   # blkid partition
   ```

   You should now see a message similar to:

   ```
   LABEL="LIVE" UUID="6676-27D3" TYPE="vfat"
   ```

   If TYPE is anything other than vfat (for example, TYPE="iso9660"), clear the first blocks of the USB flash drive:

   ```
   # dd if=/dev/zero of=partition bs=1M count=100
   ```

5. Use the `dd` command to transfer the boot ISO image to the USB device:

   ```
   # dd if=path/image_name.iso of=device
   ```

   where `path/image_name.iso` is the boot ISO image file that you downloaded and `device` is the device name for the USB flash drive. Ensure you specify the device name, not the partition name. For example:

   ```
   # dd if=/Download/Fedora-17-x86_64-DVD.iso of=/dev/sdc
   ```

3.2.2.2. Making Fedora USB Media in other Linux Distributions

To create Fedora USB media from a DVD or live image on a computer that uses a Linux distribution other than Fedora and those derived from Fedora, use one of the command-line procedures detailed in this section.
3.2.2.2.1. Making Fedora USB Media with livecd-tools

This method is not destructive, so existing data on the media is not harmed. Nevertheless, it is always a good idea to back up important data before performing sensitive disk operations.

This method works only on Linux operating systems.

1. Download a DVD or live ISO image for Fedora as shown in Section 2.1.3, “Which Files Do I Download?”

2. Plug in your USB media.

3. Find the device name for your USB media. If the media has a volume name, look up the name in /dev/disk/by-label, or use the findfs:

   ```
   su -c 'findfs LABEL="MyLabel"'
   ```

   If the media does not have a volume name, or you do not know it, consult the /var/log/messages log for details:

   ```
   su -c 'less /var/log/messages'
   ```

4. Many Linux distributions automatically mount USB media devices when you connect the device to your computer. If this is the case, unmount the device. The specific method to do this varies widely between Linux distributions and desktops. Some common methods include:

   - select File > Unmount if the operating system presents you with a window that displays the contents of the device.
   - right-click on an icon of the device and click Unmount.
   - click on an icon that represents ejecting the media — commonly, an upward-pointing triangle.

5. At a command line, type su - to become root, and enter the root password when your system prompts you.

6. Create a mount point for the image that you downloaded. For example, to use /tmp/livecd as the mount point, type mkdir /tmp/livecd and press Enter.

7. Mount the image with the following command: mount -o loop /path/to/image/file/imagefile.iso /path/to/mount/point, where /path/to/image/file is the location of the image file that you downloaded, imagefile.iso is the image file, and /path/to/mount/point is the mount point that you just created.

8. Change directory to the LiveOS directory of the image that you just mounted. mount point where you just mounted the Fedora image. For example, cd /tmp/livecd/LiveOS.

9. Run the following command: ./livecd-iso-to-disk /path/to/image/file/imagefile.iso device, where /path/to/image/file is the location of the image file that you downloaded, imagefile.iso is the image file, and device is the USB media device.
Example 3.1. Mounting a Fedora live image file and using livecd-iso-to-disk to create live USB media

You have downloaded a Fedora live image, Fedora-17-i686-Live.iso, to a folder named Downloads in your home directory. You have a USB flash drive plugged into your computer, named /dev/sdc1

Become root:

```bash
su -
```

Make a mount point for the image:

```bash
mkdir /mnt/livecd
```

Mount the image:

```bash
mount -o loop /home/Username/Downloads/Fedora-17-i686-Live.iso /mnt/livecd
```

Change into the LiveOS directory of the live CD image:

```bash
cd /mnt/livecd/LiveOS
```

Run livecd-iso-to-disk to transfer the live image to your flash drive and make the flash drive bootable:

```bash
./livecd-iso-to-disk /home/Username/Downloads/Fedora-17-i686-Live.iso /dev/sdc1
```

3.2.2.2.2. Making Fedora USB Media with dd

⚠️ Warning — These instructions could destroy data

When you perform this procedure any data on the USB flash drive is destroyed with no warning. Make sure that you specify the correct USB flash drive, and make sure that this flash drive does not contain any data that you want to keep.

Use this method for the distribution image, the minimal boot media image, or on systems with a UNIX operating system (including Mac OX X).

1. Plug in your USB flash drive.

2. Become root:

```bash
su -
```

3. Your flash drive must have a single partition with a vfat file system. To determine how it is formatted, find the name of this partition and the device itself by running dmesg shortly after connecting the drive. The device name (similar to /dev/sdc) and the partition name (similar to /dev/sdc1) both appear in several lines towards the end of the output.
4. Use the partition name to ensure that the file system type of the USB flash drive is vfat.

```
# blkid partition
```

You should now see a message similar to:

```
LABEL="LIVE" UUID="6676-27D3" TYPE="vfat"
```

If TYPE is anything other than vfat (for example, TYPE="iso9660"), clear the first blocks of the USB flash drive:

```
# dd if=/dev/zero of=partition bs=1M count=100
```

5. Use the `dd` command to transfer the boot ISO image to the USB device:

```
# dd if=~/Download/Fedora-17-x86_64-DVD.iso of=/dev/sdc
```

### 3.3. Making Minimal Boot Media

A piece of minimal boot media is a CD, DVD, or USB flash drive that contains the software to boot the system and launch the installation program, but which does not contain the software that must be transferred to the system to create a Fedora installation.

Use minimal boot media:

- to boot the system to install Fedora over a network
- to boot the system to install Fedora from a hard drive
- to use a kickstart file during installation (refer to Section 15.8.1, “Creating Kickstart Boot Media”
- to commence a network or hard-drive installation or to use an `anaconda` update or a kickstart file with a DVD installation.

You can use minimal boot media to start the installation process on 32-bit x86 systems, AMD64 or Intel 64 systems, and POWER systems. The process by which you create minimal boot media for systems of these various types is identical except in the case of AMD64 and Intel 64 systems with UEFI firmware interfaces — refer to Section 3.3.1, “UEFI-based systems”.

To make minimal boot media for 32-bit x86 systems, BIOS-based AMD64 or Intel 64 systems, and POWER systems:

1. Download the ISO image file named `boot.iso` that is available at the same location as the images of the Fedora 17 installation DVD — refer to Chapter 2, Obtaining Fedora.

2. Burn `boot.iso` to a blank CD or DVD using the same procedure detailed in Section 3.1, “Making an installation DVD” for the installation disc, or transfer the `boot.iso` file to a USB device with the `dd` command as detailed in Section 3.2, “Preparing a USB flash drive as an installation.”
As the `boot.iso` file is only around 200 MB in size, you do not need an especially large USB flash drive.

### 3.3.1. UEFI-based systems

The Fedora Project does not provide an image to produce minimal boot CDs or DVDs for UEFI-based systems. Use a USB flash drive (as described in this section) to boot the Fedora 17 installer. The full DVD installation image should function as expected.

Use the `efidisk.img` file in the `images/` directory on the Fedora 17 installation DVD to produce a bootable USB flash drive for UEFI-based systems.

1. Download an ISO image file of the Fedora 17 installation DVD as described in Chapter 2, *Obtaining Fedora*.
2. Become root:
   ```bash
   su -
   ```
3. Create a mount point for the ISO image file:
   ```bash
   # mkdir /mnt/dvdiso
   ```
4. Mount the image file:
   ```bash
   # mount DVD.iso /mnt/dvdiso -o loop
   ```
   Where `DVD.iso` is the name of the ISO image file, for example `Fedora17-x86_64-DVD.iso`.
5. Transfer `efidisk.img` from the ISO image file to your USB flash drive:
   ```bash
   # dd if=/mnt/dvdiso/images/efidisk.img of=/dev/device_name
   ```
   For example:
   ```bash
   # dd if=/mnt/dvdiso/images/efidisk.img of=/dev/sdc
   ```
6. Unmount the ISO image file:
   ```bash
   # umount /mnt/dvdiso
   ```
Part I. Installation and Booting

This part of the *Fedora Installation Guide* details the installation process itself, from various methods of booting the installer up to the point where the computer must restart to finalize the installation. This part of the manual also includes a chapter on troubleshooting problems with the installation process.
Chapter 4.

Planning for Installation on the x86 Architecture

4.1. Upgrade or Install?
For information to help you determine whether to perform an upgrade or an installation refer to Chapter 20, Upgrading Your Current System.

4.2. Is Your Hardware Compatible?
Hardware compatibility is particularly important if you have an older system or a system that you built yourself. Fedora 17 should be compatible with most hardware in systems that were factory built within the last two years. However, hardware specifications change almost daily, so it is difficult to guarantee that your hardware is 100% compatible.

The most recent list of supported hardware can be found in the Release Notes for Fedora 17, available at http://docs.fedoraproject.org/release-notes.

At the end of a successful Fedora installation process, the installation program offers you the option to provide details of your hardware configuration anonymously to the Fedora Project (refer to Section 17.4, “Hardware Profile”). You can view the statistics gathered by this method at http://smolt.fedoraproject.org/static/stats/devices.html. Viewing the list of hardware that makes up systems on which other people have successfully installed Fedora might help you determine how suitable your hardware is.

4.3. RAID and Other Disk Devices

**Important — Systems with Intel BIOS RAID sets**

Fedora 17 uses *mdraid* instead of *dmraid* for installation onto Intel BIOS RAID sets. These sets are detected automatically, and devices with Intel ISW metadata are recognized as mdraid instead of dmraid. Note that the device node names of any such devices under *mdraid* are different from their device node names under *dmraid*. Therefore, special precautions are necessary when you migrate systems with Intel BIOS RAID sets.

Local modifications to /etc/fstab, /etc/crypttab or other configuration files which refer to devices by their device node names will not work in Fedora 17. Before migrating these files, you must therefore edit them to replace device node paths with device UUIDs instead. You can find the UUIDs of devices with the *blkid* command.

4.3.1. Hardware RAID
RAID, or Redundant Array of Independent Disks, allows a group, or array, of drives to act as a single device. Configure any RAID functions provided by the mainboard of your computer, or attached controller cards, before you begin the installation process. Each active RAID array appears as one drive within Fedora.
On systems with more than one hard drive you may configure Fedora to operate several of the drives as a Linux RAID array without requiring any additional hardware.

### 4.3.2. Software RAID

You can use the Fedora installation program to create Linux software RAID arrays, where RAID functions are controlled by the operating system rather than dedicated hardware. These functions are explained in detail in *Section 9.14, “Creating a Custom Layout or Modifying the Default Layout”*. 

### 4.3.3. FireWire and USB Disks

Some FireWire and USB hard disks may not be recognized by the Fedora installation system. If configuration of these disks at installation time is not vital, disconnect them to avoid any confusion.

---

**Post-installation Usage**

You can connect and configure external FireWire and USB hard disks after installation. Most such devices are recognized by the kernel and available for use at that time.

---

### 4.4. Do You Have Enough Disk Space?

Nearly every modern-day operating system (OS) uses *disk partitions*, and Fedora is no exception. When you install Fedora, you may have to work with disk partitions. If you have not worked with disk partitions before (or need a quick review of the basic concepts), refer to *Appendix A, An Introduction to Disk Partitions* before proceeding.

The disk space used by Fedora must be separate from the disk space used by other OSes you may have installed on your system, such as Windows, OS/2, or even a different version of Linux. For x86, AMD64, and Intel 64 systems, at least two partitions (/ and swap) must be dedicated to Fedora.

Before you start the installation process, you must

- have enough *unpartitioned* disk space for the installation of Fedora, or
- have one or more partitions that may be deleted, thereby freeing up enough disk space to install Fedora.

To gain a better sense of how much space you really need, refer to the recommended partitioning sizes discussed in *Section 9.14.5, “Recommended Partitioning Scheme”*. 

If you are not sure that you meet these conditions, or if you want to know how to create free disk space for your Fedora installation, refer to *Appendix A, An Introduction to Disk Partitions*.

### 4.5. Selecting an Installation Method

What type of installation method do you wish to use? The following installation methods are available:

---

1 Unpartitioned disk space means that available disk space on the hard drives you are installing to has not been divided into sections for data. When you partition a disk, each partition behaves like a separate disk drive.
4.6. Choose a boot method

You can use several methods to boot Fedora.

Installing from a CD-ROM or DVD requires that you have a Fedora 17 CD-ROM or DVD, and you have a DVD/CD-ROM drive on a system that supports booting from it.

Your BIOS may need to be changed to allow booting from your DVD/CD-ROM drive. For more information about changing your BIOS, refer to Section 7.1.1, “Booting the Installation Program on x86, AMD64, and Intel 64 Systems”.

Other than booting from an installation CD or DVD, you can also boot the Fedora installation program from minimal boot media in the form of a bootable CD or USB flash drive. After you boot the system with a piece of minimal boot media, you complete the installation from a different installation source, such as a local hard drive or a location on a network. Refer to Section 3.3, “Making Minimal Boot Media” for instructions on making boot CDs and USB flash drives.
Finally, you can boot the installer over the network from a *preboot execution environment* (PXE) server. Refer to *Chapter 13, Setting Up an Installation Server*. Again, after you boot the system, you complete the installation from a different installation source, such as a local hard drive or a location on a network.
Preparing for Installation

5.1. Preparing for a Network Installation

Note

Make sure no installation DVD (or any other type of DVD or CD) is in your system's CD or DVD drive if you are performing a network-based installation. Having a DVD or CD in the drive might cause unexpected errors.

Ensure that you have boot media available on CD, DVD, or a USB storage device such as a flash drive.

The Fedora installation medium must be available for either a network installation (via NFS, FTP, or HTTP) or installation via local storage. Use the following steps if you are performing an NFS, FTP, or HTTP installation.

The NFS, FTP, or HTTP server to be used for installation over the network must be a separate, network-accessible server. It must provide the complete contents of the installation DVD-ROM.

Note

The Fedora installation program has the ability to test the integrity of the installation media. It works with the CD, DVD, hard drive ISO, and NFS ISO installation methods. We recommend that you test all installation media before starting the installation process, and before reporting any installation-related bugs (many of the bugs reported are actually due to improperly-burned discs). To use this test, type the following command at the boot: prompt:

```
linux mediacheck
```
Chapter 5. Preparing for Installation

Note

The public directory used to access the installation files over FTP, NFS, or HTTP is mapped to local storage on the network server. For example, the local directory `/var/www/inst/Fedora17` on the network server can be accessed as `http://network.server.com/inst/Fedora17`.

In the following examples, the directory on the installation staging server that will contain the installation files will be specified as `/location/of/disk/space`. The directory that will be made publicly available via FTP, NFS, or HTTP will be specified as `/publicly_available_directory`. For example, `/location/of/disk/space` may be a directory you create called `/var/isos`. `/publicly_available_directory` might be `/var/www/html/Fedora17`, for an HTTP install.

In the following, you will require an ISO image. An ISO image is a file containing an exact copy of the content of a DVD. To create an ISO image from a DVD use the following command:

```
dd if=/dev/dvd of=/path_to_image/name_of_image.iso
```

where `dvd` is your DVD drive device, `name_of_image` is the name you give to the resulting ISO image file, and `path_to_image` is the path to the location on your system where the resulting ISO image will be stored.

To copy the files from the installation DVD to a Linux instance, which acts as an installation staging server, continue with either Section 5.1.1, “Preparing for FTP and HTTP installation” or Section 5.1.2, “Preparing for an NFS installation”.

5.1.1. Preparing for FTP and HTTP installation

Extract the files from the ISO image of the installation DVD and place them in a directory that is shared over FTP or HTTP.

Next, make sure that the directory is shared via FTP or HTTP, and verify client access. Test to see whether the directory is accessible from the server itself, and then from another machine on the same subnet to which you will be installing.

5.1.2. Preparing for an NFS installation

For NFS installation it is not necessary to extract all the files from the ISO image. It is sufficient to make the ISO image available on the network server via NFS.

1. Transfer the ISO image to the NFS exported directory. On a Linux system, run:

```
mv /path_to_image/name_of_image.iso /publicly_available_directory/
```

where `path_to_image` is the path to the ISO image file, `name_of_image` is the name of the ISO image file, and `publicly_available_directory` is a directory that is available over NFS or that you intend to make available over NFS.
2. Use a SHA256 checksum program to verify that the ISO image that you copied is intact. Many SHA256 checksum programs are available for various operating systems. On a Linux system, run:

```
$ sha256sum name_of_image.iso
```

where `name_of_image.iso` is the name of the ISO image file. The SHA256 checksum program displays a string of 64 characters called a hash. Compare this hash to the hash displayed for this particular image on the GPG Keys page on the Fedora Project site at http://fedoraproject.org/en/keys. The two hashes should be identical.

3. Ensure that an entry for the publicly available directory exists in the `/etc/exports` file on the network server so that the directory is available via NFS.

To export a directory read-only to a specific system, use:

```
/publicly_available_directory client.ip.address (ro)
```

To export a directory read-only to all systems, use:

```
/publicly_available_directory * (ro)
```

4. On the network server, start the NFS daemon (on a Fedora system, use `/sbin/service nfs start`). If NFS is already running, reload the configuration file (on a Fedora system use `/sbin/service nfs reload`).

5. Be sure to test the NFS share following the directions in the Fedora Deployment Guide. Refer to your NFS documentation for details on starting and stopping the NFS server.

**Note**

The Fedora installation program has the ability to test the integrity of the installation media. It works with the CD, DVD, hard drive ISO, and NFS ISO installation methods. We recommend that you test all installation media before starting the installation process, and before reporting any installation-related bugs (many of the bugs reported are actually due to improperly-burned discs). To use this test, type the following command at the boot prompt:

```
linux mediacheck
```

5.2. Preparing for a Hard Drive Installation
Chapter 5. Preparing for Installation

**Note — Not all file systems supported**

Hard drive installations only work from ext2, ext3, ext4, or FAT file systems. You cannot use a hard drive formatted for any other file system as an installation source for Fedora.

To check the file system of a hard drive partition on a Windows operating system, use the **Disk Management** tool. To check the file system of a hard drive partition on a Linux operating system, use the **fdisk** tool.

**Cannot Install from LVM Partitions**

You cannot use ISO files on partitions controlled by LVM (Logical Volume Management).

Use this option to install Fedora on systems without a DVD drive or network connection.

Hard drive installations use an **ISO image** of the installation DVD. An ISO image is a file that contains an exact copy of the content of a DVD.

With these files present on a hard drive, you can choose **Hard drive** as the installation source when you boot the installation program (refer to **Section 8.1, “Installation Method”**).

Ensure that you have boot media available on CD, DVD, or a USB storage device such as a flash drive.

To prepare a hard drive as an installation source, follow these steps:

1. Obtain an ISO image of the Fedora installation DVD (refer to **Chapter 2, Obtaining Fedora**). Alternatively, if you have the DVD on physical media, you can create an image of it with the following command on a Linux system:

   ```
   dd if=/dev/dvd of=/path_to_image/name_of_image.iso
   ```

   where `dvd` is your DVD drive device, `name_of_image` is the name you give to the give to the resulting ISO image file, and `path_to_image` is the path to the location on your system where the resulting ISO image will be stored.

2. Transfer the ISO image to the hard drive.

   The ISO image must be located on a hard drive that is either internal to the computer on which you will install Fedora, or on a hard drive that is attached to that computer by USB.

3. Use a SHA256 checksum program to verify that the ISO image that you copied is intact. Many SHA256 checksum programs are available for various operating systems. On a Linux system, run:

   ```
   $ sha256sum name_of_image.iso
   ```

   where `name_of_image` is the name of the ISO image file. The SHA256 checksum program displays a string of 64 characters called a **hash**. Compare this hash to the hash displayed for this

**Note**

The Fedora installation program has the ability to test the integrity of the installation media. It works with the CD, DVD, hard drive ISO, and NFS ISO installation methods. We recommend that you test all installation media before starting the installation process, and before reporting any installation-related bugs (many of the bugs reported are actually due to improperly-burned discs). To use this test, type the following command at the boot: prompt:

```
linux mediacheck
```
System Specifications List

The installation program automatically detects and installs your computer's hardware. Although you should make sure that your hardware meets the minimum requirements to install Fedora (refer to Section 4.2, “Is Your Hardware Compatible?”) you do not usually need to supply the installation program with any specific details about your system.

However, when performing certain types of installation, some specific details might be useful or even essential.

• If you plan to use a customized partition layout, record:
  
  • The model numbers, sizes, types, and interfaces of the hard drives attached to the system. For example, Seagate ST3320613AS 320 GB on SATA0, Western Digital WD7500AAKS 750 GB on SATA1. This will allow you to identify specific hard drives during the partitioning process.

• If you are installing Fedora as an additional operating system on an existing system, record:
  
  • The mount points of the existing partitions on the system. For example, /boot on sda1, / on sda2, and /home on sdb1. This will allow you to identify specific partitions during the partitioning process.

  • Whether the hardware clock uses local time or UTC. In Linux systems, this information can be found in /etc/adjtime. Changing the hardware clock setting in Section 9.7, “Time Zone Configuration” may cause unexpected behavior in Fedora.

• If you plan to install from an image on a local hard drive:

  • The hard drive and directory that holds the image.

• If you plan to install from a network location, or install on an iSCSI target:

  • The make and model numbers of the network adapters on your system. For example, Netgear GA311. This will allow you to identify adapters when manually configuring the network.

    • IP, DHCP, and BOOTP addresses

    • Netmask

    • Gateway IP address

    • One or more name server IP addresses (DNS)

If any of these networking requirements or terms are unfamiliar to you, contact your network administrator for assistance.

• If you plan to install from a network location:

  • The location of the image on an FTP server, HTTP (web) server, or NFS server – see Section 8.1.4, “Installing via FTP or HTTP” and Section 8.1.3, “Installing via NFS” for examples.

• If you plan to install on an iSCSI target:

  • The location of the iSCSI target. Depending on your network, you might also need a CHAP username and password, and perhaps a reverse CHAP username and password – see Section 9.5.1.1, “Advanced Storage Options”.

• If your computer is part of a domain:
Chapter 6. System Specifications List

- You should verify that the domain name will be supplied by the DHCP server. If not, you will need to input the domain name manually during installation.
### Chapter 7.

## Booting the Installer

### Important — UEFI for 32-bit x86 systems

Fedora 17 does not support UEFI booting for 32-bit x86 systems. Only BIOS booting is supported.

### Important — UEFI for AMD64 and Intel 64

Note that the boot configurations of UEFI and BIOS differ significantly from each other. Therefore, the installed system must boot using the same firmware that was used during installation. You cannot install the operating system on a system that uses BIOS and then boot this installation on a system that uses UEFI.

Fedora 17 supports version 2.2 of the UEFI specification. Hardware that supports version 2.3 of the UEFI specification or later should boot and operate with Fedora 17, but the additional functionality defined by these later specifications will not be available. The UEFI specifications are available from [http://www.uefi.org/specs/agreement/](http://www.uefi.org/specs/agreement/)

To start the installation program from a Fedora DVD or from minimal boot media, follow this procedure:

1. Disconnect any external FireWire or USB disks that you do not need for installation. Refer to Section 4.3.3, "FireWire and USB Disks" for more information.

2. Power on your computer system.

3. Insert the media in your computer.

4. Power off your computer with the boot media still inside.

5. Power on your computer system.

You might need to press a specific key or combination of keys to boot from the media. On most computers, a message appears briefly on the screen very soon after you turn on the computer. Typically, it is worded something like **Press F10 to select boot device**, although the specific wording and the key that you must press varies widely from computer to computer. Consult the documentation for your computer or motherboard, or seek support from the hardware manufacturer or vendor. On Apple computers, the **C** key boots the system from the DVD drive. On older Apple hardware you might need to press **Cmd+Opt+Shift+Del** to boot from the DVD drive.

If your computer does not allow you to select a boot device as it starts up, you might need to configure your system's **Basic Input/Output System (BIOS)** to boot from the media.

To change your BIOS settings on an x86, AMD64, or Intel 64 system, watch the instructions provided on your display when your computer first boots. A line of text appears, telling you which key to press to enter the BIOS settings.
Chapter 7. Booting the Installer

Once you have entered your BIOS setup program, find the section where you can alter your boot sequence. The default is often C, A or A, C (depending on whether you boot from your hard drive [C] or a diskette drive [A]). Change this sequence so that the DVD is first in your boot order and that C or A (whichever is your typical boot default) is second. This instructs the computer to first look at the DVD drive for bootable media; if it does not find bootable media on the DVD drive, it then checks your hard drive or diskette drive.

Save your changes before exiting the BIOS. For more information, refer to the documentation that came with your system.

Note — Aborting the Installation

To abort the installation, either press Ctrl + Alt + Del or power off your computer with the power switch. You may abort the installation process without consequence at any time prior to selecting Write changes to disk on the Write partitioning to disk screen. Fedora makes no permanent changes to your computer until that point. Please be aware that stopping the installation after partitioning has begun can leave your computer unusable.

7.1. Starting the Installation Program

Important — UEFI for 32-bit x86 systems

Fedora 17 does not support UEFI booting for 32-bit x86 systems. Only BIOS booting is supported.

Important — UEFI for AMD64 and Intel 64

Note that the boot configurations of UEFI and BIOS differ significantly from each other. Therefore, the installed system must boot using the same firmware that was used during installation. You cannot install the operating system on a system that uses BIOS and then boot this installation on a system that uses UEFI.

Fedora 17 supports version 2.2 of the UEFI specification. Hardware that supports version 2.3 of the UEFI specification or later should boot and operate with Fedora 17, but the additional functionality defined by these later specifications will not be available. The UEFI specifications are available from http://www.uefi.org/specs/agreement/

To start, first make sure that you have all necessary resources for the installation. If you have already read through Chapter 4, Planning for Installation on the x86 Architecture, and followed the instructions, you should be ready to start the installation process. When you have verified that you are ready to begin, boot the installation program using the Fedora DVD or any boot media that you have created.
7.1.1. Booting the Installation Program on x86, AMD64, and Intel 64 Systems

You can boot the installation program using any one of the following media (depending upon what your system can support):

- **Fedora DVD** — Your machine supports a bootable DVD drive and you have the Fedora installation DVD.
- **Fedora live CD** — Your machine supports a bootable CD drive and you have a Fedora live CD.
- **Boot CD-ROM** — Your machine supports a bootable CD-ROM drive and you want to perform network or hard drive installation.
- **USB flash drive** — Your machine supports booting from a USB device.
- **PXE boot via network** — Your machine supports booting from the network. This is an advanced installation path. Refer to Chapter 13, Setting Up an Installation Server for additional information on this method.

To create a boot CD-ROM or to prepare your USB flash drive for booting or installation, refer to Section 3.3, “Making Minimal Boot Media”.

Insert the boot media and reboot the system.

You might need to press a specific key or combination of keys to boot from the media. On most computers, a message appears briefly on the screen very soon after you turn on the computer. Typically, it is worded something like **Press F10 to select boot device**, although the specific wording and the key that you must press varies widely from computer to computer. Consult the documentation for your computer or motherboard, or seek support from the hardware manufacturer or vendor. On Apple computers, the C key boots the system from the DVD drive. On older Apple hardware you might need to press **Cmd+Opt+Shift+Del** to boot from the DVD drive.

If your computer does not allow you to select a boot device as it starts up, you might need to configure your system's **Basic Input/Output System (BIOS)** to boot from the media.

To change your BIOS settings on an x86, AMD64, or Intel 64 system, watch the instructions provided on your display when your computer first boots. A line of text appears, telling you which key to press to enter the BIOS settings.

Once you have entered your BIOS setup program, find the section where you can alter your boot sequence. The default is often C, A or A, C (depending on whether you boot from your hard drive [C] or a diskette drive [A]). Change this sequence so that the DVD is first in your boot order and that C or A (whichever is your typical boot default) is second. This instructs the computer to first look at the DVD drive for bootable media; if it does not find bootable media on the DVD drive, it then checks your hard drive or diskette drive.

Save your changes before exiting the BIOS. For more information, refer to the documentation that came with your system.

After a short delay, the graphical boot screen appears, which contains information on a variety of boot options. Installation program automatically begins if you take no action within the first minute. For a description of the options available on this screen, refer to Section 7.1.2, “The Boot Menu”.

Alternatively, press the **Esc** key to access the boot: prompt, at which you can enter additional boot options as described in Section 7.1.3, “Additional Boot Options”.

33
Chapter 7. Booting the Installer

7.1.2. The Boot Menu
The boot media displays a graphical boot menu with two options:

Install or upgrade an existing system
   This option is the default. Choose this option to install Fedora onto your computer system using
   the graphical installation program.

Troubleshooting
   This option leads to a menu with several additional boot options.

If no key is hit within 60 seconds, the default boot option runs. To choose the default, either wait for
the timer to run out or hit Enter on the keyboard. To choose another option, use the arrow keys on
your keyboard and hit Enter when Troubleshooting is highlighted. If you want to customize the boot
options for a particular option, press the Tab key. To access the boot: prompt at which you can
specify custom boot options, press the Esc key and refer to Section 7.1.3, “Additional Boot Options”.

![Image of the boot screen]

Figure 7.1. The boot screen

For a listing and explanation of common boot options, refer to Chapter 11, Boot Options.

The boot options in the Troubleshooting menu are:

Install Fedora in basic graphics mode
   This option allows you to install Fedora in graphical mode even if the installation program is unable
   to load the correct driver for your video card. If your screen appears distorted or goes blank when
   using the Install or upgrade an existing system option, restart your computer and try this option
   instead.
Rescue a Fedora system
Choose this option to repair a problem with your installed Fedora system that prevents you from booting normally. Although Fedora is an exceptionally stable computing platform, it is still possible for occasional problems to occur that prevent booting. The rescue environment contains utility programs that allow you to fix a wide variety of these problems.

Run a memory test
This option runs an exhaustive test on the memory on your system. For more information, refer to Section 11.6.1, “Loading the Memory (RAM) Testing Mode”.

Boot from local drive
This option boots the system from the first installed disk. If you booted this disc accidentally, use this option to boot from the hard disk immediately without starting the installer.

7.1.3. Additional Boot Options

While it is easiest to boot using a DVD and perform a graphical installation, sometimes there are installation scenarios where booting in a different manner may be needed. This section discusses additional boot options available for Fedora.

To pass options to the boot loader on an x86, AMD64, or Intel 64 system, press the Esc key at boot time. The boot: prompt appears, at which you can use the boot loader options described below.

Refer to Chapter 8, Configuring Installation Source for boot options to specify your installation source, or to Chapter 11, Boot Options for additional boot options not covered in this section.

- To perform a text mode installation, at the installation boot prompt, type:

  ```bash
  linux text
  ```

- ISO images have an SHA256 checksum embedded in them. To test the checksum integrity of an ISO image, at the installation boot prompt, type:

  ```bash
  linux mediacheck
  ```

The installation program prompts you to insert a DVD or select an ISO image to test, and select OK to perform the checksum operation. This checksum operation can be performed on any Fedora DVD. It is strongly recommended to perform this operation on any Fedora DVD that was created from downloaded ISO images. This command works with the DVD, hard drive ISO, and NFS ISO installation methods.

- If you need to perform the installation in serial mode, type the following command:

  ```bash
  linux console=<device>
  ```

For text mode installations, use:

```bash
linux text console=<device>
```
In the above command, \texttt{<device>} should be the device you are using (such as ttyS0 or ttyS1). For example, \texttt{linux text console=TTYS0}.

Text mode installations using a serial terminal work best when the terminal supports UTF-8. Under UNIX and Linux, Kermit supports UTF-8. For Windows, Kermit '95 works well. Non-UTF-8 capable terminals work as long as only English is used during the installation process. An enhanced serial display can be used by passing the \texttt{utf8} command as a boot-time option to the installation program. For example:

\begin{verbatim}
linux console=TTYS0 utf8
\end{verbatim}

\subsection*{7.1.3.1. Kernel Options}

Options can also be passed to the kernel. For example, to apply updates for the \texttt{anaconda} installation program from a USB storage device enter:

\begin{verbatim}
linux updates
\end{verbatim}

For text mode installations, use:

\begin{verbatim}
linux text updates
\end{verbatim}

This command results in a prompt for the path to the device that contains updates for \texttt{anaconda}. It is not needed if you are performing a network installation and have already placed the updates image contents in \texttt{rhupdates/} on the server.

After entering any options, press \texttt{Enter} to boot using those options.

If you need to specify boot options to identify your hardware, please write them down. The boot options are needed during the boot loader configuration portion of the installation (refer to Section 9.16, \textit{"x86, AMD64, and Intel 64 Boot Loader Configuration"} for more information).

For more information on kernel options refer to Chapter 11, Boot Options.

\section*{7.2. Booting from the Network using PXE}

To boot with PXE, you need a properly configured server, and a network interface in your computer that supports PXE. For information on how to configure a PXE server, refer to Chapter 13, Setting Up an Installation Server.

Configure the computer to boot from the network interface. This option is in the BIOS, and may be labeled \texttt{Network Boot} or \texttt{Boot Services}. Once you properly configure PXE booting, the computer can boot the Fedora installation system without any other media.

To boot a computer from a PXE server:

1. Ensure that the network cable is attached. The link indicator light on the network socket should be lit, even if the computer is not switched on.

2. Switch on the computer.
3. A menu screen appears. Press the number key that corresponds to the desired option.

If your PC does not boot from the netboot server, ensure that the BIOS is configured to boot first from the correct network interface. Some BIOS systems specify the network interface as a possible boot device, but do not support the PXE standard. Refer to your hardware documentation for more information.

**Note — Multiple NICs and PXE installation**

Some servers with multiple network interfaces might not assign eth0 to the first network interface as the firmware interface knows it, which can cause the installer to try to use a different network interface from the one that was used by PXE. To change this behavior, use the following in `pxelinux.cfg/*` config files:

```
IPAPPEND 2
APPEND ksdevice=bootif
```

These configuration options above cause the installer to use the same network interface the firmware interface and PXE use. You can also use the following option:

```
ksdevice=link
```

This option causes the installer to use the first network device it finds that is linked to a network switch.
Configuring Installation Source
Before the graphical installation program starts, you may need to configure the installation source depending on the method you are using.

8.1. Installation Method

If you are installing from DVD, additional configuration will not be required unless the DVD drive is not detected. If you booted the installation from minimal boot media, use a boot prompt to select an installation method.

8.1.1. Installing from DVD

To install Fedora from a DVD, place the DVD in your DVD drive and boot your system from the DVD. Even if you booted from alternative media, you can still install Fedora from DVD media.

The installation program then probes your system and attempts to identify your DVD drive. It starts by looking for an IDE (also known as an ATAPI) DVD drive.

Note

To abort the installation process at this time, reboot your machine and then eject the boot media. You can safely cancel the installation at any point before the Write changes to disk screen. Refer to Section 9.15, “Write changes to disk” for more information.

If your DVD drive is not detected, and it is a SCSI DVD, the installation program prompts you to choose a SCSI driver. Choose the driver that most closely resembles your adapter. You may specify options for the driver if necessary; however, most drivers detect your SCSI adapter automatically.

If you booted the installer from other media and wish to use a DVD as your installation source, use the following boot option:

```
linux repo=cdrom:device
```

If you later encounter problems with the installer, you should reboot and perform the media check by running the boot option `linux mediacheck` before seeking support.

8.1.2. Installing from a Hard Drive

To specify a partition from which to install Fedora, use the `linux repo=` boot option:

```
linux repo=hd:device
```
Chapter 8. Configuring Installation Source

Select the partition containing the ISO files from the list of available partitions. Internal IDE, SATA, SCSI, and USB drive device names begin with \texttt{/dev/sd}. Each individual drive has its own letter, for example \texttt{/dev/sda}. Each partition on a drive is numbered, for example \texttt{/dev/sda1}.

Also specify the full directory path from the drive that contains the ISO image files. The following table shows some examples of how to enter this information:

<table>
<thead>
<tr>
<th>Partition type</th>
<th>Volume</th>
<th>Original path to files</th>
<th>Directory to use</th>
</tr>
</thead>
<tbody>
<tr>
<td>VFAT</td>
<td>D:\</td>
<td>D:\Downloads \Fedora17</td>
<td>/Downloads/Fedora17</td>
</tr>
<tr>
<td>ext2, ext3, ext4</td>
<td>/home</td>
<td>/home/user1/Fedora17</td>
<td>/user1/Fedora17</td>
</tr>
</tbody>
</table>

If the ISO images are in the root (top-level) directory of a partition, enter a \texttt{/}. If the ISO images are located in a subdirectory of a mounted partition, enter the name of the directory holding the ISO images within that partition. For example, if the partition on which the ISO images is normally mounted as \texttt{/home/}, and the images are in \texttt{/home/new/}, you would enter \texttt{/new/}.

\textbf{Use a leading slash}

An entry without a leading slash may cause the installation to fail.

After entering the \texttt{linux repo=} boot command, proceed with \textit{Chapter 9, Installing using anaconda}.

8.1.3. Installing via NFS

To specify an installation source for Fedora accessible by NFS, use the \texttt{linux repo=} boot option. To specify an expanded tree of installation files, type:

\begin{verbatim}
linux repo=nfs:options:server:/path
\end{verbatim}

To specify an ISO image file, type:

\begin{verbatim}
linux repo=nfsiso:options:server:/path
\end{verbatim}

- \texttt{options} — specify any NFS mount options that you require. Refer to the man pages for \texttt{mount} and \texttt{nfs} for a comprehensive list of options.

- \texttt{server} — enter the domain name or IP address of your NFS server. For example, if you are installing from a host named \texttt{eastcoast} in the domain \texttt{example.com}, enter \texttt{eastcoast.example.com}.

- \texttt{path} — the path to the exported directory.

  - If the NFS server is exporting a mirror of the Fedora installation tree, enter the directory which contains the root of the installation tree.

  - If the NFS server is exporting the ISO image of the Fedora DVD, enter the directory which contains the ISO image.
If you followed the setup described in Section 5.1.2, “Preparing for an NFS installation”, the exported directory is the one that you specified as `publicly_available_directory`.

After entering the `linux repo=` command, proceed with Chapter 9, Installing using anaconda.

### 8.1.4. Installing via FTP or HTTP

**Important — you must specify the protocol**

When you provide a URL to an installation source, you must explicitly specify `http://` or `ftp://` as the protocol.

To specify an installation source for Fedora that is available over the Internet, use the `linux repo=` boot option:

```
linux repo={ftp|http}://URL
```

For `URL`, enter the name or IP address of the FTP or HTTP site from which you are installing, and the name of the directory that contains the `/images` directory for your architecture. For example:

http://name.example.com/mirrors/fedora/F-17/Server/i386/

If your FTP or HTTP server requires user authentication, specify user and password as part of the URL as follows:

```
{ftp|http}://<user>:<password>@<hostname>[:<port>]/<directory>/
```

For example:

http://install:fedora17pw@name.example.com/mirrors/fedora/F-17/Server/i386/

After entering the `linux repo=` command, proceed with Chapter 9, Installing using anaconda.
Installing using anaconda

This chapter describes an installation using the graphical user interface of anaconda.

9.1. The Text Mode Installation Program User Interface

Important — Graphical installation recommended

We recommend that you install Fedora using the graphical interface. If you are installing Fedora on a system that lacks a graphical display, consider performing the installation over a VNC connection – see Chapter 14, Installing Through VNC. If anaconda detects that you are installing in text mode on a system where installation over a VNC connection might be possible, anaconda asks you to verify your decision to install in text mode even though your options during installation are limited.

If your system has a graphical display, but graphical installation fails, try booting with the xdriver=vesa option – refer to Chapter 11, Boot Options

Important — Graphical Interface on the Installed System

Installing in text mode does not prevent you from using a graphical interface on your system once it is installed.

Apart from the graphical installer, anaconda also includes a text-based installer.

If one of the following situations occurs, the installation program uses text mode:

• The installation system fails to identify the display hardware on your computer
• You choose the text mode installation by entering the following command at the boot: prompt

```
linux text
```

While text mode installations are not explicitly documented, those using the text mode installation program can easily follow the GUI installation instructions. However, because text mode presents you with a simpler, more streamlined installation process, certain options that are available in graphical mode are not also available in text mode. These differences are noted in the description of the installation process in this guide, and include:

• configuring advanced storage methods such as LVM, RAID, FCoE, zFCP, and iSCSI.
• customizing the partition layout
• customizing the bootloader layout
• selecting packages during installation
Chapter 9. Installing using anaconda

- configuring the installed system with firstboot

If you choose to install Fedora in text mode, you can still configure your system to use a graphical interface after installation. Refer to Section 18.3, “Switching to a Graphical Login” for instructions.

To configure options not available in text mode, consider using a boot option. For example, the `linux ip` option can be used to configure network settings. Refer to Section 11.1, “Configuring the Installation System at the Boot Menu” for instructions.

**Note**

Not every language supported in graphical installation mode is also supported in text mode. Specifically, languages written with a character set other than the Latin or Cyrillic alphabets are not available in text mode. If you choose a language written with a character set that is not supported in text mode, the installation program will present you with the English versions of the screens.

### 9.1.1. Using the Keyboard to Navigate

Navigation through the installation dialogs is performed through a simple set of keystrokes. To move the cursor, use the Left, Right, Up, and Down arrow keys. Use Tab, and Shift-Tab to cycle forward or backward through each widget on the screen. Along the bottom, most screens display a summary of available cursor positioning keys.

To "press" a button, position the cursor over the button (using Tab, for example) and press Space or Enter. To select an item from a list of items, move the cursor to the item you wish to select and press Enter. To select an item with a checkbox, move the cursor to the checkbox and press Space to select an item. To deselect, press Space a second time.

Pressing F12 accepts the current values and proceeds to the next dialog; it is equivalent to pressing the OK button.

**Warning**

Unless a dialog box is waiting for your input, do not press any keys during the installation process (doing so may result in unpredictable behavior).

### 9.2. The Graphical Installation Program User Interface

If you have used a graphical user interface (GUI) before, you are already familiar with this process; use your mouse to navigate the screens, click buttons, or enter text fields.

You can also navigate through the installation using the keyboard. The Tab key allows you to move around the screen, the Up and Down arrow keys to scroll through lists, + and - keys expand and collapse lists, while Space and Enter selects or removes from selection a highlighted item. You can also use the Alt+X key command combination as a way of clicking on buttons or making other screen selections, where X is replaced with any underlined letter appearing within that screen.
9.2.1. Screenshots during installation

Anaconda allows you to take screenshots during the installation process. At any time during installation, press Shift+Print Screen and anaconda will save a screenshot to /root/anaconda-screenshots.

If you are performing a Kickstart installation, use the autostep --autoscreenshot option to generate a screenshot of each step of the installation automatically. Refer to Section 15.3, "Creating the Kickstart File" for details of configuring a Kickstart file.

9.2.2. A Note about Virtual Consoles

The Fedora installation program offers more than the dialog boxes of the installation process. Several kinds of diagnostic messages are available to you, as well as a way to enter commands from a shell prompt. The installation program displays these messages on five virtual consoles, among which you can switch using a single keystroke combination.

A virtual console is a shell prompt in a non-graphical environment, accessed from the physical machine, not remotely. Multiple virtual consoles can be accessed simultaneously.

These virtual consoles can be helpful if you encounter a problem while installing Fedora. Messages displayed on the installation or system consoles can help pinpoint a problem. Refer to Table 9.1, "Console, Keystrokes, and Contents" for a listing of the virtual consoles, keystrokes used to switch to them, and their contents.

Generally, there is no reason to leave the default console (virtual console #6) for graphical installations unless you are attempting to diagnose installation problems.

<table>
<thead>
<tr>
<th>console</th>
<th>keystrokes</th>
<th>contents</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ctrl+alt+f1</td>
<td>graphical display</td>
</tr>
<tr>
<td>2</td>
<td>Ctrl+alt+f2</td>
<td>shell prompt</td>
</tr>
<tr>
<td>3</td>
<td>Ctrl+alt+f3</td>
<td>install log (messages from installation program)</td>
</tr>
<tr>
<td>4</td>
<td>Ctrl+alt+f4</td>
<td>system-related messages</td>
</tr>
<tr>
<td>5</td>
<td>Ctrl+alt+f5</td>
<td>other messages</td>
</tr>
</tbody>
</table>

9.3. Language Selection

Using your mouse, select the language (for example, U.S. English) you would prefer to use for the installation and as the system default (refer to the figure below).

Once you have made your selection, click Next to continue.
Figure 9.1. Language Configuration

9.4. Keyboard Configuration

Using your mouse, select the correct layout type (for example, U.S. English) for the keyboard you would prefer to use for the installation and as the system default (refer to the figure below).

Once you have made your selection, click **Next** to continue.
Fedora includes support for more than one keyboard layout for many languages. In particular, most European languages include a \texttt{latin1} option, which uses \textit{dead keys} to access certain characters, such as those with diacritical marks. When you press a dead key, nothing will appear on your screen until you press another key to “complete” the character. For example, to type \texttt{é} on a latin1 keyboard layout, you would press (and release) the \' key, and then press the \texttt{E} key. By contrast, you access this character on some other keyboards by pressing and holding down a key (such as \texttt{Alt-Gr}) while you press the \texttt{E} key. Other keyboards might have a dedicated key for this character.

\textbf{Note}

To change your keyboard layout type after you have completed the installation, use the \texttt{Keyboard Configuration Tool}.

Type the \texttt{system-config-keyboard} command in a shell prompt to launch the \texttt{Keyboard Configuration Tool}. If you are not root, it prompts you for the root password to continue.

### 9.5. Storage Devices

You can install Fedora on a large variety of storage devices. This screen allows you to select either basic or specialized storage devices.
Chapter 9. Installing using anaconda

What type of devices will your installation involve?

**Basic Storage Devices**
- Installs or upgrades to typical types of storage devices. If you're not sure which option is right for you, this is probably it.

**Specialized Storage Devices**
- Installs or upgrades to devices such as Storage Area Networks (SANs) or mainframe attached disks (DASDs), usually in an enterprise environment.

---

**Figure 9.3. Storage devices**

Basic Storage Devices

Select **Basic Storage Devices** to install Fedora on the following storage devices:

- hard drives or solid-state drives connected directly to the local system.

Specialized Storage Devices

Select **Specialized Storage Devices** to install Fedora on the following storage devices:

- *Storage area networks* (SANs)
- *Direct access storage devices* (DASDs)
- Firmware RAID devices
- Multipath devices

Use the **Specialized Storage Devices** option to configure *Internet Small Computer System Interface* (iSCSI) and FCoE (Fiber Channel over Ethernet) connections.

If you select **Basic Storage Devices**, **anaconda** automatically detects the local storage attached to the system and does not require further input from you. Proceed to **Section 9.6, “Setting the Hostname”**.

---

**9.5.1. The Storage Devices Selection Screen**

The storage devices selection screen displays all storage devices to which **anaconda** has access.
The Storage Devices Selection Screen

**Figure 9.4. Select storage devices — Basic devices**

Please select the drives you'd like to install the operating system on, as well as any drives you'd like to automatically mount to your system, below:

![Image of Basic Devices screen](image1)

0 device(s) (0 MB) selected out of 1 device(s) (20480 MB) total.

**Tip:** Selecting a drive on this screen does not necessarily mean it will be wiped by the installation process. Also, note that post-installation you may mount drives you did not select here by modifying your /etc/fstab file.

---

**Figure 9.5. Select storage devices — Multipath Devices**

Please select the drives you'd like to install the operating system on, as well as any drives you'd like to automatically mount to your system, below:

![Image of Multipath Devices screen](image2)

0 device(s) (0 MB) selected out of 4 device(s) (21078 MB) total.

**Tip:** Selecting a drive on this screen does not necessarily mean it will be wiped by the installation process. Also, note that post-installation you may mount drives you did not select here by modifying your /etc/fstab file.
Chapter 9. Installing using anaconda

Figure 9.6. Select storage devices — Other SAN Devices

Devices are grouped under the following tabs:

Basic Devices
Basic storage devices directly connected to the local system, such as hard disk drives and solid-state drives.

Firmware RAID
Storage devices attached to a firmware RAID controller.

Multipath Devices
Storage devices accessible through more than one path, such as through multiple SCSI controllers or Fiber Channel ports on the same system.

Important — device serial numbers must be 16 or 32 characters

The installer only detects multipath storage devices with serial numbers that are 16 or 32 characters in length.

Other SAN Devices
Any other devices available on a storage area network (SAN).

If you do need to configure iSCSI or FCoE storage, click Add Advanced Target and refer to Section 9.5.1.1, “Advanced Storage Options”.

To assign non-friendly multipath device names, click Device Options and uncheck Use friendly names for multipath devices.
The storage devices selection screen also contains a **Search** tab that allows you to filter storage devices either by their World Wide Identifier (WWID) or by the port, target, or logical unit number (LUN) at which they are accessed.

![Figure 9.7. The Storage Devices Search Tab](image)

The tab contains a drop-down menu to select searching by port, target, WWID, or LUN (with corresponding text boxes for these values). Searching by WWID or LUN requires additional values in the corresponding text box.

Each tab presents a list of devices detected by **anaconda**, with information about the device to help you to identify it. A small drop-down menu marked with an icon is located to the right of the column headings. This menu allows you to select the types of data presented on each device. For example, the menu on the **Multipath Devices** tab allows you to specify any of **WWID**, **Capacity**, **Vendor**, **Interconnect**, and **Paths** to include among the details presented for each device. Reducing or expanding the amount of information presented might help you to identify particular devices.

![Figure 9.8. Selecting Columns](image)

Each device is presented on a separate row, with a checkbox to its left. Click the checkbox to make a device available during the installation process, or click the **radio button** at the left of the column headings to select or deselect all the devices listed in a particular screen. Later in the installation process, you can choose to install Fedora onto any of the devices selected here, and can choose to automatically mount any of the other devices selected here as part of the installed system.

Note that the devices that you select here are not automatically erased by the installation process. Selecting a device on this screen does not, in itself, place data stored on the device at risk. Note also that any devices that you do not select here to form part of the installed system can be added to the system after installation by modifying the `/etc/fstab` file.

**Important — chain loading**

Any storage devices that you do not select on this screen are hidden from **anaconda** entirely. To **chain load** the Fedora boot loader from a different boot loader, select all the devices presented in this screen.

when you have selected the storage devices to make available during installation, click **Next** and proceed to **Section 9.10, “Initializing the Hard Disk”**
Chapter 9. Installing using anaconda

9.5.1.1. Advanced Storage Options

From this screen you can configure an iSCSI (SCSI over TCP/IP) target or FCoE (Fibre channel over ethernet) SAN (storage area network). Refer to Appendix B, ISCSI disks for an introduction to iSCSI.

![Advanced Storage Options](image)

**9.5.1.1.1. Select and configure a network interface**

If a network interface is not already active on the system, anaconda must activate one through which to connect to the storage devices. If your system has only a single network interface, anaconda automatically activates it. However, if your system has more than one network interface available, anaconda prompts you with the Select network interface dialog to choose one to use during installation.

![Select network interface](image)

1. Select an interface from the drop-down menu.
2. Click **OK**.

Anaconda activates the interface that you selected, then starts NetworkManager to allow you to configure the interface.
9.5.1.1.2. Configure iSCSI parameters

To use iSCSI storage devices for the installation, anaconda must be able to discover them as iSCSI targets and be able to create an iSCSI session to access them. Each of these steps might require a username and password for CHAP (Challenge Handshake Authentication Protocol) authentication. Additionally, you can configure an iSCSI target to authenticate the iSCSI initiator on the system to which the target is attached (reverse CHAP), both for discovery and for the session. Used together, CHAP and reverse CHAP are called mutual CHAP or two-way CHAP. Mutual CHAP provides the greatest level of security for iSCSI connections, particularly if the username and password are different for CHAP authentication and reverse CHAP authentication.

Repeat the iSCSI discovery and iSCSI login steps as many times as necessary to add all required iSCSI storage. However, you cannot change the name of the iSCSI initiator after you attempt discovery for the first time. To change the iSCSI initiator name, you must restart the installation.

Procedure 9.1. iSCSI discovery

Use the iSCSI Discovery Details dialog to provide anaconda with the information that it needs to discover the iSCSI target.
1. Enter the IP address of the iSCSI target in the **Target IP Address** field.

2. Provide a name in the **iSCSI Initiator Name** field for the iSCSI initiator in *iSCSI qualified name* (IQN) format.

   A valid IQN contains:

   - the string `iqn.` (note the period)
   - a date code that specifies the year and month in which your organization's Internet domain or subdomain name was registered, represented as four digits for the year, a dash, and two digits for the month, followed by a period. For example, represent September 2010 as 2010-09.
   - your organization's Internet domain or subdomain name, presented in reverse order with the top-level domain first. For example, represent the subdomain `storage.example.com` as `com.example.storage`
   - a colon followed by a string that uniquely identifies this particular iSCSI initiator within your domain or subdomain. For example, `:diskarrays-sn-a8675309`.

   A complete IQN therefore resembles: **iqn.2010-09.storage.example.com:diskarrays-sn-a8675309**, and *anaconda* pre-populates the **iSCSI Initiator Name** field with a name in this format to help you with the structure.

3. Use the drop-down menu to specify the type of authentication to use for iSCSI discovery:

- no credentials
- CHAP pair
- CHAP pair and a reverse pair
4. If you selected CHAP pair as the authentication type, provide the username and password for the iSCSI target in the **CHAP Username** and **CHAP Password** fields.

![Figure 9.14. CHAP pair](image)

If you selected **CHAP pair and a reverse pair** as the authentication type, provide the username and password for the iSCSI target in the **CHAP Username** and **CHAP Password** fields.
field and the username and password for the iSCSI initiator in the **Reverse CHAP Username** and **Reverse CHAP Password** fields.

![iSCSI Discovery Details](image)

**Figure 9.15. CHAP pair and a reverse pair**

5. Click **Start Discovery**. **Anaconda** attempts to discover an iSCSI target based on the information that you provided. If discovery succeeds, the **iSCSI Discovered Nodes** dialog presents you with a list of all the iSCSI nodes discovered on the target.
6. Each node is presented with a checkbox beside it. Click the checkboxes to select the nodes to use for installation.

![Figure 9.16. The iSCSI Discovered Nodes dialog](image)

7. Click Login to initiate an iSCSI session.

**Procedure 9.2. Starting an iSCSI session**

Use the iSCSI Nodes Login dialog to provide anaconda with the information that it needs to log into the nodes on the iSCSI target and start an iSCSI session.

![Figure 9.17. The iSCSI Nodes Login dialog](image)
1. Use the drop-down menu to specify the type of authentication to use for the iSCSI session:

- no credentials
- CHAP pair
- CHAP pair and a reverse pair
- Use the credentials from the discovery step

If your environment uses the same type of authentication and same username and password for iSCSI discovery and for the iSCSI session, select **Use the credentials from the discovery step** to reuse these credentials.

2. If you selected **CHAP pair** as the authentication type, provide the username and password for the iSCSI target in the **CHAP Username** and **CHAP Password** fields.
fields and the username and password for the iSCSI initiator in the Reverse CHAP Username and Reverse CHAP Password fields.

3. Click Login. Anaconda attempts to log into the nodes on the iSCSI target based on the information that you provided. The iSCSI Login Results dialog presents you with the results.

4. Click OK to continue.

9.5.1.1.3. Configure FCoE Parameters
To configure an FCoE SAN, select Add FCoE SAN and click Add Drive.

On the menu that appears in the next dialog box, select the network interface that is connected to your FCoE switch and click Add FCoE Disk(s).
Data Center Bridging (DCB) is a set of enhancements to the Ethernet protocols designed to increase the efficiency of Ethernet connections in storage networks and clusters. Enable or disable the installer's awareness of DCB with the checkbox in this dialog.

9.6. Setting the Hostname

Setup prompts you to supply a host name for this computer, either as a fully-qualified domain name (FQDN) in the format hostname.domainname or as a short host name in the format hostname. Many networks have a Dynamic Host Configuration Protocol (DHCP) service that automatically supplies connected systems with a domain name. To allow the DHCP service to assign the domain name to this machine, specify the short host name only.

Valid Hostnames

You may give your system any name provided that the full hostname is unique. The hostname may include letters, numbers and hyphens. Various programs provided by the Fedora distribution may prefer or require a FQDN as opposed to a short host name.
If your Fedora system is connected directly to the Internet, you must pay attention to additional considerations to avoid service interruptions or risk action by your upstream service provider. A full discussion of these issues is beyond the scope of this document.

**Modem Configuration**

The installation program does not configure modems. Configure these devices after installation with the **Network** utility. The settings for your modem are specific to your particular Internet Service Provider (ISP).

### 9.6.1. Edit Network Connections

**Important — Manual configuration is often needed**

When a Fedora 17 installation boots for the first time, it activates any network interfaces that you configured during the installation process. However, the installer does not prompt you to configure network interfaces on some common installation paths, for example, when you install Fedora from a DVD to a local hard drive.

When you install Fedora from a local installation source to a local storage device, be sure to configure at least one network interface manually if you require network access when the system boots for the first time.
To change your network configuration after you have completed the installation, use the **Network Administration Tool**.

Type the `system-config-network` command in a shell prompt to launch the **Network Administration Tool**. If you are not root, it prompts you for the root password to continue.

To configure a network connection manually, click the button **Configure Network**. The **Network Connections** dialog appears that allows you to configure wired, wireless, mobile broadband, VPN, and DSL connections for the system using the **NetworkManager** tool. A full description of all configurations possible with **NetworkManager** is beyond the scope of this guide. This section only details the most typical scenario of how to configure wired connections during installation. Configuration of other types of network is broadly similar, although the specific parameters that you must configure are necessarily different.

![Network Connections](image)

**Figure 9.24. Network Connections**

To add a new connection or to modify or remove a connection configured earlier in the installation process, click the tab that corresponds to the type of connection. To add a new connection of that type, click **Add**. To modify an existing connection, select it in the list and click **Edit**. In either case, a dialog box appears with a set of tabs that is appropriate to the particular connection type, as described below. To remove a connection, select it in the list and click **Delete**.

When you have finished editing network settings, click **Apply** to save the new configuration. If you reconfigured a device that was already active during installation, you must restart the device to use the new configuration — refer to **Section 9.6.1.6, “Restart a network device”**.
9.6.1.1. Options common to all types of connection

Certain configuration options are common to all connection types.

Specify a name for the connection in the **Connection name** name field.

Select **Start automatically** to start the connection automatically when the system boots.

When **NetworkManager** runs on an installed system, the **Available to all users** option controls whether a network configuration is available system-wide or not. During installation, ensure that **Available to all users** remains selected for any network interface that you configure.

9.6.1.2. The Wired tab

Use the **Wired** tab to specify or change the **media access control** (MAC) address for the network adapter, and either set the **maximum transmission unit** (MTU, in bytes) that can pass through the interface.
9.6.1.3. The 802.1x Security tab
Use the 802.1x Security tab to configure 802.1X port-based network access control (PNAC). Select Use 802.1X security for this connection to enable access control, then specify details of your network. The configuration options include:

Authentication
Choose one of the following methods of authentication:

- **TLS** for *Transport Layer Security*
- **Tunneled TLS** for *Tunneled Transport Layer Security*, otherwise known as TTLS, or EAP-TTLS
Chapter 9. Installing using anaconda

- **Protected EAP (PEAP)** for Protected Extensible Authentication Protocol

**Identity**
Provide the identity of this server.

**User certificate**
Browse to a personal X.509 certificate file encoded with *Distinguished Encoding Rules* (DER) or *Privacy Enhanced Mail* (PEM).

**CA certificate**
Browse to a X.509 certificate authority certificate file encoded with *Distinguished Encoding Rules* (DER) or *Privacy Enhanced Mail* (PEM).

**Private key**
Browse to a private key file encoded with *Distinguished Encoding Rules* (DER), *Privacy Enhanced Mail* (PEM), or the *Personal Information Exchange Syntax Standard* (PKCS#12).

**Private key password**
The password for the private key specified in the **Private key** field. Select *Show password* to make the password visible as you type it.
9.6.1.4. The IPv4 Settings tab

Use the IPv4 Settings tab to configure the IPv4 parameters for the previously selected network connection.

Use the Method drop-down menu to specify which settings the system should attempt to obtain from a Dynamic Host Configuration Protocol (DHCP) service running on the network. Choose from the following options:

**Automatic (DHCP)**

IPv4 parameters are configured by the DHCP service on the network.
Chapter 9. Installing using anaconda

Automatic (DHCP) addresses only
The IPv4 address, netmask, and gateway address are configured by the DHCP service on the network, but DNS servers and search domains must be configured manually.

Manual
IPv4 parameters are configured manually for a static configuration.

Link-Local Only
A link-local address in the 169.254/16 range is assigned to the interface.

Shared to other computers
The system is configured to provide network access to other computers. The interface is assigned an address in the 10.42.x.1/24 range, a DHCP server and DNS server are started, and the interface is connected to the default network connection on the system with network address translation (NAT).

Disabled
IPv4 is disabled for this connection.

If you selected a method that requires you to supply manual parameters, enter details of the IP address for this interface, the netmask, and the gateway in the Addresses field. Use the Add and Delete buttons to add or remove addresses. Enter a comma-separated list of DNS servers in the DNS servers field, and a comma-separated list of domains in the Search domains field for any domains that you want to include in name server lookups.

Optionally, enter a name for this network connection in the DHCP client ID field. This name must be unique on the subnet. When you assign a meaningful DHCP client ID to a connection, it is easy to identify this connection when troubleshooting network problems.

Deselect the Require IPv4 addressing for this connection to complete check box to allow the system to make this connection on an IPv6-enabled network if IPv4 configuration fails but IPv6 configuration succeeds.
9.6.1.4.1. Editing IPv4 routes
Fedora configures a number of routes automatically based on the IP addresses of a device. To edit additional routes, click the *Routes* button. The *Editing IPv4 routes* dialog appears.
Chapter 9. Installing using anaconda

Click **Add** to add the IP address, netmask, gateway address, and metric for a new static route.

Select **Ignore automatically obtained routes** to make the interface use only the routes specified for it here.

Select **Use this connection only for resources on its network** to restrict connections only to the local network.

### 9.6.1.5. The IPv6 Settings tab

Use the **IPv6 Settings tab** to configure the IPv6 parameters for the previously selected network connection.

Use the **Method** drop-down menu to specify which settings the system should attempt to obtain from a Dynamic Host Configuration Protocol (DHCP) service running on the network. Choose from the following options:

**Ignore**
IPv6 is ignored for this connection.

**Automatic**
NetworkManager uses router advertisement (RA) to create an automatic, stateless configuration.

**Automatic, addresses only**
NetworkManager uses RA to create an automatic, stateless configuration, but DNS servers and search domains are ignored and must be configured manually.

**Automatic, DHCP only**
NetworkManager does not use RA, but requests information from DHCPv6 directly to create a stateful configuration.

**Manual**
IPv6 parameters are configured manually for a static configuration.
Link-Local Only

A link-local address with the fe80::/10 prefix is assigned to the interface.

If you selected a method that requires you to supply manual parameters, enter details of the IP address for this interface, the netmask, and the gateway in the Addresses field. Use the Add and Delete buttons to add or remove addresses. Enter a comma-separated list of DNS servers in the DNS servers field, and a comma-separated list of domains in the Search domains field for any domains that you want to include in name server lookups.

Optionally, enter a name for this network connection in the DHCP client ID field. This name must be unique on the subnet. When you assign a meaningful DHCP client ID to a connection, it is easy to identify this connection when troubleshooting network problems.

Deselect the Require IPv6 addressing for this connection to complete check box to allow the system to make this connection on an IPv4-enabled network if IPv6 configuration fails but IPv4 configuration succeeds.
Figure 9.29. The IPv6 Settings tab

9.6.1.5.1. Editing IPv6 routes
Fedora configures a number of routes automatically based on the IP addresses of a device. To edit additional routes, click the Routes button. The Editing IPv6 routes dialog appears.
Click **Add** to add the IP address, netmask, gateway address, and metric for a new static route.

Select **Use this connection only for resources on its network** to restrict connections only to the local network.

### 9.6.1.6. Restart a network device

If you reconfigured a network that was already in use during installation, you must disconnect and reconnect the device in **anaconda** for the changes to take effect. **Anaconda** uses *interface configuration* (*ifcfg*) files to communicate with **NetworkManager**. A device becomes disconnected when its *ifcfg* file is removed, and becomes reconnected when its *ifcfg* file is restored, as long as **ONBOOT=yes** is set. Refer to the **Fedora Deployment Guide** available from [http://docs.fedoraproject.org/en-US/index.html](http://docs.fedoraproject.org/en-US/index.html) for more information about interface configuration files.

1. Press **Ctrl+Alt+F2** to switch to virtual terminal **tty2**.

2. Move the interface configuration file to a temporary location:

   ```sh
mv /etc/sysconfig/network-scripts/ifcfg-device_name /tmp
   ```

   where *device_name* is the device that you just reconfigured. For example, **ifcfg-eth0** is the *ifcfg* file for eth0.

   The device is now disconnected in **anaconda**.

3. Open the interface configuration file in the **vi** editor:

   ```sh
   vi /tmp/ifcfg-device_name
   ```

4. Verify that the interface configuration file contains the line **ONBOOT=yes**. If the file does not already contain the line, add it now and save the file.
5. Exit the `vi` editor.

6. Move the interface configuration file back to the `/etc/sysconfig/network-scripts/` directory:

   ```bash
   mv /tmp/ifcfg-device_name /etc/sysconfig/network-scripts/
   ```

   The device is now reconnected in `anaconda`.

7. Press `Ctrl+Alt+F6` to return to `anaconda`.

### 9.7. Time Zone Configuration

Set your time zone by selecting the city closest to your computer’s physical location. Click on the map to zoom in to a particular geographical region of the world.

Specify a time zone even if you plan to use NTP (Network Time Protocol) to maintain the accuracy of the system clock.

From here there are two ways for you to select your time zone:

- Using your mouse, click on the interactive map to select a specific city (represented by a yellow dot). A red X appears indicating your selection.
- You can also scroll through the list at the bottom of the screen to select your time zone. Using your mouse, click on a location to highlight your selection.

![Figure 9.31. Configuring the Time Zone](image)

If Fedora is the only operating system on your computer, select **System clock uses UTC**. The system clock is a piece of hardware on your computer system. Fedora uses the timezone setting to determine
the offset between the local time and UTC on the system clock. This behavior is standard for systems that use UNIX, Linux, and similar operating systems.

Click **Next** to proceed.

---

### Windows and the System Clock

Do not enable the **System clock uses UTC** option if your machine also runs Microsoft Windows. Microsoft operating systems change the BIOS clock to match local time rather than UTC. This may cause unexpected behavior under Fedora unless you have manually configured Windows 7 to use UTC.

---

#### Note

To change your time zone configuration after you have completed the installation, use the **Time and Date Properties Tool**.

Type the `system-config-date` command in a shell prompt to launch the **Time and Date Properties Tool**. If you are not root, it prompts you for the root password to continue.

To run the **Time and Date Properties Tool** as a text-based application, use the command `timeconfig`.

---

### 9.8. Set the Root Password

Setting up a root account and password is one of the most important steps during your installation. The root account is used to install packages, upgrade RPMs, and perform most system maintenance. Logging in as root gives you complete control over your system.

#### Note

The root user (also known as the superuser) has complete access to the entire system; for this reason, logging in as the root user is best done *only* to perform system maintenance or administration.
Chapter 9. Installing using anaconda

Figure 9.32. Root Password

Use the root account only for system administration. Create a non-root account for your general use and use the `su` command to change to root only when you need to perform tasks that require superuser authorization. These basic rules minimize the chances of a typo or an incorrect command doing damage to your system.

**Note**

To become root, type `su -` at the shell prompt in a terminal window and then press **Enter**. Then, enter the root password and press **Enter**.

The installation program prompts you to set a root password\(^1\) for your system. You cannot proceed to the next stage of the installation process without entering a root password.

The root password must be at least six characters long; the password you type is not echoed to the screen. You must enter the password twice; if the two passwords do not match, the installation program asks you to enter them again.

You should make the root password something you can remember, but not something that is easy for someone else to guess. Your name, your phone number, `qwerty`, `password`, `root`, 123456, and `anteater` are all examples of bad passwords. Good passwords mix numerals with upper and lower case letters and do not contain dictionary words: Aard387vark or 420BMttNT, for example. Remember that the password is case-sensitive. If you write down your password, keep it in a secure place. However, it is recommended that you do not write down this or any password you create.

---

\(^1\) A root password is the administrative password for your Fedora system. You should only log in as root when needed for system maintenance. The root account does not operate within the restrictions placed on normal user accounts, so changes made as root can have implications for your entire system.
Do not use one of the example passwords offered in this manual. Using one of these passwords could be considered a security risk.

To change your root password after you have completed the installation, use the **Root Password Tool**.

Type the `system-config-users` command in a shell prompt to launch the **User Manager**, a powerful user management and configuration tool. If you are not root, it prompts you for the root password to continue.

Enter the root password into the **Root Password** field. Fedora displays the characters as asterisks for security. Type the same password into the **Confirm** field to ensure it is set correctly. After you set the root password, select **Next** to proceed.

### 9.9. Assign Storage Devices

If you selected more than one storage device on the storage devices selection screen (refer to [Section 9.5, “Storage Devices”](#)), **anaconda** asks you to select which of these devices should be available for installation of the operating system, and which should only be attached to the file system for data storage. If you selected only one storage device, **anaconda** does not present you with this screen.

During installation, the devices that you identify here as being for data storage only are mounted as part of the file system, but are not partitioned or formatted.

Below are the storage devices you've selected to be a part of this installation. Please indicate using the arrows below which devices you'd like to use as data drives (these will not be formatted, only mounted) and which devices you'd like to use as system drives (these may be formatted).

<table>
<thead>
<tr>
<th>Model</th>
<th>Capacity</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATA HARDDISK</td>
<td>1024000 MB</td>
<td></td>
</tr>
<tr>
<td>ATA HARDDISK</td>
<td>1024000 MB</td>
<td></td>
</tr>
</tbody>
</table>

**Tip:** Install target devices will be reformatted and wiped of any data. Make sure you have backups.

![Figure 9.33. Assign storage devices](image)
The screen is split into two panes. The left pane contains a list of devices to be used for data storage only. The right pane contains a list of devices that are to be available for installation of the operating system.

Each list contains information about the devices to help you to identify them. A small drop-down menu marked with an icon is located to the right of the column headings. This menu allows you to select the types of data presented on each device. Reducing or expanding the amount of information presented might help you to identify particular devices.

Move a device from one list to the other by clicking on the device, then clicking either the button labeled with a left-pointing arrow to move it to the list of data storage devices or the button labeled with a right-pointing arrow to move it to the list of devices available for installation of the operating system.

The list of devices available as installation targets also includes a radio button beside each device. Use this radio button to specify the device that you want to use as the boot device for the system.

**Important — chain loading**

If any storage device contains a boot loader that will chain load the Fedora boot loader, include that storage device among the **Install Target Devices**. Storage devices that you identify as **Install Target Devices** remain visible to **anaconda** during boot loader configuration.

Storage devices that you identify as **Install Target Devices** on this screen are not automatically erased by the installation process unless you selected the **Use All Space** option on the partitioning screen (refer to Section 9.12, “Disk Partitioning Setup”).

When you have finished identifying devices to be used for installation, click **Next** to continue.

### 9.10. Initializing the Hard Disk

If no readable partition tables are found on existing hard disks, the installation program asks to initialize the hard disk. This operation makes any existing data on the hard disk unreadable. If your system has a brand new hard disk with no operating system installed, or you have removed all partitions on the hard disk, click **Re-initialize drive**.

The installation program presents you with a separate dialog for each disk on which it cannot read a valid partition table. Click the **Ignore all** button or **Re-initialize all** button to apply the same answer to all devices.
Upgrading an Existing System

9.11. Upgrading an Existing System

Preupgrade

Fedora includes preupgrade, a command-line tool that allows you to upgrade easily to a new version from within your existing Fedora installation.

The installation system automatically detects any existing installation of Fedora. The upgrade process updates the existing system software with new versions, but does not remove any data from users’
home directories. The existing partition structure on your hard drives does not change. Your system configuration changes only if a package upgrade demands it. Most package upgrades do not change system configuration, but rather install an additional configuration file for you to examine later.

Note that the installation medium that you are using might not contain all the software packages that you need to upgrade your computer.

9.11.1. The Upgrade Dialog

If your system contains a Fedora installation, a dialog appears asking whether you want to upgrade that installation. To perform an upgrade of an existing system, choose the appropriate installation from the drop-down list and select Next.

At least one existing installation has been detected on your system. What would you like to do?

- **Fresh Installation**
  Choose this option to install a fresh copy of Red Hat Enterprise Linux on your system. Existing software and data may be overwritten depending on your configuration choices.

- **Upgrade an Existing Installation**
  Choose this option if you would like to upgrade your existing Red Hat Enterprise Linux system. This option will preserve the existing data on your storage device(s).

Which Red Hat Enterprise Linux installation would you like to upgrade?

- Red Hat Enterprise Linux Server 5.5 (Installed on /dev/mapper/VolGroup00-LogVol00)

Figure 9.35. The Upgrade Dialog

**Manually Installed Software**

Software you have installed manually on your existing Fedora system may behave differently after an upgrade. You may need to manually reinstall or recompile this software after an upgrade to ensure it performs correctly on the updated system.
Re-installing Fedora

If you are re-installing the same version of Fedora, preserve your user data by placing it on a separate `/home` partition.

9.11.2. Upgrading Using the Installer

Installations are Recommended

In general, the Fedora Project recommends that you keep user data on a separate `/home` partition and perform a fresh installation. For more information on partitions and how to set them up, refer to Section 9.12, "Disk Partitioning Setup".

If you choose to upgrade your system using the installation program, any software not provided by Fedora that conflicts with Fedora software is overwritten. Before you begin an upgrade this way, make a list of your system's current packages for later reference:

```
rpm -qa --qf '%{NAME} %{VERSION}-%{RELEASE} %{ARCH}\n' > ~/old-pkglist.txt
```

After installation, consult this list to discover which packages you may need to rebuild or retrieve from sources other than the Fedora Project.

Next, make a backup of any system configuration data:

```
su -c 'tar czf /tmp/etc-`date +%F`.tar.gz /etc'
su -c 'mv /tmp/etc-*.tar.gz /home'
```

Make a complete backup of any important data before performing an upgrade. Important data may include the contents of your entire `/home` directory as well as content from services such as an Apache, FTP, or SQL server, or a source code management system. Although upgrades are not destructive, if you perform one improperly there is a small possibility of data loss.

Storing Backups

Note that the above examples store backup materials in a `/home` directory. If your `/home` directory is not a separate partition, you should not follow these examples verbatim! Store your backups on another device such as CD or DVD discs or an external hard disk.

For more information on completing the upgrade process later, refer to Section 18.2, "Finishing an Upgrade".

9.11.3. Upgrading Boot Loader Configuration
Your completed Fedora installation must be registered in the boot loader to boot properly. A boot loader is software on your machine that locates and starts the operating system. Refer to Appendix E, The GRUB Boot Loader for more information about boot loaders.

The installer is unable to detect the boot loader currently in use on your system.

What would you like to do?

- Update boot loader configuration
  This will update your current boot loader.
- Skip boot loader updating
  This option makes no changes to boot loader configuration. If you are using a third party boot loader, you should choose this.
- Create new boot loader configuration
  This option creates a new boot loader configuration. If you wish to switch boot loaders, you should choose this.

Figure 9.36. The Upgrade Boot Loader Dialog

If the existing boot loader was installed by a Linux distribution, the installation system can modify it to load the new Fedora system. To update the existing Linux boot loader, select Update boot loader configuration. This is the default behavior when you upgrade an existing Fedora installation.

GRUB is the standard boot loader for Fedora on 32-bit and 64-bit x86 architectures. If your machine uses another boot loader, such as BootMagic, System Commander, or the loader installed by Microsoft Windows, then the Fedora installation system cannot update it. In this case, select Skip boot loader updating. When the installation process completes, refer to the documentation for your product for assistance.

Install a new boot loader as part of an upgrade process only if you are certain you want to replace the existing boot loader. If you install a new boot loader, you may not be able to boot other operating systems on the same machine until you have configured the new boot loader. Select Create new boot loader configuration to remove the existing boot loader and install GRUB.

After you make your selection, click Next to continue. If you selected the Create new boot loader configuration option, refer to Section 9.16, “x86, AMD64, and Intel 64 Boot Loader Configuration”. If you chose to update or skip boot loader configuration, installation continues without further input from you.

9.12. Disk Partitioning Setup
**Warning — Back up your data**

It is always a good idea to back up any data that you have on your systems. For example, if you are upgrading or creating a dual-boot system, you should back up any data you wish to keep on your storage devices. Mistakes do happen and can result in the loss of all your data.

**Important — Installing in text mode**

If you install Fedora in text mode, you can only use the default partitioning schemes described in this section. You cannot add or remove partitions or file systems beyond those that the installer automatically adds or removes. If you require a customized layout at installation time, you should perform a graphical installation over a VNC connection or a kickstart installation.

Furthermore, advanced options such as LVM, encrypted filesystems, and resizable filesystems are available only in graphical mode and kickstart.

**Important — Booting from RAIDs**

If you have a RAID card, be aware that some BIOSes do not support booting from the RAID card. In cases such as these, the `/boot/` partition must be created on a partition outside of the RAID array, such as on a separate hard drive. An internal hard drive is necessary to use for partition creation with problematic RAID cards.

A `/boot/` partition is also necessary for software RAID setups.

If you have chosen to automatically partition your system, you should select **Review** and manually edit your `/boot/` partition.

Partitioning allows you to divide your hard drive into isolated sections, where each section behaves as its own hard drive. Partitioning is particularly useful if you run multiple operating systems. If you are not sure how you want your system to be partitioned, read **Appendix A, An Introduction to Disk Partitions** for more information.
Chapter 9. Installing using anaconda

Figure 9.37. Disk Partitioning Setup

On this screen you can choose to create the default partition layout in one of four different ways, or choose to partition storage devices manually to create a custom layout.

The first four options allow you to perform an automated installation without having to partition your storage devices yourself. If you do not feel comfortable with partitioning your system, choose one of these options and let the installation program partition the storage devices for you. Depending on the option that you choose, you can still control what data (if any) is removed from the system.

Your options are:

Use All Space
Select this option to remove all partitions on your hard drives (this includes partitions created by other operating systems such as Windows VFAT or NTFS partitions).

**Warning**
If you select this option, all data on the selected hard drives is removed by the installation program. Do not select this option if you have information that you want to keep on the hard drives where you are installing Fedora.

In particular, do not select this option when you configure a system to chain load the Fedora boot loader from another boot loader.
Replace Existing Linux System(s)

Select this option to remove only partitions created by a previous Linux installation. This does not remove other partitions you may have on your hard drives (such as VFAT or FAT32 partitions).

Shrink Current System

Select this option to resize your current data and partitions manually and install a default Fedora layout in the space that is freed.

**Warning**

If you shrink partitions on which other operating systems are installed, you might not be able to use those operating systems. Although this partitioning option does not destroy data, operating systems typically require some free space in their partitions. Before you resize a partition that holds an operating system that you might want to use again, find out how much space you need to leave free.

Use Free Space

Select this option to retain your current data and partitions and install Fedora in the unused space available on the storage drives. Ensure that there is sufficient space available on the storage drives before you select this option — refer to Section 4.4, “Do You Have Enough Disk Space?”.

**Warning**

If your 64-bit x86 system uses UEFI instead of BIOS, you will need to manually create a /boot partition. This partition must have an ext3 file system. If you choose to partition automatically, your system will not boot.

Create Custom Layout

Select this option to partition storage devices manually and create customized layouts. Refer to Section 9.14, “Creating a Custom Layout or Modifying the Default Layout”

Choose your preferred partitioning method by clicking the radio button to the left of its description in the dialog box.

Select Encrypt system to encrypt all partitions except the /boot partition. Refer to Appendix C, Disk Encryption for information on encryption.

Select Use LVM to enable Logical Volume Management. Refer to Appendix D, Understanding LVM for information on LVM.

To review and make any necessary changes to the partitions created by automatic partitioning, select the Review option. After selecting Review and clicking Next to move forward, the partitions created for you by anaconda appear. You can make modifications to these partitions if they do not meet your needs.
Important — chain loading

To configure the Fedora boot loader to chain load from a different boot loader, you must specify the boot drive manually. If you chose any of the automatic partitioning options, you must now select the **Review and modify partitioning layout** option before you click **Next** or you cannot specify the correct boot drive.

Important — Mixing multipath and non-multipath devices

When you install Fedora on a system with multipath and non-multipath storage devices, the automatic partitioning layout in the installer might create volume groups that contain a mix of multipath and non-multipath devices. This defeats the purpose of multipath storage.

We advise that you select only multipath or only non-multipath devices on the disk selection screen that appears after selecting automatic partitioning. Alternatively, select custom partitioning.

Click **Next** once you have made your selections to proceed.

9.13. Encrypt Partitions

If you selected the **Encrypt System** option, the installer prompts you for a passphrase with which to encrypt the partitions on the system.

Partitions are encrypted using the **Linux Unified Key Setup** — refer to **Appendix C, Disk Encryption** for more information.

Choose a passphrase for the encrypted devices. You will be prompted for this passphrase during system boot.

<table>
<thead>
<tr>
<th>Enter passphrase for encrypted partition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choose a passphrase for the encrypted devices. You will be prompted for this passphrase during system boot.</td>
</tr>
<tr>
<td>Enter passphrase:</td>
</tr>
<tr>
<td>Confirm passphrase:</td>
</tr>
</tbody>
</table>

Figure 9.38. Enter passphrase for encrypted partition

Choose a passphrase and type it into each of the two fields in the dialog box. You must provide this passphrase every time that the system boots.
9.14. Creating a Custom Layout or Modifying the Default Layout

If you chose one of the four automatic partitioning options and did not select Review, skip ahead to Section 9.17, “Package Group Selection”.

If you chose one of the automatic partitioning options and selected Review, you can either accept the current partition settings (click Next), or modify the setup manually in the partitioning screen.

If you chose to create a custom layout, you must tell the installation program where to install Fedora. This is done by defining mount points for one or more disk partitions in which Fedora is installed. You may also need to create and/or delete partitions at this time.

Warning

If your 64-bit x86 system uses UEFI instead of BIOS, you will need to manually create a /boot partition. This partition must have an ext3 file system. If you choose to partition automatically, your system will not boot.

If you have not yet planned how to set up your partitions, refer to Appendix A, An Introduction to Disk Partitions and Section 9.14.5, “Recommended Partitioning Scheme”. At a bare minimum, you need an appropriately-sized root partition, and usually a swap partition appropriate to the amount of RAM you have on the system.

Anaconda can handle the partitioning requirements for a typical installation.
Figure 9.39. Partitioning on x86, AMD64, and Intel 64 Systems

The partitioning screen contains two panes. The top pane contains a graphical representation of the hard drive, logical volume, or RAID device selected in the lower pane.

Above the graphical representation of the device, you can review the name of the drive (such as `\dev/sda` or `LogVol00`), its size (in MB), and its model as detected by the installation program.

Using your mouse, click once to highlight a particular field in the graphical display. Double-click to edit an existing partition or to create a partition out of existing free space.

The lower pane contains a list of all drives, logical volumes, and RAID devices to be used during installation, as specified earlier in the installation process — refer to Section 9.9, “Assign Storage Devices.”

Devices are grouped by type. Click on the small triangles to the left of each device type to view or hide devices of that type.

**Anaconda** displays several details for each device listed:

- **Device**
  - the name of the device, logical volume, or partition

- **Size (MB)**
  - the size of the device, logical volume, or partition (in MB)

- **Mount Point/RAID/Volume**
  - the *mount point* (location within a file system) on which a partition is to be mounted, or the name of the RAID or logical volume group of which it is a part

- **Type**
  - the type of partition. If the partition is a standard partition, this field displays the type of file system on the partition (for example, `ext4`). Otherwise, it indicates that the partition is a physical volume (LVM), or part of a software RAID

<table>
<thead>
<tr>
<th>Device</th>
<th>Size (MB)</th>
<th>Type</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>/dev/sda2</td>
<td>19979 MB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>lv_root</td>
<td>17960 MB</td>
<td>ext4</td>
<td>✓</td>
</tr>
<tr>
<td>lv_swap</td>
<td>2016 MB</td>
<td>swap</td>
<td>✓</td>
</tr>
</tbody>
</table>
Format

A check mark in this column indicates that the partition will be formatted during installation.

Beneath the lower pane are four buttons: Create, Edit, Delete, and Reset.

Select a device or partition by clicking on it in either the graphical representation in the upper pane of in the list in the lower pane, then click one of the four buttons to carry out the following actions:

Create
create a new partition, logical volume, or software RAID

Edit
change an existing partition, logical volume, or software RAID. Note that you can only shrink partitions with the Resize button, not enlarge partitions.

Delete
remove a partition, logical volume, or software RAID

Reset
undo all changes made in this screen


The Create Storage dialog allows you to create new storage partitions, logical volumes, and software RAID. Anaconda presents options as available or unavailable depending on the storage already present on the system or configured to transfer to the system.

Options are grouped under Create Partition, Create Software RAID and Create LVM as follows:
Chapter 9. Installing using anaconda

Create Partition

• **Standard Partition** — create a standard disk partition (as described in Appendix A, An Introduction to Disk Partitions) in unallocated space.

Create Software RAID
Refer to Section 9.14.3, “Create Software RAID” for more detail.

• **RAID Partition** — create a partition in unallocated space to form part of a software RAID device. To form a software RAID device, two or more RAID partitions must be available on the system.

• **RAID Device** — combine two or more RAID partitions into a software RAID device. When you choose this option, you can specify the type of RAID device to create (the RAID level). This option is only available when two or more RAID partitions are available on the system.

Create LVM Logical Volume
Refer to Section 9.14.4, “Create LVM Logical Volume” for more detail.

• **LVM Physical Volume** — create a physical volume in unallocated space.

• **LVM Volume Group** — create a volume group from one or more physical volumes. This option is only available when at least one physical volume is available on the system.

• **LVM Logical Volume** — create a logical volume on a volume group. This option is only available when at least one volume group is available on the system.


To add a new partition, select the Create button. A dialog box appears (refer to Figure 9.41, “Creating a New Partition”).

---

**Note**

You must dedicate at least one partition for this installation, and optionally more. For more information, refer to Appendix A, An Introduction to Disk Partitions.
Adding Partitions

Figure 9.41. Creating a New Partition

- **Mount Point**: Enter the partition's mount point. For example, if this partition should be the root partition, enter `/`; enter `/boot` for the `/boot` partition, and so on. You can also use the pull-down menu to choose the correct mount point for your partition. For a swap partition the mount point should not be set — setting the filesystem type to `swap` is sufficient.

- **File System Type**: Using the pull-down menu, select the appropriate file system type for this partition. For more information on file system types, refer to Section 9.14.2.1, "File System Types".

- **Allowable Drives**: This field contains a list of the hard disks installed on your system. If a hard disk's box is highlighted, then a desired partition can be created on that hard disk. If the box is not checked, then the partition will never be created on that hard disk. By using different checkbox settings, you can have `anaconda` place partitions where you need them, or let `anaconda` decide where partitions should go.

- **Size (MB)**: Enter the size (in megabytes) of the partition. Note, this field starts with 200 MB; unless changed, only a 200 MB partition will be created.

- **Additional Size Options**: Choose whether to keep this partition at a fixed size, to allow it to "grow" (fill up the available hard drive space) to a certain point, or to allow it to grow to fill any remaining hard drive space available.

  If you choose **Fill all space up to (MB)**, you must give size constraints in the field to the right of this option. This allows you to keep a certain amount of space free on your hard drive for future use.
• **Encrypt**: Choose whether to encrypt the partition so that the data stored on it cannot be accessed without a passphrase, even if the storage device is connected to another system. Refer to Appendix C, Disk Encryption for information on encryption of storage devices. If you select this option, the installer prompts you to provide a passphrase before it writes the partition to the disk.

• **OK**: Select OK once you are satisfied with the settings and wish to create the partition.

• **Cancel**: Select Cancel if you do not want to create the partition.

### 9.14.2.1. File System Types

Fedora allows you to create different partition types and file systems. The following is a brief description of the different partition types and file systems available, and how they can be used.

#### Partition types

- **standard partition** — A standard partition can contain a file system or swap space, or it can provide a container for software RAID or an LVM physical volume.

- **swap** — Swap partitions are used to support virtual memory. In other words, data is written to a swap partition when there is not enough RAM to store the data your system is processing. Refer to the Fedora Deployment Guide for additional information.

- **software RAID** — Creating two or more software RAID partitions allows you to create a RAID device. For more information regarding RAID, refer to the chapter RAID (Redundant Array of Independent Disks) in the Fedora Deployment Guide.

- **physical volume (LVM)** — Creating one or more physical volume (LVM) partitions allows you to create an LVM logical volume. LVM can improve performance when using physical disks. For more information regarding LVM, refer to the Fedora Deployment Guide.

#### File systems

- **ext4** — The ext4 file system is based on the ext3 file system and features a number of improvements. These include support for larger file systems and larger files, faster and more efficient allocation of disk space, no limit on the number of subdirectories within a directory, faster file system checking, and more robust journaling. The ext4 file system is selected by default and is highly recommended.

- **ext3** — The ext3 file system is based on the ext2 file system and has one main advantage — journaling. Using a journaling file system reduces time spent recovering a file system after a crash as there is no need to fsck the file system.

- **ext2** — An ext2 file system supports standard Unix file types (regular files, directories, symbolic links, etc). It provides the ability to assign long file names, up to 255 characters.

- **xfs** — XFS is a highly scalable, high-performance file system that supports filesystems up to 16 exabytes (approximately 16 million terabytes), files up to 8 exabytes (approximately 8 million terabytes) and directory structures containing tens of millions of entries. XFS supports metadata journaling, which facilitates quicker crash recovery. The XFS file system can also be defragmented and resized while mounted and active.

---

2 The fsck application is used to check the file system for metadata consistency and optionally repair one or more Linux file systems.
• **vfat** — The VFAT file system is a Linux file system that is compatible with Microsoft Windows long filenames on the FAT file system.

---

**Note**

The Btrfs file system is unavailable in Fedora 17.

### 9.14.3. Create Software RAID

*Redundant arrays of independent disks* (RAIDs) are constructed from multiple storage devices that are arranged to provide increased performance and — in some configurations — greater fault tolerance. Refer to the *Fedora Deployment Guide* for a description of different kinds of RAIDs.

To make a RAID device, you must first create software RAID partitions. Once you have created two or more software RAID partitions, select **RAID** to join the software RAID partitions into a RAID device.

**RAID Partition**

Choose this option to configure a partition for software RAID. This option is the only choice available if your disk contains no software RAID partitions. This is the same dialog that appears when you add a standard partition — refer to Section 9.14.2, “Adding Partitions” for a description of the available options. Note, however, that **File System Type** must be set to **software RAID**.
Chapter 9. Installing using Anaconda

### RAID Device

Choose this option to construct a RAID device from two or more existing software RAID partitions. This option is available if two or more software RAID partitions have been configured.

![Add Partition interface](image)

**Figure 9.42. Create a software RAID partition**

<table>
<thead>
<tr>
<th>Mount Point:</th>
<th>&lt;Not Applicable&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>File System Type:</td>
<td>software RAID</td>
</tr>
<tr>
<td>Allowable Drives:</td>
<td>sda 80480 MB ATA HARDDISK, sdb 80480 MB ATA HARDDISK</td>
</tr>
<tr>
<td>Size (MB):</td>
<td>200</td>
</tr>
<tr>
<td>Additional Size Options</td>
<td></td>
</tr>
<tr>
<td>○ Fixed size</td>
<td></td>
</tr>
<tr>
<td>○ Fill all space up to (MB):</td>
<td>1</td>
</tr>
<tr>
<td>○ Fill to maximum allowable size</td>
<td></td>
</tr>
<tr>
<td>□ Force to be a primary partition</td>
<td></td>
</tr>
<tr>
<td>□ Encrypt</td>
<td></td>
</tr>
</tbody>
</table>

![Make RAID Device interface](image)

**Figure 9.43. Create a RAID device**

| Mount Point: | |
| File System Type: | ext3 |
| RAID Device: | md0 |
| RAID Level: | RAID1 |
| RAID Members: | sda 81306 MB, sdb 81502 MB |
| Number of spares: | 0 |
| □ Encrypt | |
Select the file system type as for a standard partition.

Anaconda automatically suggests a name for the RAID device, but you can manually select names from md0 to md15.

Click the checkboxes beside individual storage devices to include or remove them from this RAID.

The RAID Level corresponds to a particular type of RAID. Choose from the following options:

- **RAID 0** — distributes data across multiple storage devices. Level 0 RAIDs offer increased performance over standard partitions, and can be used to pool the storage of multiple devices into one large virtual device. Note that Level 0 RAIDS offer no redundancy and that the failure of one device in the array destroys the entire array. RAID 0 requires at least two RAID partitions.

- **RAID 1** — mirrors the data on one storage device onto one or more other storage devices. Additional devices in the array provide increasing levels of redundancy. RAID 1 requires at least two RAID partitions.

- **RAID 4** — distributes data across multiple storage devices, but uses one device in the array to store parity information that safeguards the array in case any device within the array fails. Because all parity information is stored on the one device, access to this device creates a bottleneck in the performance of the array. RAID 4 requires at least three RAID partitions.

- **RAID 5** — distributes data and parity information across multiple storage devices. Level 5 RAIDs therefore offer the performance advantages of distributing data across multiple devices, but do not share the performance bottleneck of level 4 RAIDs because the parity information is also distributed through the array. RAID 5 requires at least three RAID partitions.

- **RAID 6** — level 6 RAIDs are similar to level 5 RAIDs, but instead of storing only one set of parity data, they store two sets. RAID 6 requires at least four RAID partitions.

- **RAID 10** — level 10 RAIDs are *nested RAIDs* or *hybrid RAIDs*. Level 10 RAIDs are constructed by distributing data over mirrored sets of storage devices. For example, a level 10 RAID constructed from four RAID partitions consists of two pairs of partitions in which one partition mirrors the other. Data is then distributed across both pairs of storage devices, as in a level 0 RAID. RAID 10 requires at least four RAID partitions.

### 9.14.4. Create LVM Logical Volume

**Important — LVM Unavailable in Text-Mode Installations**

LVM initial set up is not available during text-mode installation. If you need to create an LVM configuration from scratch, press `Alt+F2` to use a different virtual console, and run the `lvm` command. To return to the text-mode installation, press `Alt+F1`.

**Logical Volume Management** (LVM) presents a simple logical view of underlying physical storage space, such as a hard drives or LUNs. Partitions on physical storage are represented as physical volumes that can be grouped together into volume groups. Each volume group can be divided into multiple logical volumes, each of which is analogous to a standard disk partition. Therefore, LVM logical volumes function as partitions that can span multiple physical disks.

To read more about LVM, refer to the *Fedora Deployment Guide*. Note, LVM is only available in the graphical installation program.
LVM Physical Volume
Choose this option to configure a partition or device as an LVM physical volume. This option is the only choice available if your storage does not already contain LVM Volume Groups. This is the same dialog that appears when you add a standard partition — refer to Section 9.14.2, “Adding Partitions” for a description of the available options. Note, however, that File System Type must be set to physical volume (LVM).

Figure 9.44. Create an LVM Physical Volume

Make LVM Volume Group
Choose this option to create LVM volume groups from the available LVM physical volumes, or to add existing logical volumes to a volume group.
To assign one or more physical volumes to a volume group, first name the volume group. Then select the physical volumes to be used in the volume group. Finally, configure logical volumes on any volume groups using the Add, Edit and Delete options.

You may not remove a physical volume from a volume group if doing so would leave insufficient space for that group's logical volumes. Take for example a volume group made up of two 5 GB LVM physical volume partitions, which contains an 8 GB logical volume. The installer would not allow you to remove either of the component physical volumes, since that would leave only 5 GB in the group for an 8 GB logical volume. If you reduce the total size of any logical volumes appropriately, you may then remove a physical volume from the volume group. In the example, reducing the size of the logical volume to 4 GB would allow you to remove one of the 5 GB physical volumes.

**Make Logical Volume**

Choose this option to create an LVM logical volume. Select a mount point, file system type, and size (in MB) just as if it were a standard disk partition. You can also choose a name for the logical volume and specify the volume group to which it will belong.
Chapter 9. Installing using anaconda

9.14.5. Recommended Partitioning Scheme

9.14.5.1. x86, AMD64, and Intel 64 systems

Unless you have a reason for doing otherwise, we recommend that you create the following partitions for x86, AMD64, and Intel 64 systems:

- A swap partition
- A /boot partition
- A / partition
- A /home partition
- A swap partition (at least 256 MB) — swap partitions are used to support virtual memory. In other words, data is written to a swap partition when there is not enough RAM to store the data your system is processing.

In years past, the recommended amount of swap space increased linearly with the amount of RAM in the system. But because the amount of memory in modern systems has increased into the hundreds of gigabytes, it is now recognized that the amount of swap space that a system needs is a function of the memory workload running on that system.

Swap space is usually designated during installation, but determining the memory workload of a system at this point can be difficult. During a kickstart installation, you can request that the amount of swap space be set automatically (refer to Section 15.4, “Kickstart Options”.

However, this setting is not precisely calibrated for your system, so use the following table if you require the amount of swap space to be set more precisely.

Table 9.2. Recommended System Swap Space

<table>
<thead>
<tr>
<th>Amount of RAM in the System</th>
<th>Recommended Amount of Swap Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>4GB of RAM or less</td>
<td>a minimum of 2GB of swap space</td>
</tr>
<tr>
<td>4GB to 16GB of RAM</td>
<td>a minimum of 4GB of swap space</td>
</tr>
</tbody>
</table>
Recommended Partitioning Scheme

<table>
<thead>
<tr>
<th>Amount of RAM in the System</th>
<th>Recommended Amount of Swap Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>16GB to 64GB of RAM</td>
<td>a minimum of 8GB of swap space</td>
</tr>
<tr>
<td>64GB to 256GB of RAM</td>
<td>a minimum of 16GB of swap space</td>
</tr>
<tr>
<td>256GB to 512GB of RAM</td>
<td>a minimum of 32GB of swap space</td>
</tr>
</tbody>
</table>

Note that you can obtain better performance by distributing swap space over multiple storage devices, particularly on systems with fast drives, controllers, and interfaces.

- **A /boot/ partition (250 MB)**
  
The partition mounted on `/boot/` contains the operating system kernel (which allows your system to boot Fedora), along with files used during the bootstrap process. For most users, a 250 MB boot partition is sufficient.

**Important — Supported file systems**

The GRUB bootloader in Fedora 17 supports only the ext2, ext3, and ext4 (recommended) file systems. You cannot use any other file system for `/boot/`, such as Btrfs, XFS, or VFAT.

**Note**

If your hard drive is more than 1024 cylinders (and your system was manufactured more than two years ago), you may need to create a `/boot/` partition if you want the `/` (root) partition to use all of the remaining space on your hard drive.

**Note**

If you have a RAID card, be aware that some BIOSes do not support booting from the RAID card. In cases such as these, the `/boot/` partition must be created on a partition outside of the RAID array, such as on a separate hard drive.

- **A root partition (3.0 GB - 5.0 GB)**
  
  This is where “/” (the root directory) is located. In this setup, all files (except those stored in `/boot/`) are on the root partition.

  A 3.0 GB partition allows you to install a minimal installation, while a 5.0 GB root partition lets you perform a full installation, choosing all package groups.
**Root and /root**

The / (or root) partition is the top of the directory structure. The /root directory (sometimes pronounced “slash-root”) directory is the home directory of the user account for system administration.

- **A home partition (at least 100 MB)**

  To store user data separately from system data, create a dedicated partition within a volume group for the /home directory. This will enable you to upgrade or reinstall Fedora without erasing user data files.

  Many systems have more partitions than the minimum listed above. Choose partitions based on your particular system needs. Refer to Section 9.14.5.1.1, “Advice on Partitions” for more information.

  If you create many partitions instead of one large / partition, upgrades become easier. Refer to the description of the Edit option in Section 9.14, “Creating a Custom Layout or Modifying the Default Layout” for more information.

The following table summarizes minimum partition sizes for the partitions containing the listed directories. You do not have to make a separate partition for each of these directories. For instance, if the partition containing /foo must be at least 500 MB, and you do not make a separate /foo partition, then the / (root) partition must be at least 500 MB.

<table>
<thead>
<tr>
<th>Directory</th>
<th>Minimum size</th>
</tr>
</thead>
<tbody>
<tr>
<td>/</td>
<td>250 MB</td>
</tr>
<tr>
<td>/usr</td>
<td>250 MB, but avoid placing this on a separate partition</td>
</tr>
<tr>
<td>/tmp</td>
<td>50 MB</td>
</tr>
<tr>
<td>/var</td>
<td>384 MB</td>
</tr>
<tr>
<td>/home</td>
<td>100 MB</td>
</tr>
<tr>
<td>/boot</td>
<td>250 MB</td>
</tr>
</tbody>
</table>

**Leave Excess Capacity Unallocated**

Only assign storage capacity to those partitions you require immediately. You may allocate free space at any time, to meet needs as they occur. To learn about a more flexible method for storage management, refer to Appendix D, Understanding LVM.

If you are not sure how best to configure the partitions for your computer, accept the default partition layout.
9.14.5.1.1. Advice on Partitions
Optimal partition setup depends on the usage for the Linux system in question. The following tips may help you decide how to allocate your disk space.

- Consider encrypting any partitions that might contain sensitive data. Encryption prevents unauthorized people from accessing the data on the partitions, even if they have access to the physical storage device. In most cases, you should at least encrypt the /home partition.

- Each kernel installed on your system requires approximately 10 MB on the /boot partition. Unless you plan to install a great many kernels, the default partition size of 250 MB for /boot should suffice.

**Important — Supported file systems**
The GRUB bootloader in Fedora 17 supports only the ext2, ext3, and ext4 (recommended) file systems. You cannot use any other file system for /boot, such as Btrfs, XFS, or VFAT.

- The /var directory holds content for a number of applications, including the Apache web server. It also is used to store downloaded update packages on a temporary basis. Ensure that the partition containing the /var directory has enough space to download pending updates and hold your other content.

**Warning**
The PackageKit update software downloads updated packages to /var/cache/yum/ by default. If you partition the system manually, and create a separate /var/ partition, be sure to create the partition large enough (3.0 GB or more) to download package updates.

- The /usr directory holds the majority of software content on a Fedora system. For an installation of the default set of software, allocate at least 4 GB of space. If you are a software developer or plan to use your Fedora system to learn software development skills, you may want to at least double this allocation.

**Do not place /usr on a separate file system**
If /usr is on a separate file system from /, the boot process becomes much more complex because /usr contains boot-critical components. In some situations (like installations on iSCSI drives), the boot process might not work at all.

- Consider leaving a portion of the space in an LVM volume group unallocated. This unallocated space gives you flexibility if your space requirements change but you do not wish to remove data from other partitions to reallocate storage.
Chapter 9. Installing using anaconda

- If you separate subdirectories into partitions, you can retain content in those subdirectories if you decide to install a new version of Fedora over your current system. For instance, if you intend to run a MySQL database in `/var/lib/mysql`, make a separate partition for that directory in case you need to reinstall later.

- If you are creating a custom partition layout on a non-EFI x86 system, you are strongly advised to create a separate, 1MB BIOS boot partition. This is only recommended on the disk you are installing the bootloader on and if any of the following conditions apply:
  
  • The disk contains a GPT partition table.
  
  • The installer has already initialized the disk for you.
  
  • You selected **Use All Space** in the Disk Partitioning Setup.

  This boot partition will be used by the GRUB boot loader for storage.

The following table is a possible partition setup for a system with a single, new 80 GB hard disk and 1 GB of RAM. Note that approximately 10 GB of the volume group is unallocated to allow for future growth.

### Example Usage

This setup is not optimal for all use cases.

**Example 9.1. Example partition setup**

#### Table 9.4. Example partition setup

<table>
<thead>
<tr>
<th>Partition</th>
<th>Size and type</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/boot</code></td>
<td>250 MB ext3 partition</td>
</tr>
<tr>
<td>swap</td>
<td>2 GB swap</td>
</tr>
<tr>
<td>LVM physical volume</td>
<td>Remaining space, as one LVM volume group</td>
</tr>
</tbody>
</table>

The physical volume is assigned to the default volume group and divided into the following logical volumes:

#### Table 9.5. Example partition setup: LVM physical volume

<table>
<thead>
<tr>
<th>Partition</th>
<th>Size and type</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>/</code></td>
<td>13 GB ext4</td>
</tr>
<tr>
<td><code>/var</code></td>
<td>4 GB ext4</td>
</tr>
<tr>
<td><code>/home</code></td>
<td>50 GB ext4</td>
</tr>
</tbody>
</table>

### 9.15. Write changes to disk

The installer prompts you to confirm the partitioning options that you selected. Click **Write changes to disk** to allow the installer to partition your hard drive and install Fedora.
Last chance to cancel safely

Up to this point in the installation process, the installer has made no lasting changes to your computer. When you click Write changes to disk, the installer will allocate space on your hard drive and start to transfer Fedora into this space. Depending on the partitioning option that you chose, this process might include erasing data that already exists on your computer.

To revise any of the choices that you made up to this point, click Go back. To cancel installation completely, switch off your computer. To switch off most computers at this stage, press the power button and hold it down for a few seconds.

After you click Write changes to disk, allow the installation process to complete. If the process is interrupted (for example, by you switching off or resetting the computer, or by a power outage) you will probably not be able to use your computer until you restart and complete the Fedora installation process, or install a different operating system.

9.16. x86, AMD64, and Intel 64 Boot Loader Configuration

To boot the system without boot media, you usually need to install a boot loader. A boot loader is the first software program that runs when a computer starts. It is responsible for loading and transferring control to the operating system kernel software. The kernel, in turn, initializes the rest of the operating system.

Installing in text mode

If you install Fedora in text mode, the installer configures the bootloader automatically and you cannot customize bootloader settings during the installation process.

GRUB (GRand Unified Bootloader), which is installed by default, is a very powerful boot loader. GRUB can load a variety of free operating systems, as well as proprietary operating systems with chain-loading (the mechanism for loading unsupported operating systems, such as Windows, by loading another boot loader). Note that Fedora 17 uses GRUB 2. GRUB Legacy is no longer actively developed.3

The GRUB menu defaults to being hidden, except on dual-boot systems. To show the GRUB menu during system boot, press and hold the Shift key before the kernel is loaded. (Any other key works as well but the Shift key is the safest to use.)

![Boot Loader Configuration](image)

If there are no other operating systems on your computer, or you are completely removing any other operating systems the installation program will install GRUB as your boot loader without any intervention. In that case you may continue on to Section 9.17, “Package Group Selection”.

You may have a boot loader installed on your system already. An operating system may install its own preferred boot loader, or you may have installed a third-party boot loader. If your boot loader does not recognize Linux partitions, you may not be able to boot Fedora. Use GRUB as your boot loader to boot Linux and most other operating systems. Follow the directions in this chapter to install GRUB.

If you install GRUB, it may overwrite your existing boot loader.

By default, the installation program installs GRUB in the master boot record or MBR, of the device for the root file system. To decline installation of a new boot loader, unselect Install boot loader on /dev/sda.
Warning

If you choose not to install GRUB for any reason, you will not be able to boot the system directly, and you must use another boot method (such as a commercial boot loader application). Use this option only if you are sure you have another way of booting the system!

If you have other operating systems already installed, Fedora attempts to automatically detect and configure GRUB to boot them. You may manually configure any additional operating systems if GRUB does not detect them.

To add, remove, or change the detected operating system settings, use the options provided.

Add
Select Add to include an additional operating system in GRUB.

Select the disk partition which contains the bootable operating system from the drop-down list and give the entry a label. GRUB displays this label in its boot menu.

Edit
To change an entry in the GRUB boot menu, select the entry and then select Edit.

Delete
To remove an entry from the GRUB boot menu, select the entry and then select Delete.

Select Default beside the preferred boot partition to choose your default bootable OS. You cannot move forward in the installation unless you choose a default boot image.

Note

The Label column lists what you must enter at the boot prompt, in non-graphical boot loaders, in order to boot the desired operating system.

Once you have loaded the GRUB boot screen, use the arrow keys to choose a boot label or type e for edit. You are presented with a list of items in the configuration file for the boot label you have selected.

Boot loader passwords provide a security mechanism in an environment where physical access to your server is available.

If you are installing a boot loader, you should create a password to protect your system. Without a boot loader password, users with access to your system can pass options to the kernel which can compromise your system security. With a boot loader password in place, the password must first be entered before selecting any non-standard boot options. However, it is still possible for someone with physical access to the machine to boot from a diskette, CD-ROM, DVD, or USB media if the BIOS supports it. Security plans which include boot loader passwords should also address alternate boot methods.
Chapter 9. Installing using anaconda

**GRUB Passwords Not Required**

You may not require a GRUB password if your system only has trusted operators, or is physically secured with controlled console access. However, if an untrusted person can get physical access to your computer's keyboard and monitor, that person can reboot the system and access GRUB. A password is helpful in this case.

If you choose to use a boot loader password to enhance your system security, be sure to select the checkbox labeled **Use a boot loader password**.

Once selected, enter a password and confirm it.

Whenever you are required to enter this password, you will also be asked for a username, which is root.

GRUB stores the password in encrypted form, so it cannot be read or recovered. If you forget the boot password, boot the system normally and then change the password entry in the /etc/grub.d/00_header file. Then, run `grub2-mkconfig` with root privileges to update the `grub.cfg` file with your updated password. If you cannot boot, you may be able to use the rescue mode on the Fedora installation DVD to reset the GRUB password.

You can later change the username in the /etc/grub.d/01_users file.

**GRUB recognizes only the QWERTY keyboard layout**

When selecting a GRUB password, be aware that GRUB recognizes only the QWERTY keyboard layout, regardless of the keyboard actually attached to the system. If you use a keyboard with a significantly different layout, it might be more effective to memorize a pattern of keystrokes rather than the word that the pattern produces.

To configure more advanced boot loader options, such as changing the drive order or passing options to the kernel, be sure **Configure advanced boot loader options** is selected before clicking **Next**.

**9.16.1. Advanced Boot Loader Configuration**

Now that you have chosen which boot loader to install, you can also determine where you want the boot loader to be installed. You may install the boot loader in one of two places:

- **The master boot record (MBR)** — This is the recommended place to install a boot loader, unless the MBR already starts another operating system loader, such as System Commander. The MBR is a special area on your hard drive that is automatically loaded by your computer's BIOS, and is the earliest point at which the boot loader can take control of the boot process. If you install it in the MBR, when your machine boots, GRUB presents a boot prompt. You can then boot Fedora or any other operating system that you have configured the boot loader to boot.

- **The first sector of your boot partition** — This is recommended if you are already using another boot loader on your system. In this case, your other boot loader takes control first. You can then configure that boot loader to start GRUB, which then boots Fedora.
GRUB as a Secondary Boot Loader

If you install GRUB as a secondary boot loader, you must reconfigure your primary boot loader whenever you install and boot from a new kernel. The kernel of an operating system such as Microsoft Windows does not boot in the same fashion. Most users therefore use GRUB as the primary boot loader on dual-boot systems.

Figure 9.49. Boot Loader Installation

Note

If you have a RAID card, be aware that some BIOSes do not support booting from the RAID card. In cases such as these, the boot loader should not be installed on the MBR of the RAID array. Rather, the boot loader should be installed on the MBR of the same drive as the /boot/ partition was created.

If your system only uses Fedora, you should choose the MBR.

Click the Change Drive Order button if you would like to rearrange the drive order or if your BIOS does not return the correct drive order. Changing the drive order may be useful if you have multiple SCSI adapters, or both SCSI and IDE adapters, and you want to boot from the SCSI device.

If installing from USB, ensure boot loader is installed to hard drive

If you are installing Fedora from a USB, the boot loader will by default be installed to the MBR on the USB rather than the MBR on the hard drive. This will prevent the system booting once the installation is complete. To avoid this, select Change Device and reverse the order of the BIOS drives. /dev/sda is typically the hard drive and should be first in the BIOS Drive Order.
Chapter 9. Installing using anaconda

**Note**

While partitioning your hard drive, keep in mind that the BIOS in some older systems cannot access more than the first 1024 cylinders on a hard drive. If this is the case, leave enough room for the `/boot` Linux partition on the first 1024 cylinders of your hard drive to boot Linux. The other Linux partitions can be after cylinder 1024.

In `parted`, 1024 cylinders equals 528MB. For more information, refer to:

http://www.pcguide.com/ref/hdd/bios/sizeMB504-c.html

9.16.2. Rescue Mode

Rescue mode provides the ability to boot a small Fedora environment entirely from boot media or some other boot method instead of the system's hard drive. There may be times when you are unable to get Fedora running completely enough to access files on your system's hard drive. Using rescue mode, you can access the files stored on your system's hard drive, even if you cannot actually run Fedora from that hard drive. If you need to use rescue mode, try the following method:

- Boot an x86, AMD64, or Intel 64 system from any installation medium, such as CD, DVD, USB, or PXE, and type `linux rescue` at the installation boot prompt. Refer to Chapter 19, Basic System Recovery for a more complete description of rescue mode.

For additional information, refer to the Fedora Deployment Guide.

9.16.3. Alternative Boot Loaders

**GRUB** is the default bootloader for Fedora, but is not the only choice. A variety of open-source and proprietary alternatives to **GRUB** are available to load Fedora, including **LILO**, **SYSLINUX**, and **Acronis Disk Director Suite**.

**Important**

The Fedora Project does not support third-party boot loaders.

9.17. Package Group Selection

Now that you have made most of the choices for your installation, you are ready to confirm the default package selection or customize packages for your system.

The Package Installation Defaults screen appears and details the default package set for your Fedora installation. This screen varies depending on the version of Fedora you are installing.
Installing in text mode

If you install Fedora in text mode, you cannot make package selections. The installer automatically selects packages only from the base and core groups. These packages are sufficient to ensure that the system is operational at the end of the installation process, ready to install updates and new packages. To change the package selection, complete the installation, then use the Add/Remove Software application to make desired changes.

Figure 9.50. Package Group Selection

By default, the Fedora installation process loads a selection of software that is suitable for a system deployed as a basic server. Note that this installation does not include a graphical environment. To include a selection of software suitable for other roles, click the radio button that corresponds to one of the following options:

Graphical Desktop
This option provides the OpenOffice.org productivity suite, graphical tools such as the GIMP, and multimedia applications.

Software Development
This option provides the necessary tools to compile software on your Fedora system.

Web server
This option provides the Apache web server.

Minimal
This option provides only the packages essential to run Fedora. A minimal installation provides the basis for a single-purpose server or desktop appliance and maximizes performance and security on such an installation.
Chapter 9. Installing using anaconda

If you choose to accept the current package list, skip ahead to Section 9.18, “Installing Packages”.

To select a component, click on the checkbox beside it (refer to Figure 9.50, “Package Group Selection”).

To customize your package set further, select the Customize now option on the screen. Clicking Next takes you to the Package Group Selection screen.

9.17.1. Installing from Additional Repositories

You can define additional repositories to increase the software available to your system during installation. A repository is a network location that stores software packages along with metadata that describes them. Many of the software packages used in Fedora require other software to be installed. The installer uses the metadata to ensure that these requirements are met for every piece of software you select for installation.

The basic options are:

- The Installation Repo repository is automatically selected for you. This represents the collection of software available on your installation CD or DVD.
- The Fedora 17 - i386 repository contains the complete collection of software that was released as Fedora 17, with the various pieces of software in their versions that were current at the time of release. If you are installing from the Fedora 17 DVD or set of CDs, this option does not offer you anything extra. However, if you are installing from a Fedora Live CD, this option provides access to far more software than is included on the disk. Note that the computer must have access to the internet to use this option.
- The Fedora 17 - i386 - Updates repository contains the complete collection of software that was released as Fedora 17, with the various pieces of software in their most current stable versions. This option not only installs the software that you select, but makes sure that it is fully updated as well. Note that the computer must have access to the internet to use this option.

For more information about clustering with Fedora 17, refer to the Fedora 17 Cluster Suite Overview, available from https://access.redhat.com/knowledge/docs/manuals/.

![Edit Repository](image)

Figure 9.51. Adding a software repository
To include software from extra repositories, select **Add additional software repositories** and provide the location of the repository.

To edit an existing software repository location, select the repository in the list and then select **Modify repository**.

**Network Access Required**

If you change the repository information during a non-network installation, such as from a Fedora DVD, the installer prompts you for network configuration information.

If you change the repository information during a non-network installation, such as from a Fedora DVD, the installer prompts you for network configuration information.

![Select network interface](image)

**Figure 9.52. Select network interface**

1. Select an interface from the drop-down menu.
2. Click **OK**.

**Anaconda** activates the interface that you selected, then starts **NetworkManager** to allow you to configure the interface.
Figure 9.53. Network Connections

For details of how to use NetworkManager, refer to Section 9.6, “Setting the Hostname”

If you select Add additional software repositories, the Edit repository dialog appears. Provide a Repository name and the Repository URL for its location.

Fedora Software Mirrors

To find a Fedora software mirror near you, refer to http://mirrors.fedoraproject.org/publiclist/.

Once you have located a mirror, to determine the URL to use, find the directory on the mirror that contains a directory named repodata.

Once you provide information for an additional repository, the installer reads the package metadata over the network. Software that is specially marked is then included in the package group selection system.

Backtracking Removes Repository Metadata

If you choose Back from the package selection screen, any extra repository data you may have entered is lost. This allows you to effectively cancel extra repositories. Currently there is no way to cancel only a single repository once entered.
9.17.2. Customizing the Software Selection

Additional Language Support

Your Fedora system automatically supports the language that you selected at the start of the installation process. To include support for additional languages, select the package group for those languages from the Languages category.

Select Custom now to specify the software packages for your final system in more detail. This option causes the installation process to display an additional customization screen when you select Next.

Fedora divides the included software into package groups. For ease of use, the package selection screen displays these groups as categories.

You can select package groups, which group components together according to function (for example, X Window System and Editors), individual packages, or a combination of the two.

To view the package groups for a category, select the category from the list on the left. The list on the right displays the package groups for the currently selected category.

To specify a package group for installation, select the check box next to the group. The box at the bottom of the screen displays the details of the package group that is currently highlighted. None of the packages from a group will be installed unless the check box for that group is selected.

If you select a package group, Fedora automatically installs the base and mandatory packages for that group. To change which optional packages within a selected group will be installed, select the
Optional Packages button under the description of the group. Then use the check box next to an individual package name to change its selection.

In the package selection list on the right, you can use the context menu as a shortcut to select or deselect base and mandatory packages or all optional packages.

![Package Selection List Context Menu](image-url)

After you choose the desired packages, select Next to proceed. The installer checks your selection, and automatically adds any extra packages required to use the software you selected. When you have finished selecting packages, click Close to save your optional package selections and return to the main package selection screen.

The packages that you select are not permanent. After you boot your system, use the Add/Remove Software tool to either install new software or remove installed packages. To run this tool, from the main menu, select System → Administration → Add/Remove Software. The Fedora software management system downloads the latest packages from network servers, rather than using those on the installation discs.

9.17.2.1. Core Network Services

All Fedora installations include the following network services:

- centralized logging through syslog
- email through SMTP (Simple Mail Transfer Protocol)
- network file sharing through NFS (Network File System)
- remote access through SSH (Secure SHell)
- resource advertising through mDNS (multicast DNS)

The default installation also provides:

- network file transfer through HTTP (HyperText Transfer Protocol)
- printing through CUPS (Common UNIX Printing System)
- remote desktop access through VNC (Virtual Network Computing)

Some automated processes on your Fedora system use the email service to send reports and messages to the system administrator. By default, the email, logging, and printing services do not accept connections from other systems. Fedora installs the NFS sharing, HTTP, and VNC components without enabling those services.
You may configure your Fedora system after installation to offer email, file sharing, logging, printing and remote desktop access services. The SSH service is enabled by default. You may use NFS to access files on other systems without enabling the NFS sharing service.

### 9.18. Installing Packages

At this point there is nothing left for you to do until all the packages have been installed. How quickly this happens depends on the number of packages you have selected and your computer's speed.

Depending on the available resources, you might see the following progress bar while the installer resolves dependencies of the packages you selected for installation:

![Installation Starting](image)

**Figure 9.56. Starting installation**

Fedora reports the installation progress on the screen as it writes the selected packages to your system.

![Packages completed](image)

**Figure 9.57. Packages completed**

For your reference, a complete log of your installation can be found in `/root/install.log` once you reboot your system.

After installation completes, select **Reboot** to restart your computer. Fedora ejects any loaded discs before the computer reboots.

### 9.19. Installation Complete

Congratulations! Your Fedora installation is now complete!

The installation program prompts you to prepare your system for reboot. Remember to remove any installation media if it is not ejected automatically upon reboot.

After your computer's normal power-up sequence has completed, Fedora loads and starts. By default, the start process is hidden behind a graphical screen that displays a progress bar. Eventually, a `login:` prompt or a GUI login screen (if you installed the X Window System and chose to start X automatically) appears.

The first time you start your Fedora system in run level 5 (the graphical run level), the **FirstBoot** tool appears, which guides you through the Fedora configuration. Using this tool, you can set your
Chapter 9. Installing using anaconda

system time and date, install software, configure your machine to receive software updates, and more. **FirstBoot** lets you configure your environment at the beginning, so that you can get started using your Fedora system quickly.
Troubleshooting Installation on an Intel or AMD System

This section discusses some common installation problems and their solutions.

For debugging purposes, anaconda logs installation actions into files in the /tmp directory. These files include:

/tmp/anaconda.log
  general anaconda messages

/tmp/program.log
  all external programs run by anaconda

/tmp/storage.log
  extensive storage module information

/tmp/yum.log
  yum package installation messages

/tmp/syslog
  hardware-related system messages

If the installation fails, the messages from these files are consolidated into /tmp/anaconda-tb-identifier, where identifier is a random string.

All of the files above reside in the installer's ramdisk and are thus volatile. To make a permanent copy, copy those files to another system on the network using scp on the installation image (not the other way round).

10.1. You are unable to boot Fedora

10.1.1. Are You Unable to Boot With Your RAID Card?

If you have performed an installation and cannot boot your system properly, you may need to reinstall and create your partitions differently.

Some BIOSes do not support booting from RAID cards. At the end of an installation, a text-based screen showing the boot loader prompt (for example, GRUB: ) and a flashing cursor may be all that appears. If this is the case, you must repartition your system.

Whether you choose automatic or manual partitioning, you must install your /boot partition outside of the RAID array, such as on a separate hard drive. An internal hard drive is necessary to use for partition creation with problematic RAID cards.

You must also install your preferred boot loader (GRUB or LILO) on the MBR of a drive that is outside of the RAID array. This should be the same drive that hosts the /boot/ partition.

Once these changes have been made, you should be able to finish your installation and boot the system properly.
10.1.2. Is Your System Displaying Signal 11 Errors?

A signal 11 error, commonly known as a segmentation fault, means that the program accessed a memory location that was not assigned to it. A signal 11 error may be due to a bug in one of the software programs that is installed, or faulty hardware.

If you receive a fatal signal 11 error during your installation, it is probably due to a hardware error in memory on your system's bus. Like other operating systems, Fedora places its own demands on your system's hardware. Some of this hardware may not be able to meet those demands, even if they work properly under another OS.

Ensure that you have the latest installation updates and images. Review the online errata to see if newer versions are available. If the latest images still fail, it may be due to a problem with your hardware. Commonly, these errors are in your memory or CPU-cache. A possible solution for this error is turning off the CPU-cache in the BIOS, if your system supports this. You could also try to swap your memory around in the motherboard slots to check if the problem is either slot or memory related.

Another option is to perform a media check on your installation DVD. Anaconda, the installation program, has the ability to test the integrity of the installation media. It works with the DVD, hard drive ISO, and NFS ISO installation methods. The Fedora Project recommends that you test all installation media before starting the installation process, and before reporting any installation-related bugs (many of the bugs reported are actually due to improperly-burned DVDs). To use this test, type the following command at the boot: or yaboot: prompt:

```
linux mediacheck
```

For more information concerning signal 11 errors, refer to:

http://www.bitwizard.nl/sig11/

10.2. Trouble Beginning the Installation

10.2.1. Problems with Booting into the Graphical Installation

There are some video cards that have trouble booting into the graphical installation program. If the installation program does not run using its default settings, it tries to run in a lower resolution mode. If that still fails, the installation program attempts to run in text mode.

One possible solution is to use only a basic video driver during installation. You can do this either by selecting **Install system with basic video driver** on the boot menu, or using the **xdriver=vesa** boot option at the boot prompt. Alternatively, you can force the installer to use a specific screen resolution with the **resolution=** boot option. This option may be most helpful for laptop users. Another solution to try is the **driver=** option to specify the driver that should be loaded for your video card. If this works, you should report it as a bug, because the installer failed to detect your video card automatically. Refer to Chapter 11, Boot Options for more information on boot options.
To disable frame buffer support and allow the installation program to run in text mode, try using the `nofb` boot option. This command may be necessary for accessibility with some screen reading hardware.

10.3. Trouble During the Installation

10.3.1. No devices found to install Fedora Error Message

If you receive an error message stating **No devices found to install Fedora**, there is probably a SCSI controller that is not being recognized by the installation program.

10.3.2. Saving traceback messages

If **anaconda** encounters an error during the graphical installation process, it presents you with a crash reporting dialog box:

![Figure 10.1. The Crash Reporting Dialog Box](image-url)
Chapter 10. Troubleshooting Installation on an Intel or AMD System

Debug
shows you the details of the error:

![Exception Occurred](image)

An unhandled exception has occurred. This is most likely a bug. Please save a copy of the detailed exception and file a bug report.

firstboot 1.110.10 exception report

Traceback (most recent call last):
  File "/usr/sbin/firstboot", line 192, in <module>
    config.moduleList = loadModules(config.moduleDir, config.mode)
  File "/usr/lib/python2.6/site-packages/firstboot/loader.py", line 140, in loadModu
    obj.loadModules(mode=mode)
  File "/usr/lib/python2.6/site-packages/firstboot/moduleset.py", line 111, in loadI
    self.moduleList = loadModules(self.path, mode)
  File "/usr/lib/python2.6/site-packages/firstboot/loader.py", line 101, in loadModu
    obj = loaded.moduleClass()
  File "/usr/share/rhn/up2date_client/firstboot/rhsm_subscriptions.py", line 23, in 
    managergui.MainWindow._init__(self)
  File "/usr/share/rhsm/gui/managergui.py", line 255, in __init__

Figure 10.2. Details of the Crash

Save
saves details of the error locally or remotely:

Exit
exits the installation process.
If you select **Save** from the main dialog, you can choose from the following options:

- **Red Hat Global Support** automatically saves details of the error to a location within Red Hat Global Support using **FTP**.

- **ftp** saves details of the error to a remote directory using **FTP**.

- **local** saves details of the error to the local hard drive, in a directory that you select:

- **scp** saves details of the error to a remote host using **SCP**.

**Cancel** cancels saving the error report.
10.3.3. Trouble with Partition Tables

If you receive an error after the Disk Partitioning Setup (Section 9.12, “Disk Partitioning Setup”) phase of the installation saying something similar to

    The partition table on device hda was unreadable. To create new partitions it must be initialized, causing the loss of ALL DATA on this drive.

you may not have a partition table on that drive or the partition table on the drive may not be recognizable by the partitioning software used in the installation program.

Users who have used programs such as EZ-BIOS have experienced similar problems, causing data to be lost (assuming the data was not backed up before the installation began) that could not be recovered.

No matter what type of installation you are performing, backups of the existing data on your systems should always be made.

10.3.4. Using Remaining Space

You have a swap and a / (root) partition created, and you have selected the root partition to use the remaining space, but it does not fill the hard drive.

If your hard drive is more than 1024 cylinders, you must create a /boot partition if you want the / (root) partition to use all of the remaining space on your hard drive.

10.3.5. Other Partitioning Problems

If you create partitions manually, but cannot move to the next screen, you probably have not created all the partitions necessary for installation to proceed.

You must have the following partitions as a bare minimum:

- A / (root) partition
- A <swap> partition of type swap

**Note**

When defining a partition's type as swap, do not assign it a mount point. Anaconda automatically assigns the mount point for you.

10.4. Problems After Installation

10.4.1. Trouble With the Graphical GRUB Screen on an x86-based System?
If you are experiencing problems with GRUB, you may need to disable the graphical boot screen. To do this, temporarily alter the setting at boot time before changing it permanently.

At boot time, press Esc to reach the GRUB splash screen. Select the GRUB line, and type e.

Edit the kernel line to remove rhgb.

Press Enter to exit the editing mode.

Once the boot loader screen has returned, type b to boot the system.

If your problems with GRUB are now resolved and you want to make the change permanent, become the root user and edit the /etc/default/grub file.

Within the grub file, comment out the line which begins with GRUB_TERMINAL=console by inserting the # character at the beginning of the line.

Refresh the grub.cfg file by running grub2-mkconfig with root privileges. The changes you have made will then take effect.

You may re-enable the graphical boot screen by uncommenting (or adding) the above line back into the /etc/default/grub file.

**10.4.2. Blocked by a GRUB command line after upgrading?**

If you have restarted your machine after upgrading Fedora but cannot progress beyond the GRUB command line, you will need to issue commands to boot the operating system and then make the changes persistent once Fedora has loaded.

1. At the GRUB command line, display the superseded GRUB configuration file with the following command:

   ```
   cat (hdpartitionnumber,drivenumber)/grub/grub.conf
   ```

   `partitionnumber` and `drivenumber` refer to the location of your Fedora /boot directory. If you do not know the location, boot the machine using a Fedora live CD to find out and then reboot to return to the GRUB command line. Refer to Section E.4.1, “Device Names” for help with partition numbering.

2. In the GRUB configuration file, locate the first linux and initrd lines and paste them as individual commands. For example:

   ```
   linux /vmlinuz-3.3.0-1.fc17.x86_64 ro root=/dev/mapper/VolGroup-lv_root rd_LVM_LV=VolGroup/lv_root rd_LVM_LV=VolGroup/lv_swap rd_NO_LUKS rd_NO_MD rd_NO_DM LANG=en_US.UTF-8 SYSFONT=latarcyrheb-sun16 KEYTABLE=us rhgb quiet
   ```

   ```
   initrd /initramfs-3.3.0-1.fc17.x86_64.img
   ```

3. Run the boot command.

4. Once Fedora has loaded, refresh the GRUB configuration file to make the changes persistent:

   ```
   grub2-mkconfig -o /boot/grub2/grub.cfg
   ```
10.4.3. Booting into a Graphical Environment

If you have installed the X Window System but are not seeing a graphical desktop environment once you log into your system, you can start the X Window System graphical interface using the command `startx`.

Once you enter this command and press **Enter**, the graphical desktop environment is displayed.

Note, however, that this is just a one-time fix and does not change the log in process for future log ins.

To set up your system so that you can log in at a graphical login screen, you must edit one file, `/etc/inittab`, by changing just one number in the runlevel section. When you are finished, reboot the computer. The next time you log in, you are presented with a graphical login prompt.

Open a shell prompt. If you are in your user account, become root by typing the `su` command.

Now, type `gedit /etc/inittab` to edit the file with `gedit`. The file `/etc/inittab` opens. Within the first screen, a section of the file which looks like the following appears:

```
# Default runlevel. The runlevels used are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
#id:3:initdefault:
```

To change from a console to a graphical login, you should change the number in the line `id:3:initdefault:` from a 3 to a 5.

**Warning**

Change only the number of the default runlevel from 3 to 5.

Your changed line should look like the following:

```
#id:5:initdefault:
```

When you are satisfied with your change, save and exit the file using the `Ctrl+Q` keys. A window appears and asks if you would like to save the changes. Click **Save**.

The next time you log in after rebooting your system, you are presented with a graphical login prompt.

10.4.4. Problems with the X Window System (GUI)

If you are having trouble getting X (the X Window System) to start, you may not have installed it during your installation.
Problems with the X Server Crashing and Non-Root Users

If you want X, you can either install the packages from the Fedora installation media or perform an upgrade.

If you elect to upgrade, select the X Window System packages, and choose GNOME, KDE, or both, during the upgrade package selection process.

Refer to Section 18.3, “Switching to a Graphical Login” for more detail on installing a desktop environment.

10.4.5. Problems with the X Server Crashing and Non-Root Users

If you are having trouble with the X server crashing when anyone logs in, you may have a full file system (or, a lack of available hard drive space).

To verify that this is the problem you are experiencing, run the following command:

```
df -h
```

The `df` command should help you diagnose which partition is full. For additional information about `df` and an explanation of the options available (such as the `-h` option used in this example), refer to the `df` man page by typing `man df` at a shell prompt.

A key indicator is 100% full or a percentage above 90% or 95% on a partition. The `/home/` and `/tmp/` partitions can sometimes fill up quickly with user files. You can make some room on that partition by removing old files. After you free up some disk space, try running X as the user that was unsuccessful before.

10.4.6. Problems When You Try to Log In

If you did not create a user account in the firstboot screens, switch to a console by pressing `Ctrl`+`Alt`+`F2`, log in as root and use the password you assigned to root.

If you cannot remember your root password, boot your system as `linux single`.

If you are using an x86-based system and GRUB is your installed boot loader, type `e` for edit when the GRUB boot screen has loaded. You are presented with a list of items in the configuration file for the boot label you have selected.

Choose the line that starts with `kernel` and type `e` to edit this boot entry.

At the end of the `kernel` line, add:

```
single
```

Press `Enter` to exit edit mode.

Once the boot loader screen has returned, type `b` to boot the system.

Once you have booted into single user mode and have access to the `#` prompt, you must type `passwd root`, which allows you to enter a new password for root. At this point you can type `shutdown -r now` to reboot the system with the new root password.

If you cannot remember your user account password, you must become root. To become root, type `su -` and enter your root password when prompted. Then, type `passwd <username>`. This allows you to enter a new password for the specified user account.
Chapter 10. Troubleshooting Installation on an Intel or AMD System

If the graphical login screen does not appear, check your hardware for compatibility issues.

10.4.7. Is Your RAM Not Being Recognized?

Sometimes, the kernel does not recognize all of your memory (RAM). The following procedure will allow you to confirm this and then adjust the kernel if necessary.

1. Run the `cat /proc/meminfo` command and verify that the displayed quantity is the same as the known amount of RAM in your system. If they are not equal, you can first make a temporary change to confirm whether editing the kernel will be effective.

2. Reboot, and once you have loaded the GRUB boot screen, type `e` for edit.

3. You are presented with a list of items in the configuration file for the boot label you have selected. Choose the line that starts with `kernel` and type `e` to edit this boot entry.

4. At the end of the `kernel` line, add

   ```
   mem=xxM
   ```

   where `xx` equals the amount of RAM in your system, then press `Enter` to exit edit mode.

5. Once the boot loader screen has returned, type `b` to boot the system.

6. Run `cat /proc/meminfo` again. If the known amount of RAM in your system is now displayed, add the following line to the `/etc/grub.d/10_linux` file to make the change permanent:

   ```
   mem=xxM
   ```

   Replace `xx` with the amount of RAM you have in megabytes.

7. To update the `grub.cfg` file so that the change will take effect, run `grub2-mkconfig` with root privileges.

In `10_linux`, the above example would look similar to the following:

```
default=0
timeout=30
splashimage=(hd0,1)/grub/splash.xpm.gz
menuentry 'Fedora Linux, with Linux 3.1.0-0.rc6.git0.3.fc16.x86_64'
  set root=(hd0,1)
  linux /vmlinuz-(2.6.32.130.el6.i686 ro root=UUID=04a07c13-e6bf-6d5a-b207-002689545705
         mem=8192M
    initrd /initrd-(2.6.32.130.el6.i686.img
```

10.4.8. Your Printer Does Not Work

If you are not sure how to set up your printer or are having trouble getting it to work properly, try using the **Printer Configuration Tool**.

Type the `system-config-printer` command at a shell prompt to launch the **Printer Configuration Tool**. If you are not root, it prompts you for the root password to continue.
10.4.9. Apache HTTP Server or Sendmail stops responding during startup

If Apache HTTP Server (httpd) or Sendmail stops responding during startup, make sure the following line is in the /etc/hosts file:

```
127.0.0.1  localhost.localdomain  localhost
```
Part II. Advanced installation options

This part of the *Fedora Installation Guide* covers more advanced or uncommon methods of installing Fedora, including:

- boot options.
- installing without media.
- installing through VNC.
- using **kickstart** to automate the installation process.
Chapter 11.

Boot Options

The Fedora installation system includes a range of functions and options for administrators. To use boot options, enter `linux option` at the `boot:` prompt.

To access the `boot:` prompt on a system that displays a graphical boot screen, press the Esc key while the graphical boot screen is displayed.

If you specify more than one option, separate each of the options by a single space. For example:

```
linux option1 option2 option3
```

Anaconda Boot Options

The anaconda installer has many boot options, most are listed on the wiki [http://fedoraproject.org/wiki/Anaconda/Options](http://fedoraproject.org/wiki/Anaconda/Options).

Kernel Boot Options


Rescue Mode

The Fedora installation and rescue discs may either boot with rescue mode, or load the installation system. For more information on rescue discs and rescue mode, refer to [Section 11.6.3, “Booting Your Computer with the Rescue Mode”](#).

11.1. Configuring the Installation System at the Boot Menu

You can use the boot menu to specify a number of settings for the installation system, including:

- language
- display resolution
- interface type
- Installation method
- network settings
11.1.1. Specifying the Language
To set the language for both the installation process and the final system, specify the ISO code for that language with the `lang` option. Use the `keymap` option to configure the correct keyboard layout.

For example, the ISO codes `el_GR` and `gr` identify the Greek language and the Greek keyboard layout:

```
linux lang=el_GR keymap=gr
```

11.1.2. Configuring the Interface
To use a specific display resolution, enter `resolution=setting` as a boot option. For example, to set the display resolution to 1024×768, enter:

```
linux resolution=1024x768
```

To run the installation process in `text` mode, enter:

```
linux text
```

To enable support for a serial console, enter `serial` as an additional option.

Use `display=ip:0` to allow remote display forwarding. In this command, `ip` should be replaced with the IP address of the system on which you want the display to appear.

On the system you want the display to appear on, you must execute the command `xhost +remotehostname`, where `remotehostname` is the name of the host from which you are running the original display. Using the command `xhost +remotehostname` limits access to the remote display terminal and does not allow access from anyone or any system not specifically authorized for remote access.

11.1.3. Updating `anaconda`
You can install Fedora with a newer version of the `anaconda` installation program than the one supplied on your installation media.

The boot option

```
linux updates
```

presents you with a prompt that asks you for a disk image containing `anaconda` updates. You do not need to specify this option if you are performing a network installation and have already placed the updates image contents in `rhupdates/` on the server.

To load the `anaconda` updates from a network location instead, use:

```
linux updates=
```
followed by the URL for the location where the updates are stored.

### 11.1.4. Specifying the Installation Method

**askmethod** and **asknetwork** are deprecated.

The **askmethod** and **asknetwork** options are no longer available. Use **root=** to specify the installation method, and see Section 11.1.5, “Specifying the Network Settings” to configure network interfaces.

To specify the installation method from the **boot:** prompt, use the **repo** option. Refer to Table 11.1, “Installation methods” for the supported installation methods.

**Table 11.1. Installation methods**

<table>
<thead>
<tr>
<th>Installation method</th>
<th>Option format</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVD drive</td>
<td>**repo=cdrom:**device</td>
</tr>
<tr>
<td>Hard Drive</td>
<td>**repo=hd:**device/path</td>
</tr>
<tr>
<td>HTTP Server</td>
<td><strong>repo=<a href="http://host/path">http://host/path</a></strong></td>
</tr>
<tr>
<td>FTP Server</td>
<td><strong>repo=ftp://username:password@host/path</strong></td>
</tr>
<tr>
<td>NFS Server</td>
<td>**repo=nfs:**server:/path</td>
</tr>
<tr>
<td>ISO images on an NFS Server</td>
<td>**repo=nfsiso:**server:/path</td>
</tr>
</tbody>
</table>

### 11.1.5. Specifying the Network Settings

Normally, **anaconda** prompts you to configure a network interface if one is needed during installation. However, if your network cannot be configured automatically via DHCP and you need a network connection from the beginning of the installation, you can provide network settings with options at the **boot:** prompt. Such a connection may be required if you need to access an **updates.img** or kickstart file over a network, for example.

The available network configuration boot options include:

- **ip**
  - the IP address for system

- **netmask**
  - the netmask for the system

- **gateway**
  - the IP address of the network gateway

- **dns**
  - the IP address of the network DNS server

- **ksdevice**
  - the network device to use with these settings
This example configures the network settings for an installation system that uses the IP address 192.168.1.10 for interface eth0:

```
linux ip=192.168.1.10 netmask=255.255.255.0 gateway=192.168.1.1 dns=192.168.1.3 ksdevice=eth0
```

If you specify the network configuration and network device at the boot: prompt, these settings are used for the installation process and the Networking Devices and Configure TCP/IP dialogs do not appear.

### 11.2. Enabling Remote Access to the Installation System

You may access a graphical interface for the installation system from any other system. To remotely access the graphical display of an installation system, use client software that supports the VNC (Virtual Network Computing) display protocol.

#### Installing a VNC Client on Fedora

Fedora includes the VNC client `vncviewer`. To obtain `vncviewer`, install the `tigervnc` package.

The installation system supports two methods of establishing a VNC connection. You may start the installation, and manually login to the graphical display with a VNC client on another system. Alternatively, you may configure the installation system to automatically connect to a VNC client on the network that is running in listening mode.

#### 11.2.1. Enabling Remote Access with VNC

To enable remote graphical access to the installation system, enter two options at the prompt:

```
linux vnc vncpassword=qwerty
```

The `vnc` option enables the VNC service. The `vncpassword` option sets a password for remote access. The example shown above sets the password as `qwerty`.

#### VNC Passwords

The VNC password must be at least six characters long.

Specify the language, keyboard layout and network settings for the installation system with the screens that follow. You may then access the graphical interface through a VNC client. The installation system displays the correct connection setting for the VNC client:

```
Starting VNC...
The VNC server is now running.
Please connect to computer.mydomain.com:1 to begin the install...
Starting graphical installation...
```
You may then login to the installation system with a VNC client. To run the \texttt{vncviewer} client on Fedora, choose 	exttt{Applications} \rightarrow \texttt{Accessories} \rightarrow \texttt{VNC Viewer}, or type the command \texttt{vncviewer} in a terminal window. Enter the server and display number in the \texttt{VNC Server} dialog. For the example above, the \texttt{VNC Server} is \texttt{computer.mydomain.com:1}.

\section*{11.2.2. Connecting the Installation System to a VNC Listener}

To have the installation system automatically connect to a VNC client, first start the client in listening mode. On Fedora systems, use the \texttt{-listen} option to run \texttt{vncviewer} as a listener. In a terminal window, enter the command:

\begin{verbatim}
  vncviewer -listen
\end{verbatim}

\begin{warn}
\textbf{Firewall Reconfiguration Required}

By default, \texttt{vncviewer} uses TCP port 5500 when in listening mode. To permit connections to this port from other systems, choose \texttt{System} \rightarrow \texttt{Administration} \rightarrow \texttt{Firewall}. Select \texttt{Other ports}, and \texttt{Add}. Enter \texttt{5500} in the \texttt{Port(s)} field, and specify \texttt{tcp} as the \texttt{Protocol}.
\end{warn}

Once the listening client is active, start the installation system and set the VNC options at the \texttt{boot:} prompt. In addition to \texttt{vnc} and \texttt{vncpassword} options, use the \texttt{vncconnect} option to specify the name or IP address of the system that has the listening client. To specify the TCP port for the listener, add a colon and the port number to the name of the system.

For example, to connect to a VNC client on the system \texttt{desktop.mydomain.com} on the port 5500, enter the following at the \texttt{boot:} prompt:

\begin{verbatim}
  linux vnc vncpassword=qwerty vncconnect=desktop.mydomain.com:5500
\end{verbatim}

\section*{11.2.3. Enabling Remote Access with ssh}

To enable remote access to a text mode installation to monitor and debug the installer, use the \texttt{sshd=1} option at the \texttt{boot:} prompt:

\begin{verbatim}
  linux sshd=1
\end{verbatim}

You can then connect to the installation system with the \texttt{ssh} utility. The \texttt{ssh} command requires the name or IP address of the installation system, and a password if you specified one (for example, in a kickstart file).

\section*{11.3. Logging to a Remote System During the Installation}

By default, the installation process sends log messages to the console as they are generated. You may specify that these messages go to a remote system that runs a \texttt{syslog} service.
To configure remote logging, add the `syslog` option. Specify the IP address of the logging system, and the UDP port number of the log service on that system. By default, syslog services that accept remote messages listen on UDP port 514.

For example, to connect to a syslog service on the system `192.168.1.20`, enter the following at the `boot:` prompt:

```
linux syslog=192.168.1.20:514
```

### 11.3.1. Configuring a Log Server

Fedora uses `rsyslog` to provide a syslog service. The default configuration of `rsyslog` rejects messages from remote systems.

![Warning] Only Enable Remote Syslog Access on Secured Networks

The `rsyslog` configuration detailed below does not make use of any of the security measures available in `rsyslog` Crackers may slow or crash systems that permit access to the logging service, by sending large quantities of false log messages. In addition, hostile users may intercept or falsify messages sent to the logging service over the network.

To configure a Fedora system to accept log messages from other systems on the network, edit the file `/etc/rsyslog.conf`. You must use `root` privileges to edit the file `/etc/rsyslog.conf`. Uncomment the following lines by removing the hash preceding them:

```
$ModLoad imudp.so
$UDPServerRun 514
```

Restart the `rsyslog` service to apply the change:

```
su -c '/sbin/service rsyslog restart'
```

Enter the `root` password when prompted.

![Warning] Firewall Reconfiguration Required

By default, the syslog service listens on UDP port 514. To permit connections to this port from other systems, choose `System` → `Administration` → `Firewall`. Select `Other ports`, and `Add`. Enter `514` in the `Port(s)` field, and specify `udp` as the `Protocol`.

### 11.4. Automating the Installation with Kickstart

You can allow an installation to run unattended by using Kickstart. A `Kickstart` file specifies settings for an installation. Once the installation system boots, it can read a Kickstart file and carry out the installation process without any further input from a user.
Every Installation Produces a Kickstart File

The Fedora installation process automatically writes a Kickstart file that contains the settings for the installed system. This file is always saved as /root/anaconda-ks.cfg. You may use this file to repeat the installation with identical settings, or modify copies to specify settings for other systems.

Important — Kickstart installations and firstboot

Firstboot does not run after a system is installed from a Kickstart file unless a desktop and the X Window System were included in the installation and graphical login was enabled. Either specify a user with the user option in the Kickstart file before installing additional systems from it (refer to Section 15.4, “Kickstart Options” for details) or log into the installed system with a virtual console as root and add users with the adduser command.

Fedora includes a graphical application to create and modify Kickstart files by selecting the options that you require. Use the package system-config-kickstart to install this utility. To load the Fedora Kickstart editor, choose Applications → System Tools → Kickstart.

Kickstart files list installation settings in plain text, with one option per line. This format lets you modify your Kickstart files with any text editor, and write scripts or applications that generate custom Kickstart files for your systems.

To automate the installation process with a Kickstart file, use the ks option to specify the name and location of the file:

```
linux ks=location/kickstart-file.cfg
```

You may use Kickstart files that are held on either removable storage, a hard drive, or a network server. Refer to Table 11.2, "Kickstart sources" for the supported Kickstart sources.

### Table 11.2. Kickstart sources

<table>
<thead>
<tr>
<th>Kickstart source</th>
<th>Option format</th>
</tr>
</thead>
<tbody>
<tr>
<td>DVD drive</td>
<td>ks=cdrom:/directory/ks.cfg</td>
</tr>
<tr>
<td>Hard Drive</td>
<td>ks=hd:/device/directory/ks.cfg</td>
</tr>
<tr>
<td>Other Device</td>
<td>ks=file:/device/directory/ks.cfg</td>
</tr>
<tr>
<td>HTTP Server</td>
<td>ks=<a href="http://server.mydomain.com/directory/ks.cfg">http://server.mydomain.com/directory/ks.cfg</a></td>
</tr>
<tr>
<td>FTP Server</td>
<td>ks=ftp://server.mydomain.com/directory/ks.cfg</td>
</tr>
<tr>
<td>NFS Server</td>
<td>ks=nfs:server.mydomain.com:/directory/ks.cfg</td>
</tr>
</tbody>
</table>

To obtain a Kickstart file from a script or application on a Web server, specify the URL of the application with the ks= option. If you add the option kssendmac, the request also sends HTTP.
headers to the Web application. Your application can use these headers to identify the computer. This line sends a request with headers to the application http://server.mydomain.com/kickstart.cgi:

```
linux ks=http://server.mydomain.com/kickstart.cgi kssendmac
```

## 11.5. Enhancing Hardware Support

By default, Fedora attempts to automatically detect and configure support for all of the components of your computer. Fedora supports the majority of hardware in common use with the software drivers that are included with the operating system. To support other devices you may supply additional drivers during the installation process, or at a later time.

### 11.5.1. Overriding Automatic Hardware Detection

For some models of device automatic hardware configuration may fail, or cause instability. In these cases, you may need to disable automatic configuration for that type of device, and take additional steps to manually configure the device after the installation process is complete.

**Check the Release Notes**

Refer to the Release Notes for information on known issues with specific devices.

To override the automatic hardware detection, use one or more of the following options:

**Table 11.3. Hardware Options**

<table>
<thead>
<tr>
<th>Compatibility</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable all hardware detection</td>
<td>noprobe</td>
</tr>
<tr>
<td>Disable graphics, keyboard, and mouse detection</td>
<td>headless</td>
</tr>
<tr>
<td>Disable passing keyboard and mouse information to stage 2 of the installation program</td>
<td>nopass</td>
</tr>
<tr>
<td>Use basic VESA driver for video</td>
<td>xdriver=vesa</td>
</tr>
<tr>
<td>Disable shell access on virtual console 2 during installation</td>
<td>noshell</td>
</tr>
<tr>
<td>Disable advanced configuration and power interface (ACPI)</td>
<td>acpi=off</td>
</tr>
<tr>
<td>Disable machine check exception (MCE) CPU self-diagnosis.</td>
<td>nomce</td>
</tr>
<tr>
<td>Disable non-uniform memory access on the AMD64 architecture</td>
<td>numa-off</td>
</tr>
<tr>
<td>Force kernel to detect a specific amount of memory, where (xxx) is a value in megabytes</td>
<td>mem=xxxm</td>
</tr>
<tr>
<td>Enable DMA only for IDE and SATA drives</td>
<td>libata.dma=1</td>
</tr>
<tr>
<td>Disable BIOS-assisted RAID</td>
<td>nodmraid</td>
</tr>
<tr>
<td>Disable Firewire device detection</td>
<td>nofirewire</td>
</tr>
<tr>
<td>Disable parallel port detection</td>
<td>noparport</td>
</tr>
<tr>
<td>Disable PC Card (PCMCIA) device detection</td>
<td>nopcmcia</td>
</tr>
</tbody>
</table>
### 11.6. Using the Maintenance Boot Modes

**11.6.1. Loading the Memory (RAM) Testing Mode**

Faults in memory modules may cause your system to freeze or crash unpredictably. In some cases, memory faults may only cause errors with particular combinations of software. For this reason, you should test the memory of a computer before you install Fedora for the first time, even if it has previously run other operating systems.

Fedora includes the **Memtest86+** memory testing application. To boot your computer in memory testing mode, choose **Memory test** at the boot menu. The first test starts immediately. By default, **Memtest86+** carries out a total of ten tests.

In most cases, a single successful pass with **Memtest86+** is sufficient to verify that your RAM is in good condition. In some rare circumstances, however, errors that went undetected on the first pass might appear on subsequent passes. To perform a thorough test of the RAM on an important system, leave **Memtest86+** running overnight or for a few days.


To halt the tests and reboot your computer, enter **Esc** at any time.

**11.6.2. Verifying boot media**

You can test the integrity of an ISO-based installation source before using it to install Fedora. These sources include DVD, and ISO images stored on a hard drive or NFS server. Verifying that the ISO images are intact before you attempt an installation helps to avoid problems that are often encountered during installation.

Fedora offers you two ways to test installation ISOs:

- select **OK** at the prompt to test the media before installation when booting from the Fedora DVD

---

<table>
<thead>
<tr>
<th>Compatibility</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable all probing of network hardware</td>
<td>nonet</td>
</tr>
</tbody>
</table>

**Additional Screen**

The **isa** option causes the system to display an additional text screen at the beginning of the installation process. Use this screen to configure the ISA devices on your computer.

**Important**

Other kernel boot options have no particular meaning for **anaconda** and do not affect the installation process. However, if you use these options to boot the installation system, **anaconda** will preserve them in the bootloader configuration.
Chapter 11. Boot Options

- boot Fedora with the option `mediacheck` option.

### 11.6.3. Booting Your Computer with the Rescue Mode

You may boot a command-line Linux system from either a rescue disc or an installation disc, without installing Fedora on the computer. This enables you to use the utilities and functions of a running Linux system to modify or repair systems that are already installed on your computer.

The rescue disc starts the rescue mode system by default. To load the rescue system with the installation disc, choose `Rescue installed system` from the boot menu.

Specify the language, keyboard layout and network settings for the rescue system with the screens that follow. The final setup screen configures access to the existing system on your computer.

By default, rescue mode attaches an existing operating system to the rescue system under the directory `/mnt/sysimage/`.

### 11.6.4. Upgrading your computer

A previous boot option, `upgrade`, has been superceded by a stage in the installation process where the installation program prompts you to upgrade or reinstall earlier versions of Fedora that it detects on your system.

However, the installation program may not correctly detect a previous version of Fedora if the contents of the `/etc/redhat-release` file have changed. The boot option `upgradeany` relaxes the test that the installation program performs and allows you to upgrade a Fedora installation that the installation program has not correctly identified.
Chapter 12.

Installing Without Media

**Linux Required**

This procedure assumes you are already using Fedora or another relatively modern Linux distribution, and the **GRUB** boot loader. It also assumes you are a somewhat experienced Linux user.

This section discusses how to install Fedora on your system without making any additional physical media. Instead, you can use your existing **GRUB** boot loader to start the installation program.

### 12.1. Retrieving Boot Files

To perform an installation without media or a PXE server, your system must have two files stored locally, a kernel and an initial RAM disk.

Copy the `vmlinuz` and `initrd.img` files from a Fedora DVD (or DVD image) to the `/boot/` directory, renaming them to `vmlinuz-install` and `initrd.img-install`. You must have root privileges to write files into the `/boot/` directory.

### 12.2. Editing the GRUB Configuration

The **GRUB** boot loader uses the configuration files `/etc/default/grub` and the scripts in `etc/grub.d/`. To configure **GRUB** to boot from the new files, add a boot stanza to `/etc/grub.d/40_custom` that refers to them.

A minimal boot stanza looks like the following listing:

```plaintext
menuentry "Fedora Linux" {
    set root=(hd0,1)
    linux /vmlinuz-install
    initrd /initrd.img-install
}
```

You will also need to specify the location of the second stage installer image by adding an option to the end of the `linux` line of the boot stanza. For example:

```plaintext
linux /vmlinuz-install stage2=http://my.internal.server/17/x86_64/os/
```

If the second stage image and the package repositories you will be downloading from are on the same server, use the `repo=` option instead.

You may wish to add additional options to the end of the `linux` line, which will set preliminary options in **Anaconda** that the user normally sets interactively. For a list of available installer boot options, refer to **Chapter 11, Boot Options**.

The following options are generally useful for medialess installations:

- `ip=`
- `repo=`
Chapter 12. Installing Without Media

- `lang=`
- `keymap=`
- `ksdevice=` (if installation requires an interface other than eth0)
- `vnc` and `vncpassword=` for a remote installation

When you are finished, run `grub2-mkconfig` with root privileges and open the `grub.cfg` file to view the updated configuration. Locate your new menu entry stanza and determine its place in the stanza order.

Finally, change the `GRUB_DEFAULT` option in `/etc/default/grub` to point to the new stanza you added. 0 will refer to the first stanza, 1 to the second, and so on. For example:

```
grub_default=0
```

Alternatively, specify the menu entry title. This is particularly useful if you have a number of menu entries across the various script files.

```
grub_default="Fedora Linux"
```

**12.3. Booting to Installation**

Reboot the system. **GRUB** boots the installation kernel and RAM disk, including any options you set. You may now refer to the appropriate chapter in this guide for the next step. If you chose to install remotely using VNC, refer to Section 11.2, “Enabling Remote Access to the Installation System” for assistance in connecting to the remote system.
Setting Up an Installation Server

**Experience Required**

This appendix is intended for users with previous Linux experience. If you are a new user, you may want to install using minimal boot media or the distribution DVD instead.

**Warning**

The instructions in this appendix configures an automated install server. The default configuration includes destruction of all existing data on all disks for hosts that install using this method. This is often different from other network install server configurations which may provide for an interactive installation experience.

Fedora allows for installation over a network using the NFS, FTP, or HTTP protocols. A network installation can be started from a boot CD-ROM, a bootable flash memory drive, or by using the `repo=` boot option with the Fedora DVD. Alternatively, if the system to be installed contains a network interface card (NIC) with Pre-Execution Environment (PXE) support, it can be configured to boot from files on another networked system rather than local media such as a DVD.

For a PXE network installation, the client's NIC with PXE support sends out a broadcast request for DHCP information. The DHCP server provides the client with an IP address, other network information such as name server, the IP address or hostname of the `tftp` server (which provides the files necessary to start the installation program), and the location of the files on the `tftp` server. This is possible because of PXELINUX, which is part of the `syslinux` package.

In the past, administrators needed to perform a great deal of manual configuration to produce an installation server. However, if you have a server running Fedora or a similar operating system on your local network, you can use `cobbler` to perform these tasks. To configure a PXE server manually, see Section 13.5, "Manually configure a PXE server".

To perform the tasks in this section, switch to the `root` account with the command `su -`. As an alternative, you can run a command with the `-c` option, using the form `su -c 'command'`.

**13.1. Setting Up cobbler**

To install `cobbler` use the following command:

```
yum -y install cobbler
```

The `cobbler` command can check its own settings for validity and report the results. Run the following command to check the settings:

```
cobbler check
```

Verify SELinux is configured for `cobbler`:
Chapter 13. Setting Up an Installation Server

```bash
setsebool -P httpd_can_network_connect_cobbler 1
```

Other SELinux booleans may apply, and can be listed with:

```bash
getsebool -a|grep cobbler
```

Change the settings in the `/etc/cobbler/settings` file to reflect the IP address information for the server. You must change at least the `server` and `next_server` options, although these options may point to the same IP address.

If you are not already running a DHCP server, you should also change the `manage_dhcp` option to `1`. If you are running a DHCP server, configure it according to the instructions found in the `syslinux` package documentation. For more information, refer to your local files `/usr/share/doc/syslinux-version/syslinux.doc` and `/usr/share/doc/syslinux-version/pxelinux.doc`.

### 13.2. Setting Up the Distribution

To set up a distribution from a full Fedora DVD or ISO image, use this procedure.

#### Network Locations

To create a local mirror from an existing network source, skip this section and refer instead to Section 13.3, “Mirroring a Network Location”.

1. If you are using a DVD disc or ISO image, Create a directory mount point:

   ```bash
   mkdir /mnt/dvd
   ```

   To mount a physical DVD disc, use the following command:

   ```bash
   mount -o context=system_u:object_r:httpd_sys_content_t:s0 /dev/dvd /mnt/dvd
   ```

   To mount a DVD ISO image, use the following command:

   ```bash
   mount -ro loop,context=system_u:object_r:httpd_sys_content_t:s0 /path/to/image.iso /mnt/dvd
   ```

   If SELinux enabled, use the default label

   If SELinux is enabled, use the default `iso9660_t` label instead of `httpd_sys_content_t`.

2. To support NFS installation, create a file `/etc/exports` and add the following line to it:

   ```bash
   /mnt/dvd *(ro,async)
   ```
Start the NFS server using the following commands:

```
/sbin/service rpcbind start /sbin/service nfs start
```

3. To support HTTP installation, use `yum` to install the Apache web server if it is not already installed:

```
yum -y install httpd
```

Make a link to the mounted disc in the Apache public content area:

```
ln -s /mnt/dvd /var/www/html/distro
```

### 13.3. Mirroring a Network Location

If you do not have discs or ISO images for a distribution, you can use `cobbler` to create an installation server. The `cobbler` command can fetch the distribution over the network as part of the import process.

Locate the distribution on the network. The location may be on the local network or reached at a remote site via FTP, HTTP, or rsync protocols.

### 13.4. Importing the Distribution

To offer a distribution through more than one installation method, perform additional `cobbler import` tasks using a different name for each method. For best results, use the installation method as part of the name, so it appears in the client's boot menu.

1. To import the DVD disc or ISO distribution into `cobbler`, run this command:

   ```
cobbler import --path=/mnt/dvd --name=distro_name
   ```

   For `distro_name`, substitute a meaningful name for the distribution.

   To import a local or remote network distribution into `cobbler`, run this command. Replace `network_URI` with the URI you found in Section 13.3, “Mirroring a Network Location”, and `distro_name` as above:

   ```
cobbler import --path=network_URI --name=distro_name
   ```

**Importing a Source**

When `cobbler` imports a distribution with the commands above, it copies all the files to the server's local storage, which may take some time.

If you do not want to make local copies of the distribution because clients can already reach its location, use the `--available-as` option.

```
cobbler import --path=/mnt/dvd --name=distro_name --available-as=network_URI
```
Chapter 13. Setting Up an Installation Server

```plaintext
  cobbler import --path=network_URI --name=distro_name --available-as=network_URI
```

For `network_URI`, substitute the appropriate network location of the distribution. This URI indicates how the server makes the distribution available to its clients. The examples above assume that your `cobbler` server reaches the mirror location at the same URI as the clients. If not, substitute an appropriate URI for the `--path` option. The following examples are URI locations that work if you have been following the procedures in this section, and your server's IP address is `192.168.1.1`:

- nfs://192.168.1.1:/mnt/dvd
- http://192.168.1.1:/distro

If necessary, replace `192.168.1.1` with the IP address for your `cobbler` server.

2. Run the command `cobbler sync` to apply the changes. To check that your `cobbler` server is listening on the correct ports, use the `netstat -lp` command.

### Firewall Considerations

Depending on your server's configuration, you may need to use the `system-config-securitylevel` command to permit access to some or all of these network services:

- 67 or bootps, for the DHCP/BOOTP server
- 69 or tftp, for providing the PXE loader
- 80 or http, if the `cobbler` server is to provide HTTP installation service
- 20 and 21 or ftp, if the `cobbler` server is to provide FTP installation service
- 111 or sunrpc, if the `cobbler` server is to provide NFS installation service

## 13.5. Manually configure a PXE server

The following steps must be performed to prepare for a PXE installation:

1. Configure the network (NFS, FTP, HTTP) server to export the installation tree.
2. Configure the files on the `tftp` server necessary for PXE booting.
3. Configure which hosts are allowed to boot from the PXE configuration.
4. Start the `tftp` service.
5. Configure DHCP.
6. Boot the client, and start the installation.

### 13.5.1. Setting up the Network Server
First, configure an NFS, FTP, or HTTP server to export the entire installation tree for the version and variant of Fedora to be installed. Refer to Section 5.1, “Preparing for a Network Installation” for detailed instructions.

### 13.5.2. PXE Boot Configuration

The next step is to copy the files necessary to start the installation to the tftp server so they can be found when the client requests them. The tftp server is usually the same server as the network server exporting the installation tree.

BIOS and EFI configuration differs for this procedure.

#### 13.5.2.1. Configuring for BIOS

1. If tftp-server is not yet installed, run `yum install tftp-server`.

2. In the tftp-server config file at `/etc/xinet.d/tftp`, change the disabled parameter from yes to no.

3. Configure your DHCP server to use the boot images packaged with SYSLINUX. (If you do not have a DHCP server installed, refer to the DHCP Servers chapter in the Fedora Deployment Guide.)

A sample configuration in `/etc/dhcp/dhcpd.conf` might look like:

```plaintext
option space pxelinux;
option pxelinux.magic code 208 = string;
option pxelinux.configfile code 209 = text;
option pxelinux.pathprefix code 210 = text;
option pxelinux.reboottime code 211 = unsigned integer 32;

subnet 10.0.0.0 netmask 255.255.255.0 {
    option routers 10.0.0.254;
    range 10.0.0.2 10.0.0.253;
    class "pxeclients" {
        match if substring (option vendor-class-identifier, 0, 9) = "PXEClient";
        next-server 10.0.0.1;

        if option arch = 00:06 {
            filename "pxelinux/bootia32.efi";
        } else if option arch = 00:07 {
            filename "pxelinux/bootx64.efi";
        } else {
            filename "pxelinux/pxelinux.0";
        }
    }
}

host example-ia32 {
    hardware ethernet XX:YY:ZZ:11:22:33;
    fixed-address 10.0.0.2;
}
```

4. You now need the `pxelinux.0` file from the SYSLINUX package installed with Fedora. Create a `pxelinux` directory within `tftpboot` and copy `pxelinux.0` into it:
Chapter 13. Setting Up an Installation Server

5. Create a `pxelinux.cfg` directory within `pxelinux`:

   ```
   mkdir /var/lib/tftpboot/pxelinux/pxelinux.cfg
   ```

6. Add a config file to this directory. The file should either be named `default` or named after the IP address. For example, if your machine's IP address is 10.0.0.1, the filename would be `0A000001`.

   A sample config file at `/var/lib/tftpboot/pxelinux/pxelinux.cfg/default` might look like:

   ```
   default vesamenu.c32
   prompt 1
   timeout 600
   display boot.msg
   
   label linux
   menu label ^Install or upgrade an existing system
   menu default
   kernel vmlinuz
   append initrd=initrd.img inst.repo=http://dl.fedoraproject.org/pub/fedora/linux/development/17/x86_64/os/
   label vesa
   menu label Install system with ^basic video driver
   kernel vmlinuz
   append initrd=initrd.img xdriver=vesa nomodeset
   label rescue
   menu label ^Rescue installed system
   kernel vmlinuz
   append initrd=initrd.img rescue
   label local
   menu label Boot from ^local drive
   localboot 0xffff
   label memtest86
   menu label ^Memory test
   kernel memtest
   append -
   ```

   If both the stage 2 installer image and the package repositories you intend to download from are on the same server, use the `repo=` boot option. If they are on separate servers, use `stage2=` instead.

   For instructions on how to specify the installation source, refer to Chapter 8, Configuring Installation Source

7. Copy the splash image into your `tftp` root directory:

   ```
   cp /boot/grub/splash.xpm.gz /var/lib/tftpboot/pxelinux/splash.xpm.gz
   ```

8. Copy the boot images into your `tftp` root directory:
13.5.2.2. Configuring for EFI

1. If `tftp-server` is not yet installed, run `yum install tftp-server`.

2. In the `tftp-server` config file at `/etc/xinet.d/tftp`, change the `disabled` parameter from `yes` to `no`.

3. Create a directory path within `tftpboot` for the EFI boot images, and then copy them from your boot directory:

   ```
   mkdir /var/lib/tftpboot/pxelinux
   mkdir /var/lib/tftpboot/pxelinux/bootx64.efi
   cp /boot/efi/EFI/redhat/grub.efi /var/lib/tftpboot/pxelinux/bootx64.efi
   ```

4. Configure your DHCP server to use the EFI boot images packaged with GRUB. (If you do not have a DHCP server installed, refer to the `DHCP Servers` chapter in the `Fedora Deployment Guide`.)

   A sample configuration in `/etc/dhcp/dhcpd.conf` might look like:

   ```
   option space PXE;
   option PXE.mtftp-ip code 1 = ip-address;
   option PXE.mtftp-cport code 2 = unsigned integer 16;
   option PXE.mtftp-sport code 3 = unsigned integer 16;
   option PXE.mtftp-tmout code 4 = unsigned integer 8;
   option PXE.mtftp-delay code 5 = unsigned integer 8;
   option arch code 93 = unsigned integer 16; # RFC4578
   subnet 10.0.0.0 netmask 255.255.255.0 {
       option routers 10.0.0.254;
       range 10.0.0.2 10.0.0.253;
       class "pxeclients" {
           match if substring (option vendor-class-identifier, 0, 9) = "PXEClient";
           next-server 10.0.0.1;
           if option arch = 00:06 {
               filename "pxelinux/bootia32.efi";
           } else if option arch = 00:07 {
               filename "pxelinux/bootx64.efi";
           } else {
               filename "pxelinux/pxelinux.0";
           }
       }
   }
   host example-ia32 {
       hardware ethernet XX:YY:ZZ:11:22:33;
       fixed-address 10.0.0.2;
   }
   ```
5. Create a `pxelinux.cfg` directory within `pxelinux`:

```bash
mkdir /var/lib/tftpboot/pxelinux/pxelinux.cfg
```

6. Add a config file to this directory. The file should either be named `efidefault` or named after the IP address. For example, if your machine's IP address is 10.0.0.1, the filename would be `0A000001`.

A sample config file at `/var/lib/tftpboot/pxelinux/pxelinux.cfg/efidefault` might look like:

```bash
default=0
timeout=1
splashimage=(nd)/splash.xpm.gz
hiddenmenu
title RHEL
   root (nd)
   kernel /rawhide-x86_64/vmlinuz
   initrd /rawhide-x86_64/initrd.img
```

For instructions on how to specify the installation source, refer to Chapter 8, Configuring Installation Source

7. Copy the splash image into your `tftp` root directory:

```bash
cp /boot/grub/splash.xpm.gz /var/lib/tftpboot/pxelinux/splash.xpm.gz
```

8. Copy the boot images into your `tftp` root directory:

```bash
cp /path/to/x86_64/os/images/pxeboot/{vmlinuz,initrd.img} /var/lib/tftpboot/pxelinux/
   rawhide-x86_64/
```

9. Reboot the system, and select the network device as your boot device when prompted.

**13.5.3. Starting the tftp Server**

On the DHCP server, verify that the `tftp-server` package is installed with the command `rpm -q tftp-server`.

`tftp` is an xinetd-based service. Configure xinetd to process tftp requests by editing `/etc/xinetd.d/tftp` so that `disable = no`.

Start the `tftp` service with the following commands:

```bash
systemctl start xinetd.service
systemctl enable xinetd.service
```

These commands configure the `tftp` and `xinetd` services to immediately turn on and also configure them to start at boot.

**13.5.4. Adding a Custom Boot Message**
13.5.5. Performing the PXE Installation

For instructions on how to configure the network interface card with PXE support to boot from the network, consult the documentation for the NIC. It varies slightly per card.

If your NIC does not support PXE booting, you can still PXE boot your system by using the gPXE bootloader. The Fedora Project does not distribute gPXE — refer to the Etherboot Project website at http://etherboot.org/wiki/start for more information.

After the system boots the installation program, refer to the Chapter 9, Installing using anaconda.
Installing Through VNC

The Fedora installer (anaconda) offers you two interactive modes of operation. The original mode is a text-based interface. The newer mode uses GTK+ and runs in the X Window environment. This chapter explains how you can use the graphical installation mode in environments where the system lacks a proper display and input devices typically associated with a workstation. This scenario is typical of systems in datacenters, which are often installed in a rack environment and do not have a display, keyboard, or mouse. Additionally, a lot of these systems even lack the ability to connect a graphical display. Given that enterprise hardware rarely needs that ability at the physical system, this hardware configuration is acceptable.

Even in these environments, however, the graphical installer remains the recommended method of installation. The text mode environment lacks a lot of capabilities found in the graphical mode. Many users still feel that the text mode interface provides them with additional power or configuration ability not found in the graphical version. The opposite is true. Much less development effort is put in to the text-mode environment and specific things (for example, LVM configuration, partition layout, package selection, and bootloader configuration) are deliberately left out of the text mode environment. The reasons for this are:

- Less screen real estate for creating user interfaces similar to those found in the graphical mode.
- Difficult internationalization support.
- Desire to maintain a single interactive installation code path.

Anaconda therefore includes a Virtual Network Computing (VNC) mode that allows the graphical mode of the installer to run locally, but display on a system connected to the network. Installing in VNC mode provides you with the full range of installation options, even in situations where the system lacks a display or input devices.

14.1. VNC Viewer

Performing a VNC installation requires a VNC viewer running on your workstation or other terminal computer. Locations where you might want a VNC viewer installed:

- Your workstation
- Laptop on a datacenter crash cart

VNC is open source software licensed under the GNU General Public License.

- VNC clients are available in the repositories of most Linux distributions. Use your package manager to search for a client for your chosen distribution. For example, on Fedora, install the tigervnc package:

  ```
  # yum install tigervnc
  ```

- TightVNC is available for Windows at http://www.tightvnc.com/

- MacOS X includes built-in VNC support as of version 10.5. In the Finder, click the Go menu and choose Connect to Server. In the server address field, you can type vnc://SERVER:DISPLAY, where SERVER is the IP address or DNS host name of the VNC server you wish to connect to and DISPLAY is the VNC display number (usually 1), and click Connect.

Once you have verified you have a VNC viewer available, it's time to start the installation.
14.2. VNC Modes in Anaconda

Anaconda offers two modes for VNC installation. The mode you select will depend on the network configuration in your environment.

14.2.1. Direct Mode

Direct mode VNC in anaconda is when the client initiates a connection to the VNC server running in anaconda. Anaconda will tell you when to initiate this connection in the VNC viewer. Direct mode can be activated by either of the following commands:

- Specify `vnc` as a boot argument.
- Specify the `vnc` command in the kickstart file used for installation.

When you activate VNC mode, anaconda will complete the first stage of the installer and then start VNC to run the graphical installer. The installer will display a message on the console in the following format:

```
Running anaconda VERSION, the PRODUCT system installer - please wait...
```

Anaconda will also tell you the IP address and display number to use in your VNC viewer. At this point, you need to start the VNC viewer and connect to the target system to continue the installation. The VNC viewer will present anaconda to you in graphical mode.

There are some disadvantages to direct mode, including:

- Requires visual access to the system console to see the IP address and port to connect the VNC viewer to.
- Requires interactive access to the system console to complete the first stage of the installer.

If either of these disadvantages would prevent you from using direct mode VNC in anaconda, then connect mode is probably more suited to your environment.

14.2.2. Connect Mode

Certain firewall configurations or instances where the target system is configured to obtain a dynamic IP address may cause trouble with the direct VNC mode in anaconda. In addition, if you lack a console on the target system to see the message that tells you the IP address to connect to, then you will not be able to continue the installation.

The VNC connect mode changes how VNC is started. Rather than anaconda starting up and waiting for you to connect, the VNC connect mode allows anaconda to automatically connect to your view. You won't need to know the IP address of the target system in this case.

To activate the VNC connect mode, pass the `vnc vncconnect` boot parameter:

```
boot: linux vnc vncconnect=HOST[:port]
```

Replace HOST with your VNC viewer's IP address or DNS host name. Specifying the port is optional. Before starting the installation process on the target system, start up your VNC viewer and have it wait for an incoming connection.

Start the installation and when your VNC viewer displays the graphical installer, you are ready to go.
14.3. Installation Using VNC

Now that you have installed a VNC viewer application and selected a VNC mode for use in anaconda, you are ready to begin the installation.

14.3.1. Installation Example

The easiest way to perform an installation using VNC is to connect another computer directly to the network port on the target system. The laptop on a datacenter crash cart usually fills this role. If you are performing your installation this way, make sure you follow these steps:

1. Connect the laptop or other workstation to the target system using a crossover cable. If you are using regular patch cables, make sure you connect the two systems using a small hub or switch. Most recent Ethernet interfaces will automatically detect if they need to be crossover or not, so it may be possible to connect the two systems directly using a regular patch cable.

2. Configure the VNC viewer system to use a RFC 1918 address with no gateway. This private network connection will only be used for the purpose of installation. Configure the VNC viewer system to be 192.168.100.1/24. If that address is in use, just pick something else in the RFC 1918 address space that is available to you.

3. Start the installation on the target system.
   a. Booting the installation DVD.
      
      If booting the installation DVD, make sure vnc is passed as a boot parameter. To add the vnc parameter, you will need a console attached to the target system that allows you to interact with the boot process. Enter the following at the prompt:

      ```
      boot: linux vnc
      ```

   b. Boot over the network.
      
      If the target system is configured with a static IP address, add the vnc command to the kickstart file. If the target system is using DHCP, add `vnc vncconnect=HOST[:port]` to the boot arguments for the target system. HOST is the IP address or DNS host name of the VNC viewer system. Specifying the port is optional. Enter the following at the prompt:

      ```
      boot: linux vnc vncconnect=HOST[:port]
      ```

4. When prompted for the network configuration on the target system, assign it an available RFC 1918 address in the same network you used for the VNC viewer system. For example, 192.168.100.2/24.

   **Note**

   This IP address is only used during installation. You will have an opportunity to configure the final network settings, if any, later in the installer.
5. Once the installer indicates it is starting anaconda, you will be instructed to connect to the system using the VNC viewer. Connect to the viewer and follow the graphical installation mode instructions found in the product documentation.

### 14.3.2. Kickstart Considerations

If your target system will be booting over the network, VNC is still available. Just add the `vnc` command to the kickstart file for the system. You will be able to connect to the target system using your VNC viewer and monitor the installation progress. The address to use is the one the system is configured with via the kickstart file.

If you are using DHCP for the target system, the reverse `vnc vncconnect` method may work better for you. Rather than adding the `vnc` boot parameter to the kickstart file, add the `vnc vncconnect=HOST[:port]` parameter to the list of boot arguments for the target system. For HOST, put the IP address or DNS host name of the VNC viewer system. Specifying the port is optional. See the next section for more details on using the vncconnect mode.

### 14.3.3. Firewall Considerations

If you are performing the installation where the VNC viewer system is a workstation on a different subnet from the target system, you may run into network routing problems. VNC works fine so long as your viewer system has a route to the target system and ports 5900 and 5901 are open. If your environment has a firewall, make sure ports 5900 and 5901 are open between your workstation and the target system.

In addition to passing the `vnc` boot parameter, you may also want to pass the `vncpassword` parameter in these scenarios. While the password is sent in plain text over the network, it does provide an extra step before a viewer can connect to a system. Once the viewer connects to the target system over VNC, no other connections are permitted. These limitations are usually sufficient for installation purposes.

**Important**

Be sure to use a temporary password for the `vncpassword` option. It should not be a password you use on any systems, especially a real root password.

If you continue to have trouble, consider using the `vnc vncconnect` parameter. In this mode of operation, you start the viewer on your system first telling it to listen for an incoming connection. Pass `vnc vncconnect=HOST[:port]` at the boot prompt and the installer will attempt to connect to the specified HOST (either a hostname or IP address). Specifying the port is optional.

### 14.4. References

- Anaconda boot options: [http://fedoraproject.org/wiki/Anaconda/Options](http://fedoraproject.org/wiki/Anaconda/Options)
- Kickstart documentation: [http://fedoraproject.org/wiki/Anaconda/Kickstart](http://fedoraproject.org/wiki/Anaconda/Kickstart)
Chapter 15.

Kickstart Installations

15.1. What are Kickstart Installations?

Many system administrators would prefer to use an automated installation method to install Fedora on their machines. To answer this need, Red Hat created the kickstart installation method. Using kickstart, a system administrator can create a single file containing the answers to all the questions that would normally be asked during a typical installation.

Kickstart files can be kept on a single server system and read by individual computers during the installation. This installation method can support the use of a single kickstart file to install Fedora on multiple machines, making it ideal for network and system administrators.

Kickstart provides a way for users to automate a Fedora installation.

All kickstart scriptlets and the log files of their execution are stored in the /tmp directory to assist with debugging installation failures.

Note — /tmp/netinfo no longer used

Anaconda now configures network interfaces with NetworkManager. Consequently, kickstart users that referenced the network settings located in /tmp/netinfo in previous versions of Fedora must now source the ifcfg files in /etc/sysconfig/network-scripts.

15.2. How Do You Perform a Kickstart Installation?

Kickstart installations can be performed using a local DVD, a local hard drive, or via NFS, FTP, or HTTP.

To use kickstart, you must:

1. Create a kickstart file.
2. Create a boot media with the kickstart file or make the kickstart file available on the network.
3. Make the installation tree available.
4. Start the kickstart installation.

This chapter explains these steps in detail.

15.3. Creating the Kickstart File

The kickstart file is a simple text file, containing a list of items, each identified by a keyword. You can create it by using the Kickstart Configurator application, or writing it from scratch. The Fedora installation program also creates a sample kickstart file based on the options that you selected during installation. It is written to the file /root/anaconda-ks.cfg. You should be able to edit it with any text editor or word processor that can save files as ASCII text.

First, be aware of the following issues when you are creating your kickstart file:
Section must be specified in order. Items within the sections do not have to be in a specific order unless otherwise specified. The section order is:

- Command section — Refer to Section 15.4, “Kickstart Options” for a list of kickstart options. You must include the required options.

- The %packages section — Refer to Section 15.5, “Package Selection” for details.

- The %pre and %post sections — These two sections can be in any order and are not required. Refer to Section 15.6, “Pre-installation Script” and Section 15.7, “Post-installation Script” for details.

- Items that are not required can be omitted.

- Omitting any required item results in the installation program prompting the user for an answer to the related item, just as the user would be prompted during a typical installation. Once the answer is given, the installation continues unattended (unless it finds another missing item).

- Lines starting with a pound (also known as hash) sign (#) are treated as comments and are ignored.

- For kickstart upgrades, the following items are required:
  - Language
  - Installation method
  - Device specification (if device is needed to perform the installation)
  - Keyboard setup
  - The upgrade keyword
  - Boot loader configuration

If any other items are specified for an upgrade, those items are ignored (note that this includes package selection).

### 15.4. Kickstart Options

The following options can be placed in a kickstart file. If you prefer to use a graphical interface for creating your kickstart file, use the Kickstart Configurator application. Refer to Chapter 16, Kickstart Configurator for details.

#### Note

If the option is followed by an equals mark (=), a value must be specified after it. In the example commands, options in brackets ([ ]) are optional arguments for the command.

**autopart** (optional)

Automatically create partitions — 1 GB or more root (/) partition, a swap partition, and an appropriate boot partition for the architecture. One or more of the default partition sizes can be redefined with the part directive.
• **--encrypted** — Should all devices with support be encrypted by default? This is equivalent to checking the Encrypt checkbox on the initial partitioning screen.

• **--passphrase=** — Provide a default system-wide passphrase for all encrypted devices.

• **--escrowcert=URL_of_X.509_certificate** — Store data encryption keys of all encrypted volumes as files in `/root`, encrypted using the X.509 certificate from the URL specified with `URL_of_X.509_certificate`. The keys are stored as a separate file for each encrypted volume. This option is only meaningful if **--encrypted** is specified.

• **--backuppassphrase=** — Add a randomly-generated passphrase to each encrypted volume. Store these passphrases in separate files in `/root`, encrypted using the X.509 certificate specified with **--escrowcert**. This option is only meaningful if **--escrowcert** is specified.

### Ignoredisk (optional)

Causes the installer to ignore the specified disks. This is useful if you use autopartition and want to be sure that some disks are ignored. For example, without **ignoredisk**, attempting to deploy on a SAN-cluster the kickstart would fail, as the installer detects passive paths to the SAN that return no partition table.

The syntax is:

```
ignoredisk --drives=drive1,drive2,...
```

where `driveN` is one of `sda`, `sdb`, `hda`, etc.

To ignore a multipath device that does not use logical volume management (LVM), use the format `disk/by-id/dm-uuid-mpath-WWID`, where `WWID` is the world-wide identifier for the device. For example, to ignore a disk with WWID `2416CD96995134CA5D787F08A5AA11017`, use:

```
ignoredisk --drives=disk/by-id/dm-uuid-mpath-2416CD96995134CA5D787F08A5AA11017
```

Multipath devices that use LVM are not assembled until after *anaconda* has parsed the kickstart file. Therefore, you cannot specify these devices in the format `dm-uuid-mpath`. Instead, to ignore a multipath device that uses LVM, use the format `disk/by-id/scsi-WWID`, where `WWID` is the world-wide identifier for the device. For example, to ignore a disk with WWID `580958EC5510947BE8C0360F604351918`, use:

```
ignoredisk --drives=disk/by-id/scsi-580958EC5510947BE8C0360F604351918
```

**Warning — Never specify multipath devices by device names like mpatha**

Device names like `mpatha` are not specific to a particular disk. The disk named `/dev/mpatha` during installation might not be the one that you expect it to be. Therefore, the **ignoredisk** command could target the wrong disk.

• **--only-use** — specifies a list of disks for the installer to use. All other disks are ignored. For example, to use disk `sda` during installation and ignore all other disks:

```
ignoredisk --only-use=sda
```
Chapter 15. Kickstart Installations

To include a multipath device that does not use LVM:

```
ignoredisk --only-use=disk/by-id/dm-uuid-mpath-2416CD96995134CA5D787F00A5AA11017
```

To include a multipath device that uses LVM:

```
ignoredisk --only-use=disk/by-id/scsi-58095BEC5510947BE8C0360F604351918
```

**autostep (optional)**

Similar to `interactive` except it goes to the next screen for you. It is used mostly for debugging.

- **--autoscreenshot** — Take a screenshot at every step during installation and copy the images over to `/root/anaconda-screenshots` after installation is complete. This is most useful for documentation.

**auth or authconfig (required)**

Sets up the authentication options for the system. It is similar to the `authconfig` command, which can be run after the install. By default, passwords are normally encrypted and are not shadowed.

- **--enablenis** — Turns on NIS support. By default, `--enablenis` uses whatever domain it finds on the network. A domain should almost always be set by hand with the `--nisdomain=` option.

- **--nisdomain=** — NIS domain name to use for NIS services.

- **--nisserver=** — Server to use for NIS services (broadcasts by default).

- **--useshadow** or **--enableshadow** — Use shadow passwords.

- **--enableldap** — Turns on LDAP support in `/etc/nsswitch.conf`, allowing your system to retrieve information about users (for example, their UIDs, home directories, and shells) from an LDAP directory. To use this option, you must install the `nss-pam-ldapd` package. You must also specify a server and a base DN (distinguished name) with `--ldapserver=` and `--ldapbasedn=`.

- **--enableldapauth** — Use LDAP as an authentication method. This enables the `pam_ldap` module for authentication and changing passwords, using an LDAP directory. To use this option, you must have the `nss-pam-ldapd` package installed. You must also specify a server and a base DN with `--ldapserver=` and `--ldapbasedn=`. If your environment does not use TLS (Transport Layer Security), use the `--disableldaptls` switch to ensure that the resulting configuration file works.

- **--ldapserver=** — If you specified either `--enableldap` or `--enableldapauth`, use this option to specify the name of the LDAP server to use. This option is set in the `/etc/ldap.conf` file.

- **--ldapbasedn=** — If you specified either `--enableldap` or `--enableldapauth`, use this option to specify the DN in your LDAP directory tree under which user information is stored. This option is set in the `/etc/ldap.conf` file.

- **--enableldaptls** — Use TLS (Transport Layer Security) lookups. This option allows LDAP to send encrypted usernames and passwords to an LDAP server before authentication.
• **--disableldaptls** — Do not use TLS (Transport Layer Security) lookups in an environment that uses LDAP for authentication.

• **--enablekrb5** — Use Kerberos 5 for authenticating users. Kerberos itself does not know about home directories, UIDs, or shells. If you enable Kerberos, you must make users' accounts known to this workstation by enabling LDAP, NIS, or Hesiod or by using the `/usr/sbin/useradd` command. If you use this option, you must have the `pam_krb5` package installed.

• **--krb5realm=** — The Kerberos 5 realm to which your workstation belongs.

• **--krb5kdc=** — The KDC (or KDCs) that serve requests for the realm. If you have multiple KDCs in your realm, separate their names with commas (,).

• **--krb5adminserver=** — The KDC in your realm that is also running kadmind. This server handles password changing and other administrative requests. This server must be run on the master KDC if you have more than one KDC.

• **--enablehesiod** — Enable Hesiod support for looking up user home directories, UIDs, and shells. More information on setting up and using Hesiod on your network is in `/usr/share/doc/glibc-2.x.x/README.hesiod`, which is included in the `glibc` package. Hesiod is an extension of DNS that uses DNS records to store information about users, groups, and various other items.

• **--hesiodlhs** and **--hesiodrhs** — The Hesiod LHS (left-hand side) and RHS (right-hand side) values, set in `/etc/nesiod.conf`. The Hesiod library uses these values to search DNS for a name, similar to the way that LDAP uses a base DN.

To look up user information for the username jim, the Hesiod library looks up `jim.passwd<LHS><RHS>`, which should resolve to a TXT record that contains a string identical to an entry for that user in the `passwd` file: `jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`. To look up groups, the Hesiod library looks up `jim.group<LHS><RHS>` instead.

To look up users and groups by number, make `501.uid` a CNAME for `jim.passwd`, and `501.gid` a CNAME for `jim.group`. Note that the library does not place a period (.) in front of the LHS and RHS values when performing a search. Therefore, if the LHS and RHS values need to have a period placed in front of them, you must include the period in the values you set for **--hesiodlhs** and **--hesiodrhs**.

• **--enablesmbauth** — Enables authentication of users against an SMB server (typically a Samba or Windows server). SMB authentication support does not know about home directories, UIDs, or shells. If you enable SMB, you must make users' accounts known to the workstation by enabling LDAP, NIS, or Hesiod or by using the `/usr/sbin/useradd` command.

• **--smbservers=** — The name of the servers to use for SMB authentication. To specify more than one server, separate the names with commas (,).

• **--smbworkgroup=** — The name of the workgroup for the SMB servers.

• **--enablecache** — Enables the `nscd` service. The `nscd` service caches information about users, groups, and various other types of information. Caching is especially helpful if you choose to distribute information about users and groups over your network using NIS, LDAP, or Hesiod.

• **--passalgo** — To set up the SHA-256 hashing algorithm, run the command `authconfig --passalgo=sha256 --kickstart`. 

---

To look up user information for the username jim, the Hesiod library looks up `jim.passwd<LHS><RHS>`, which should resolve to a TXT record that contains a string identical to an entry for that user in the `passwd` file: `jim:*:501:501:Jungle Jim:/home/jim:/bin/bash`. To look up groups, the Hesiod library looks up `jim.group<LHS><RHS>` instead.

To look up users and groups by number, make `501.uid` a CNAME for `jim.passwd`, and `501.gid` a CNAME for `jim.group`. Note that the library does not place a period (.) in front of the LHS and RHS values when performing a search. Therefore, if the LHS and RHS values need to have a period placed in front of them, you must include the period in the values you set for **--hesiodlhs** and **--hesiodrhs**.

• **--enablesmbauth** — Enables authentication of users against an SMB server (typically a Samba or Windows server). SMB authentication support does not know about home directories, UIDs, or shells. If you enable SMB, you must make users' accounts known to the workstation by enabling LDAP, NIS, or Hesiod or by using the `/usr/sbin/useradd` command.

• **--smbservers=** — The name of the servers to use for SMB authentication. To specify more than one server, separate the names with commas (,).

• **--smbworkgroup=** — The name of the workgroup for the SMB servers.

• **--enablecache** — Enables the `nscd` service. The `nscd` service caches information about users, groups, and various other types of information. Caching is especially helpful if you choose to distribute information about users and groups over your network using NIS, LDAP, or Hesiod.

• **--passalgo** — To set up the SHA-256 hashing algorithm, run the command `authconfig --passalgo=sha256 --kickstart`. 

---
To set up the SHA-512 hashing algorithm, run `authconfig --passalgo=sha512 --kickstart`.

Remove the `--enablemd5` option if it is present.

**bootloader (required)**

Specifies how the boot loader should be installed. This option is required for both installations and upgrades.

**Important**

If you select text mode for a kickstart installation, make sure that you specify choices for the partitioning, bootloader, and package selection options. These steps are automated in text mode, and *anaconda* cannot prompt you for missing information. If you do not provide choices for these options, *anaconda* will stop the installation process.

- **--append=** — Specifies kernel parameters. To specify multiple parameters, separate them with spaces. For example:

  ```
  bootloader --location=mbr --append="hdd=ide-scsi ide=nodma"
  ```

- **--driveorder** — Specify which drive is first in the BIOS boot order. For example:

  ```
  bootloader --driveorder=sda,hda
  ```

- **--location=** — Specifies where the boot record is written. Valid values are the following: `mbr` (the default), `partition` (installs the boot loader on the first sector of the partition containing the kernel), or `none` (do not install the boot loader).

- **--password=** — If using GRUB, sets the GRUB boot loader password to the one specified with this option. This should be used to restrict access to the GRUB shell, where arbitrary kernel options can be passed.

- **--md5pass=** — If using GRUB, similar to `--password=` except the password should already be encrypted.

- **--timeout=** — Specify the number of seconds before the bootloader times out and boots the default option. Specifying 0 will tell GRUB not to display these menus.

- **--upgrade** — Upgrade the existing boot loader configuration, preserving the old entries. This option is only available for upgrades.

**clearpart (optional)**

Removes partitions from the system, prior to creation of new partitions. By default, no partitions are removed.
Kickstart Options

Note

If the `clearpart` command is used, then the `--onpart` command cannot be used on a logical partition.

- **--all** — Erases all partitions from the system.
- **--drives** — Specifies which drives to clear partitions from. For example, the following clears all the partitions on the first two drives on the primary IDE controller:

  ```
  clearpart --drives=hda,hdb --all
  ```

To clear a multipath device that does not use `logical volume management` (LVM), use the format `disk/by-id/dm-uuid-mpath-WWID`, where `WWID` is the `world-wide identifier` for the device. For example, to clear a disk with WWID `2416CD96995134CA5D787F00A5AA11017`, use:

```
clearpart --drives=disk/by-id/dm-uuid-mpath-2416CD96995134CA5D787F00A5AA11017
```

Multipath devices that use LVM are not assembled until after `anaconda` has parsed the kickstart file. Therefore, you cannot specify these devices in the format `dm-uuid-mpath`. Instead, to clear a multipath device that uses LVM, use the format `disk/by-id/scsi-WWID`, where `WWID` is the `world-wide identifier` for the device. For example, to clear a disk with WWID `58095BEC5510947BE8C0360F604351918`, use:

```
clearpart --drives=disk/by-id/scsi-58095BEC5510947BE8C0360F604351918
```

Warning — Never specify multipath devices by device names like `mpatha`

Device names like `mpatha` are not specific to a particular disk. The disk named `/dev/mpatha` during installation might not be the one that you expect it to be. Therefore, the `clearpart` command could target the wrong disk.

- **--initlabel** — Initializes the disk label to the default for your architecture (for example `msdos` for x86). It is useful so that the installation program does not ask if it should initialize the disk label if installing to a brand new hard drive.
- **--linux** — Erases all Linux partitions.
- **--none** (default) — Do not remove any partitions.

`cmdline` (optional)

Perform the installation in a completely non-interactive command line mode. Any prompts for interaction halts the install.
Chapter 15. Kickstart Installations

device (optional)
On most PCI systems, the installation program autoprobes for Ethernet and SCSI cards properly. On older systems and some PCI systems, however, kickstart needs a hint to find the proper devices. The \texttt{device} command, which tells the installation program to install extra modules, is in this format:

\begin{verbatim}
device <moduleName> --opts=<options>
\end{verbatim}

- \texttt{<moduleName>} — Replace with the name of the kernel module which should be installed.
- \texttt{--opts=} — Mount options to use for mounting the NFS export. Any options that can be specified in /\texttt{etc/fstab} for an NFS mount are allowed. The options are listed in the \texttt{nfs(5)} man page. Multiple options are separated with a comma.

driverdisk (optional)
Driver diskettes can be used during kickstart installations. You must copy the driver diskettes’s contents to the root directory of a partition on the system’s hard drive. Then you must use the \texttt{driverdisk} command to tell the installation program where to look for the driver disk.

\begin{verbatim}
driverdisk <partition> --source=<url> --biospart=<biospart> [--type=<fstype>]
\end{verbatim}

Alternatively, a network location can be specified for the driver diskette:

\begin{verbatim}
driverdisk --source=ftp://path/to/dd.img
driverdisk --source=http://path/to/dd.img
driverdisk --source=nfs:host:/path/to/img
\end{verbatim}

- \texttt{<partition>} — Partition containing the driver disk.
- \texttt{<url>} — URL for the driver disk. NFS locations can be given in the form \texttt{nfs:host:/path/to/img}.
- \texttt{<biospart>} — BIOS partition containing the driver disk (for example, \texttt{82p2}).
- \texttt{--type=} — File system type (for example, vfat or ext2).

firewall (optional)
This option corresponds to the \textbf{Firewall Configuration} screen in the installation program:

\begin{verbatim}
firewall --enabled|--disabled [--trust=] <device> [--port=]
\end{verbatim}

- \texttt{--enabled} or \texttt{--enable} — Reject incoming connections that are not in response to outbound requests, such as DNS replies or DHCP requests. If access to services running on this machine is needed, you can choose to allow specific services through the firewall.
- \texttt{--disabled} or \texttt{--disable} — Do not configure any iptables rules.
- \texttt{--trust=} — Listing a device here, such as \texttt{eth0}, allows all traffic coming from that device to go through the firewall. To list more than one device, use \texttt{--trust eth0 --trust eth1}. Do NOT use a comma-separated format such as \texttt{--trust eth0, eth1}.
- \texttt{<incoming>} — Replace with one or more of the following to allow the specified services through the firewall.
  - \texttt{--ssh}
• **--smtp**
• **--http**
• **--ftp**

• **--port=** — You can specify that ports be allowed through the firewall using the port:protocol format. For example, to allow IMAP access through your firewall, specify `imap:tcp`. Numeric ports can also be specified explicitly; for example, to allow UDP packets on port 1234 through, specify `1234:udp`. To specify multiple ports, separate them by commas.

**firstboot (optional)**

Determine whether the firstboot starts the first time the system is booted. If enabled, the firstboot package must be installed. If not specified, this option is disabled by default.

• **--enable** or **--enabled** — The Setup Agent is started the first time the system boots.

• **--disable** or **--disabled** — The Setup Agent is not started the first time the system boots.

• **--reconfig** — Enable the Setup Agent to start at boot time in reconfiguration mode. This mode enables the language, mouse, keyboard, root password, security level, time zone, and networking configuration options in addition to the default ones.

**graphical (optional)**

Perform the kickstart installation in graphical mode. This is the default.

**halt (optional)**

Halt the system after the installation has successfully completed. This is similar to a manual installation, where anaconda displays a message and waits for the user to press a key before rebooting. During a kickstart installation, if no completion method is specified, this option is used as the default.

The **halt** option is equivalent to the **shutdown -h** command.

For other completion methods, refer to the **poweroff, reboot, and shutdown** kickstart options.

**install (optional)**

 Tells the system to install a fresh system rather than upgrade an existing system. This is the default mode. For installation, you must specify the type of installation from **cdrom, harddrive, nfs, or url** (for FTP or HTTP installations). The install command and the installation method command must be on separate lines.

• **cdrom** — Install from the first optical drive on the system.

• **harddrive** — Install from a Fedora installation tree on a local drive, which must be either vfat or ext2.

• **--biospart=**

  BIOS partition to install from (such as 82).

• **--partition=**

  Partition to install from (such as sdb2).

• **--dir=**
Chapter 15. Kickstart Installations

Directory containing the **variant** directory of the installation tree.

For example:

```
harddrive --partition=hdb2 --dir=/tmp/install-tree
```

- **nfs** — Install from the NFS server specified.
  - **--server=**
    Server from which to install (hostname or IP).
  - **--dir=**
    Directory containing the **variant** directory of the installation tree.
  - **--opts=**
    Mount options to use for mounting the NFS export. (optional)

For example:

```
nfs --server=nfsserver.example.com --dir=/tmp/install-tree
```

- **url** — Install from an installation tree on a remote server via FTP or HTTP.

For example:

```
url --url http://<server>/<dir>
```

or:

```
url --url ftp://<username>:<password>@<server>/<dir>
```

**iscsi** (optional)

iscsi --ipaddr= [options].

Specifies additional iSCSI storage to be attached during installation. If you use the **iscsi** parameter, you must also assign a name to the iSCSI node, using the **iscsiname** parameter earlier in the kickstart file.

We recommend that wherever possible you configure iSCSI storage in the system BIOS or firmware (iBFT for Intel systems) rather than use the **iscsi** parameter. **Anaconda** automatically detects and uses disks configured in BIOS or firmware and no special configuration is necessary in the kickstart file.

If you must use the **iscsi** parameter, ensure that networking is activated at the beginning of the installation, and that the **iscsi** parameter appears in the kickstart file before you refer to iSCSI disks with parameters such as **clearpart** or **ignoredisk**.

- **--port=** (mandatory) — the port number (typically, **--port=3260**)
- **--user=** — the username required to authenticate with the target
- **--password=** — the password that corresponds with the username specified for the target
• **--reverse-user=** — the username required to authenticate with the initiator from a target that uses reverse CHAP authentication

• **--reverse-password=** — the password that corresponds with the username specified for the initiator

**iscsiname** (optional)

Assigns a name to an iSCSI node specified by the iscsi parameter. If you use the *iscsi* parameter in your kickstart file, you must specify *iscsiname* earlier in the kickstart file.

**keyboard** (required)

Sets the default keyboard type for the system. The available keyboard types are:

• **be-latin1** — Belgian

• **bg_bds-utf8** — Bulgarian

• **bg_pho-utf8** — Bulgarian (Phonetic)

• **br-abnt2** — Brazilian (ABNT2)

• **cf** — French Canadian

• **croat** — Croatian

• **cz-us-qwertz** — Czech

• **cz-lat2** — Czech (qwerty)

• **de** — German

• **de-latin1** — German (latin1)

• **de-latin1-nodeadkeys** — German (latin1 without dead keys)

• **dvorak** — Dvorak

• **dk** — Danish

• **dk-latin1** — Danish (latin1)

• **es** — Spanish

• **et** — Estonian

• **fi** — Finnish

• **fi-latin1** — Finnish (latin1)

• **fr** — French

• **fr-latin9** — French (latin9)

• **fr-latin1** — French (latin1)

• **fr-pc** — French (pc)
• fr_CH — Swiss French
• fr_CH-latin1 — Swiss French (latin1)
• gr — Greek
• hu — Hungarian
• hu101 — Hungarian (101 key)
• is-latin1 — Icelandic
• it — Italian
• it-ibm — Italian (IBM)
• it2 — Italian (it2)
• jp106 — Japanese
• ko — Korean
• la-latin1 — Latin American
• mk-utf — Macedonian
• nl — Dutch
• no — Norwegian
• pl2 — Polish
• pt-latin1 — Portuguese
• ro — Romanian
• ru — Russian
• sr-cy — Serbian
• sr-latin — Serbian (latin)
• sv-latin1 — Swedish
• sg — Swiss German
• sg-latin1 — Swiss German (latin1)
• sk-qwerty — Slovak (qwerty)
• slovene — Slovenian
• trq — Turkish
• uk — United Kingdom
• ua-utf — Ukrainian
• us-acentos — U.S. International
• **us** — U.S. English

The file `/usr/lib/python2.6/site-packages/system_config_keyboard/keyboard_models.py` on 32-bit systems or `/usr/lib64/python2.6/site-packages/system_config_keyboard/keyboard_models.py` on 64-bit systems also contains this list and is part of the `system-config-keyboard` package.

**lang** *(required)*

Sets the language to use during installation and the default language to use on the installed system. For example, to set the language to English, the kickstart file should contain the following line:

```
lang en_US
```

The file `/usr/share/system-config-language/locale-list` provides a list of the valid language codes in the first column of each line and is part of the `system-config-language` package.

Certain languages (for example, Chinese, Japanese, Korean, and Indic languages) are not supported during text-mode installation. If you specify one of these languages with the `lang` command, the installation process continues in English, but the installed system uses your selection as its default language.

**langsupport** *(deprecated)*

The `langsupport` keyword is deprecated and its use will cause an error message to be printed to the screen and installation to halt. Instead of using the `langsupport` keyword, you should now list the support package groups for all languages you want supported in the `%packages` section of your kickstart file. For instance, adding support for French means you should add the following to `%packages`:

```
@french-support
```

**logvol** *(optional)*

Create a logical volume for Logical Volume Management (LVM) with the syntax:

```
logvol <mntpoint> --vgname=<name> --size=<size> --name=<name> <options>
```

The options are as follows:

- **--noformat** — Use an existing logical volume and do not format it.
- **--useexisting** — Use an existing logical volume and reformat it.
- **--fstype** — Sets the file system type for the logical volume. Valid values are `xfs`, `ext2`, `ext3`, `ext4`, `swap`, `vfat`, and `hfs`.
- **--fsoptions** — Specifies a free form string of options to be used when mounting the filesystem. This string will be copied into the `/etc/fstab` file of the installed system and should be enclosed in quotes.
- **--grow** — Tells the logical volume to grow to fill available space (if any), or up to the maximum size setting.
- **--maxsize** — The maximum size in megabytes when the logical volume is set to grow. Specify an integer value here such as **500** (do not include the unit).
Chapter 15. Kickstart Installations

- **--recommended** — Determine the size of the logical volume automatically.

- **--percent** — Specify the amount by which to grow the logical volume, as a percentage of the free space in the volume group after any statically-sized logical volumes are taken into account. This option must be used in conjunction with the **--size** and **--grow** options for `logvol`.

- **--encrypted** — Specifies that this logical volume should be encrypted, using the passphrase provided in the **--passphrase** option. If you do not specify a passphrase, *anaconda* uses the default, system-wide passphrase set with the `autopart --passphrase` command, or stops the installation and prompts you to provide a passphrase if no default is set.

- **--passphrase** — Specifies the passphrase to use when encrypting this logical volume. You must use this option together with the **--encrypted** option; by itself it has no effect.

- **--escrowcert=URL_of_X.509_certificate** — Store data encryption keys of all encrypted volumes as files in `/root`, encrypted using the X.509 certificate from the URL specified with `URL_of_X.509_certificate`. The keys are stored as a separate file for each encrypted volume. This option is only meaningful if **--encrypted** is specified.

- **--backuppassphrase** — Add a randomly-generated passphrase to each encrypted volume. Store these passphrases in separate files in `/root`, encrypted using the X.509 certificate specified with **--escrowcert**. This option is only meaningful if **--escrowcert** is specified.

- **--label** — assign a label to an individual volume.

Create the partition first, create the logical volume group, and then create the logical volume. For example:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

Create the partition first, create the logical volume group, and then create the logical volume to occupy 90% of the remaining space in the volume group. For example:

```
part pv.01 --size 1 --grow
volgroup myvg pv.01
logvol / --vgname=myvg --size=1 --name=rootvol --grow --percent=90
```

**logging** (optional)

This command controls the error logging of *anaconda* during installation. It has no effect on the installed system.

- **--host** — Send logging information to the given remote host, which must be running a syslogd process configured to accept remote logging.

- **--port** — If the remote syslogd process uses a port other than the default, it may be specified with this option.

- **--level** — One of debug, info, warning, error, or critical.

Specify the minimum level of messages that appear on tty3. All messages will still be sent to the log file regardless of this level, however.
**mediacheck** (optional)
If given, this will force anaconda to run mediacheck on the installation media. This command requires that installs be attended, so it is disabled by default.

**monitor** (optional)
If the monitor command is not given, anaconda will use X to automatically detect your monitor settings. Please try this before manually configuring your monitor.

- **--hsync**= — Specifies the horizontal sync frequency of the monitor.
- **--monitor**= — Use specified monitor; monitor name should be from the list of monitors in /usr/share/hwdata/MonitorsDB from the hwdata package. The list of monitors can also be found on the X Configuration screen of the Kickstart Configurator. This is ignored if --hsync or --vsync is provided. If no monitor information is provided, the installation program tries to probe for it automatically.
- **--noprobe**= — Do not try to probe the monitor.
- **--vsync**= — Specifies the vertical sync frequency of the monitor.

**mouse** (deprecated)
The mouse keyword is deprecated.

**network** (optional)
Configures network information for the target system and activates network devices in the installer environment. The device specified in the first **network** command is activated automatically if network access is required during installation, for example, during a network installation or installation over VNC. You can also explicitly require device to activate in the installer environment with the **--activate** option.

---

**How to manually input network settings**

If you need to manually specify network settings during an otherwise-automated kickstart installation, do not use **network**. Instead, boot the system with the **asknetwork** option (refer to Section 15.10, “Starting a Kickstart Installation”), which will prompt **anaconda** to ask you for network settings rather than use the default settings. **anaconda** will ask this before fetching the kickstart file.

Once the network connection is established, you can only reconfigure network settings with those specified in your kickstart file.
Note

You will only be prompted for information about your network:

- before fetching the kickstart file if you are using the `asknetwork` boot option
- when the network is first accessed once the kickstart file has been fetched, if the network was not used to fetch it and you have provided no kickstart network commands

- **--activate** — activate this device in the installer environment.

  If you use the `--activate` option on a device that has already been activated (for example, an interface you configured with boot options so that the system could retrieve the kickstart file) the device is reactivated to use the details specified in the kickstart file.

  Use the `--nodefroute` option to prevent the device from using the default route.

  The `activate` option is new in Fedora 16.

- **--biosdevname=0** — disables consistent network device naming (refer to Appendix A in the Fedora System Administrators Guide).

- **--bootproto=** — One of `dhcp`, `bootp`, `ibft`, or `static`.

  The `ibft` option is new in Fedora 16.

  The `bootproto` option defaults to `dhcp`. `bootp` and `dhcp` are treated the same.

  The DHCP method uses a DHCP server system to obtain its networking configuration. As you might guess, the BOOTP method is similar, requiring a BOOTP server to supply the networking configuration. To direct a system to use DHCP:

  ```
  network --bootproto=dhcp
  ```

  To direct a machine to use BOOTP to obtain its networking configuration, use the following line in the kickstart file:

  ```
  network --bootproto=bootp
  ```

  To direct a machine to use the configuration specified in iBFT, use:

  ```
  network --bootproto=ibft
  ```

  The static method requires that you specify the IP address, netmask, gateway, and nameserver in the kickstart file. As the name implies, this information is static and is used during and after the installation.

  All static networking configuration information must be specified on one line; you cannot wrap lines using a backslash as you can on a command line. A line that specifies static networking in a kickstart file is therefore more complex than lines that specify DHCP, BOOTP, or iBFT. Note
that the examples on this page have line breaks in them for presentation reasons; they would not work in an actual kickstart file.

```bash
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0
--gateway=10.0.2.254 --nameserver=10.0.2.1
```

You can also configure multiple nameservers here. To do so, specify them as a comma-delimited list in the command line.

```bash
network --bootproto=static --ip=10.0.2.15 --netmask=255.255.255.0
--gateway=10.0.2.254 --nameserver 192.168.2.1,192.168.3.1
```

- `-device=` — specifies the device to be configured (and eventually activated) with the `network` command. For the first `network` command, `-device=` defaults (in order of preference) to one of:
  1. the device specified by the `ksdevice` boot option
  2. the device activated automatically to fetch the kickstart file
  3. the device selected in the `Networking Devices` dialog

The behavior of any subsequent `network` command is unspecified if its `-device` option is missing. Take care to specify a `-device` option for any network command beyond the first.

You can specify a device in one of five ways:

- the device name of the interface, for example, `eth0`
- the MAC address of the interface, for example, `00:12:34:56:78:9a`
- the keyword `link`, which specifies the first interface with its link in the `up` state
- the keyword `bootif`, which uses the MAC address that `pxelinux` set in the `BOOTIF` variable. Set `IPAPPEND 2` in your `pxelinux.cfg` file to have `pxelinux` set the `BOOTIF` variable.
- the keyword `ibft`, which uses the MAC address of the interface specified by iBFT

```bash
network --bootproto=dhcp --device=eth0
```

- `-ip=` — IP address of the device.
- `-ipv6=` — IPv6 address of the device, or `auto` to use automatic neighbor discovery, or `dhcp` to use DHCPv6.
- `-gateway=` — Default gateway as a single IPv4 or IPv6 address.
- `-nameserver=` — Primary nameserver, as an IP address. Multiple nameservers must each be separated by a comma.
- `-nodefroute` — Prevents the interface being set as the default route. Use this option when you activate additional devices with the `-activate=` option, for example, a NIC on a separate subnet for an iSCSI target.

The `nodefroute` option is new in Fedora 16.

- `-nodns` — Do not configure any DNS server.
Chapter 15. Kickstart Installations

- `--netmask=` — Network mask of the device.
- `--hostname=` — Hostname for the installed system.
- `--ethtool=` — Specifies additional low-level settings for the network device which will be passed to the ethtool program.
- `--onboot=` — Whether or not to enable the device at boot time.
- `--dhcpclass=` — The DHCP class.
- `--mtu=` — The MTU of the device.
- `--noipv4` — Disable IPv4 on this device.
- `--noipv6` — Disable IPv6 on this device.

`part` or `partition` (required for installs, ignored for upgrades)

Creates a partition on the system.

If more than one Fedora installation exists on the system on different partitions, the installation program prompts the user and asks which installation to upgrade.

**Warning**

As of Fedora 16, you need a biosboot partition in order to successfully install the bootloader on a disk that contains a GPT/GUID partition table. This includes disks initialized by the installer. This partition can be created with the kickstart option `part biosboot --fstype=biosboot --size=1`.

However, if the disk already has a biosboot partition, adding a "part biosboot" option is unnecessary.

**Warning**

All partitions created are formatted as part of the installation process unless `--noformat` and `--onpart` are used.

**Important**

If you select text mode for a kickstart installation, make sure that you specify choices for the partitioning, bootloader, and package selection options. These steps are automated in text mode, and `anaconda` cannot prompt you for missing information. If you do not provide choices for these options, `anaconda` will stop the installation process.
For a detailed example of part in action, refer to Section 15.4.1, "Advanced Partitioning Example".

- `<mntpoint multipath --name= --device= --rule=>` — The `<mntpoint>` is where the partition is mounted and must be of one of the following forms:

  - `<path>`
    For example, `/`, `/usr`, `/home`

  - `swap`
    The partition is used as swap space.
    To determine the size of the swap partition automatically, use the `--recommended` option:
    ```bash
    swap --recommended
    ```
    The size assigned will be effective but not precisely calibrated for your system.
    If you wish to set the swap partition more precisely, refer to Section 9.14.5, "Recommended Partitioning Scheme".

  - `raid.<id>`
    The partition is used for software RAID (refer to `raid`).

  - `pv.<id>`
    The partition is used for LVM (refer to `logvol`).

  - `--size=` — The minimum partition size in megabytes. Specify an integer value here such as 500 (do not include the unit).

    **Important --size value must be high**
    If the `--size` value is too small, the installation will fail. Set the `--size` value as the minimum amount of space you require. For size recommendations, refer to Section 9.14.5, "Recommended Partitioning Scheme".

  - `--grow` — Tells the partition to grow to fill available space (if any), or up to the maximum size setting.
**Note**

If you use `--grow` without setting `--maxsize` on a swap partition, *Anaconda* will limit the maximum size of the swap partition. For systems that have less than 2GB of physical memory, the imposed limit is twice the amount of physical memory. For systems with more than 2GB, the imposed limit is the size of physical memory plus 2GB.

- **--maxsize** — The maximum partition size in megabytes when the partition is set to grow. Specify an integer value here such as **500** (do not include the unit).

- **--noformat** — Specifies that the partition should not be formatted, for use with the **--onpart** command.

- **--onpart** or **--usepart** — Specifies the device on which to place the partition. For example:

  ```
  partition /home --onpart=hda1
  ```

  puts `/home` on `/dev/hda1`.

  The device must already exist on the system; the **--onpart** option will not create it.

- **--ondisk** or **--ondrive** — Forces the partition to be created on a particular disk. For example, **--ondisk=sdb** puts the partition on the second SCSI disk on the system.

  To specify a multipath device that does not use *logical volume management* (LVM), use the format `disk/by-id/dm-uuid-mpath-WWID`, where `WWID` is the world-wide identifier for the device. For example, to specify a disk with WWID `2416CD96995134CA5D787F00A5AA11017`, use:

  ```
  part / --fstype=ext3 --grow --asprimary --size=100 --ondisk=disk/by-id/dm-uuid-mpath-2416CD96995134CA5D787F00A5AA11017
  ```

  Multipath devices that use LVM are not assembled until after *anaconda* has parsed the kickstart file. Therefore, you cannot specify these devices in the format `dm-uuid-mpath`. Instead, to specify a multipath device that uses LVM, use the format `disk/by-id/scsi-WWID`, where `WWID` is the world-wide identifier for the device. For example, to specify a disk with WWID `58095BEC5510947BE8C0360F604351918`, use:

  ```
  part / --fstype=ext3 --grow --asprimary --size=100 --ondisk=disk/by-id/scsi-58095BEC5510947BE8C0360F604351918
  ```
Warning — Never specify multipath devices by device names like mpatha

Device names like mpatha are not specific to a particular disk. The disk named /dev/mpatha during installation might not be the one that you expect it to be. Therefore, the part command could target the wrong disk or partition.

- --asprimary — Forces automatic allocation of the partition as a primary partition, or the partitioning fails.

- --type= (replaced by fstype) — This option is no longer available. Use fstype.

- --fsoptions — Specifies a free form string of options to be used when mounting the filesystem. This string will be copied into the /etc/fstab file of the installed system and should be enclosed in quotes.

- --fsprofile — Specifies a usage type to be passed to the program that makes a filesystem on this partition. A usage type defines a variety of tuning parameters to be used when making a filesystem. For this option to work, the filesystem must support the concept of usage types and there must be a configuration file that lists valid types. For ext2, ext3, and ext4, this configuration file is /etc/mke2fs.conf.

- --fstype= — Sets the file system type for the partition. Valid values are xfs, ext2, ext3, ext4, swap, vfat, and hfs.

- --recommended — Determine the size of the partition automatically.

- --onbiosdisk — Forces the partition to be created on a particular disk as discovered by the BIOS.

- --encrypted — Specifies that this partition should be encrypted, using the passphrase provided in the --passphrase option. If you do not specify a passphrase, anaconda uses the default, system-wide passphrase set with the autopart --passphrase command, or stops the installation and prompts you to provide a passphrase if no default is set.

- --passphrase= — Specifies the passphrase to use when encrypting this partition. You must use this option together with the --encrypted option; by itself it has no effect.

- --escrowcert=URL_of_X.509_certificate — Store data encryption keys of all encrypted partitions as files in /root, encrypted using the X.509 certificate from the URL specified with URL_of_X.509_certificate. The keys are stored as a separate file for each encrypted partition. This option is only meaningful if --encrypted is specified.

- --backuppassphrase= — Add a randomly-generated passphrase to each encrypted partition. Store these passphrases in separate files in /root, encrypted using the X.509 certificate specified with --escrowcert. This option is only meaningful if --escrowcert is specified.

- --label= — assign a label to an individual partition.
Chapter 15. Kickstart Installations

**Note**

If partitioning fails for any reason, diagnostic messages appear on virtual console 3.

**poweroff** (optional)

Shut down and power off the system after the installation has successfully completed. Normally during a manual installation, anaconda displays a message and waits for the user to press a key before rebooting. During a kickstart installation, if no completion method is specified, the **halt** option is used as default.

The **poweroff** option is equivalent to the **shutdown** -p command.

**Note**

The **poweroff** option is highly dependent on the system hardware in use. Specifically, certain hardware components such as the BIOS, APM (advanced power management), and ACPI (advanced configuration and power interface) must be able to interact with the system kernel. Contact your manufacturer for more information on your system's APM/ACPI abilities.

For other completion methods, refer to the **halt**, **reboot**, and **shutdown** kickstart options.

**raid** (optional)

Assembles a software RAID device. This command is of the form:

```
raid <mntpoint> --level=<level> --device=<mddevice> <partitions*>  
```

- **<mntpoint>** — Location where the RAID file system is mounted. If it is /, the RAID level must be 1 unless a boot partition (/boot) is present. If a boot partition is present, the /boot partition must be level 1 and the root (/) partition can be any of the available types. The `<partitions*>` (which denotes that multiple partitions can be listed) lists the RAID identifiers to add to the RAID array.

- **--level** — RAID level to use (0, 1, or 5).

- **--device** — Name of the RAID device to use (such as md0 or md1). RAID devices range from md0 to md15, and each may only be used once.

- **--spares** — Specifies the number of spare drives allocated for the RAID array. Spare drives are used to rebuild the array in case of drive failure.

- **--grow** — Only supported for RAID0. Tells the RAID device to grow to fill available space (if any), or up to the maximum size setting.

- **--fsprofile** — Specifies a usage type to be passed to the program that makes a filesystem on this partition. A usage type defines a variety of tuning parameters to be used when making a filesystem. For this option to work, the filesystem must support the concept of usage types and there must be a configuration file that lists valid types. For ext2, ext3, and ext4, this configuration file is /etc/mke2fs.conf.
Kickstart Options

- **--fstype=** — Sets the file system type for the RAID array. Valid values are xfs, ext2, ext3, ext4, swap, vfat, and hfs.

- **--fsoptions=** — Specifies a free form string of options to be used when mounting the filesystem. This string will be copied into the /etc/fstab file of the installed system and should be enclosed in quotes.

- **--noformat** — Use an existing RAID device and do not format the RAID array.

- **--useexisting** — Use an existing RAID device and reformat it.

- **--encrypted** — Specifies that this RAID device should be encrypted, using the passphrase provided in the **--passphrase** option. If you do not specify a passphrase, anaconda uses the default, system-wide passphrase set with the autopart **--passphrase** command, or stops the installation and prompts you to provide a passphrase if no default is set.

- **--passphrase=** — Specifies the passphrase to use when encrypting this RAID device. You must use this option together with the **--encrypted** option; by itself it has no effect.

- **--escrowcert=** — Store the data encryption key for this device in a file in /root, encrypted using the X.509 certificate from the URL specified with **URL_of_X.509_certificate**. This option is only meaningful if **--encrypted** is specified.

- **--backuppassphrase=** — Add a randomly-generated passphrase to this device. Store the passphrase in a file in /root, encrypted using the X.509 certificate specified with **--escrowcert**. This option is only meaningful if **--escrowcert** is specified.

The following example shows how to create a RAID level 1 partition for /, and a RAID level 5 for /usr, assuming there are three SCSI disks on the system. It also creates three swap partitions, one on each drive.

```
part raid.01 --size=60 --ondisk=sda
part raid.02 --size=60 --ondisk=sdb
part raid.03 --size=60 --ondisk=sdc

part swap --size=128 --ondisk=sda
part swap --size=128 --ondisk=sdb
part swap --size=128 --ondisk=sdc

part raid.11 --size=1 --grow --ondisk=sda
part raid.12 --size=1 --grow --ondisk=sdb
part raid.13 --size=1 --grow --ondisk=sdc

raid / --level=1 --device=md0 raid.01 raid.02 raid.03
raid /usr --level=5 --device=md1 raid.11 raid.12 raid.13
```

For a detailed example of raid in action, refer to Section 15.4.1, "Advanced Partitioning Example".

**reboot** (optional)

Reboot after the installation is successfully completed (no arguments). Normally, kickstart displays a message and waits for the user to press a key before rebooting.

The **reboot** option is equivalent to the **shutdown -r** command.

For other completion methods, refer to the **halt**, **poweroff**, and **shutdown** kickstart options.
Chapter 15. Kickstart Installations

The `halt` option is the default completion method if no other methods are explicitly specified in the kickstart file.

**Note**

Use of the `reboot` option may result in an endless installation loop, depending on the installation media and method.

**repo** (optional)

Configures additional yum repositories that may be used as sources for package installation. Multiple repo lines may be specified.

```
repo --name=<repoid> [--baseurl=<url> | --mirrorlist=<url>]
```

- **--name** — The repo id. This option is required.
- **--baseurl** — The URL for the repository. The variables that may be used in yum repo config files are not supported here. You may use one of either this option or --mirrorlist, not both.
- **--mirrorlist** — The URL pointing at a list of mirrors for the repository. The variables that may be used in yum repo config files are not supported here. You may use one of either this option or --baseurl, not both.

**rootpw** (required)

Sets the system's root password to the `<password>` argument.

```
rootpw [--iscrypted] <password>
```

- **--iscrypted** — If this is present, the password argument is assumed to already be encrypted.

**selinux** (optional)

 Sets the state of SELinux on the installed system. SELinux defaults to enforcing in anaconda.

```
selinux [--disabled][--enforcing][--permissive]
```

- **--enforcing** — Enables SELinux with the default targeted policy being enforced.

**Note**

If the `selinux` option is not present in the kickstart file, SELinux is enabled and set to `--enforcing` by default.

- **--permissive** — Outputs warnings based on the SELinux policy, but does not actually enforce the policy.
- **--disabled** — Disables SELinux completely on the system.
For more information regarding SELinux for Fedora, refer to the Fedora Deployment Guide.

**services** (optional)
Modifies the default set of services that will run under the default runlevel. The list of disabled services is processed before the list of enabled services. Therefore, if a service appears on both lists, it is enabled.

- **--disabled** — Disable the services given in the comma separated list.
- **--enabled** — Enable the services given in the comma separated list.

*Do not include spaces in the list of services*

If you include spaces in the comma-separated list, kickstart will enable or disable only the services up to the first space. For example:

```
services --disabled auditd, cups,smartd, nfslock
```

will disable only the `auditd` service. To disable all four services, this entry should include no spaces between services:

```
services --disabled auditd,cups,smartd,nfslock
```

**shutdown** (optional)
Shut down the system after the installation has successfully completed. During a kickstart installation, if no completion method is specified, the `halt` option is used as default.

The `shutdown` option is equivalent to the `shutdown` command.

For other completion methods, refer to the `halt`, `poweroff`, and `reboot` kickstart options.

**skipx** (optional)
If present, X is not configured on the installed system.

*Package selection might configure X*

If you install a display manager among your package selection options, this package will create an X configuration, and the installed system will default to run level 5. The effect of the `skipx` option is overridden.

**sshpw** (optional)

During installation, you can interact with `anaconda` and monitor its progress over an SSH connection. Use the `sshpw` command to create temporary accounts through which to log on. Each instance of the command creates a separate account that exists only in the installation environment. These accounts are not transferred to the installed system.

```
sshpw --username=<name> <password> [--iscrypted|--plaintext] [--lock]
```
Chapter 15. Kickstart Installations

- **--username** — Provides the name of the user. This option is required.
- **--iscrypted** — Specifies that the password is already encrypted.
- **--plaintext** — Specifies that the password is in plain text and not encrypted.
- **--lock** — If this is present, the new user account is locked by default. That is, the user will not be able to login from the console.

**Important — You must boot with sshd=1**

By default, the ssh server is not started during installation. To make ssh available during installation, boot the system with the kernel boot option `sshd=1`. Refer to Section 11.2.3, “Enabling Remote Access with ssh” for details of how to specify this kernel option at boot time.

**text (optional)**

Perform the kickstart installation in text mode. Kickstart installations are performed in graphical mode by default.

**Important**

If you select text mode for a kickstart installation, make sure that you specify choices for the partitioning, bootloader, and package selection options. These steps are automated in text mode, and anaconda cannot prompt you for missing information. If you do not provide choices for these options, anaconda will stop the installation process.

**timezone (required)**

Sets the system time zone to `<timezone>` which may be any of the time zones listed by timeconfig.

```
timezone [--utc] <timezone>
```

- **--utc** — If present, the system assumes the hardware clock is set to UTC (Greenwich Mean) time.

**upgrade (optional)**

Tells the system to upgrade an existing system rather than install a fresh system. You must specify one of `cdrom`, `harddrive`, `nfs`, or `url` (for FTP and HTTP) as the location of the installation tree. Refer to `install` for details.

**user (optional)**

Creates a new user on the system.

```
user --name=<username> [--groups=<list>] [--homedir=<homedir>] [--password=<password>] [--iscrypted] [--shell=<shell>] [--uid=<uid] [--name=]
```

- **--name=** — Provides the name of the user. This option is required.
Kickstart Options

• **--groups=** — In addition to the default group, a comma separated list of group names the user should belong to. The groups must exist before the user account is created.

• **--homedir=** — The home directory for the user. If not provided, this defaults to /home/<username>.

• **--password=** — The new user’s password. If not provided, the account will be locked by default.

• **--iscrypted=** — Is the password provided by --password already encrypted or not?

• **--shell=** — The user’s login shell. If not provided, this defaults to the system default.

• **--uid=** — The user’s UID. If not provided, this defaults to the next available non-system UID.

**vnc (optional)**

Allows the graphical installation to be viewed remotely via VNC. This method is usually preferred over text mode, as there are some size and language limitations in text installs. With no options, this command will start a VNC server on the machine with no password and will print out the command that needs to be run to connect a remote machine.

```
vnc [--host=<hostname>] [--port=<port>] [--password=<password>]
```

• **--host=** — Instead of starting a VNC server on the install machine, connect to the VNC viewer process listening on the given hostname.

• **--port=** — Provide a port that the remote VNC viewer process is listening on. If not provided, anaconda will use the VNC default.

• **--password=** — Set a password which must be provided to connect to the VNC session. This is optional, but recommended.

**volgroup (optional)**

Use to create a Logical Volume Management (LVM) group with the syntax:

```
volgroup <name> <partition> <options>
```

The options are as follows:

• **--noformat** — Use an existing volume group and do not format it.

• **--useexisting** — Use an existing volume group and reformat it.

• **--pesize=** — Set the size of the physical extents.

Create the partition first, create the logical volume group, and then create the logical volume. For example:

```
part pv.01 --size 3000
volgroup myvg pv.01
logvol / --vgname=myvg --size=2000 --name=rootvol
```

For a detailed example of **volgroup** in action, refer to Section 15.4.1, “Advanced Partitioning Example”.

**xconfig (optional)**
Chapter 15. Kickstart Installations

Configures the **X Window System**. If you install the **X Window System** with a kickstart file that does not include the `xconfig` command, you must provide the **X** configuration manually during installation.

Do not use this command in a kickstart file that does not install the **X Window System**.

- **--driver** — Specify the X driver to use for the video hardware.
- **--videoram=** — Specifies the amount of video RAM the video card has.
- **--defaultdesktop=** — Specify either GNOME or KDE to set the default desktop (assumes that GNOME Desktop Environment and/or KDE Desktop Environment has been installed through `%packages`).
- **--startxonboot** — Use a graphical login on the installed system.

**zerombr** (optional)

If `zerombr` is specified any invalid partition tables found on disks are initialized. This destroys all of the contents of disks with invalid partition tables.

Note that this command was previously specified as `zerombr yes`. This form is now deprecated; you should now simply specify `zerombr` in your kickstart file instead.

**%include** (optional)

Use the `%include /path/to/file` command to include the contents of another file in the kickstart file as though the contents were at the location of the `%include` command in the kickstart file.

### 15.4.1. Advanced Partitioning Example

The following is a single, integrated example showing the `clearpart`, `raid`, `part`, `volgroup`, and `logvol` kickstart options in action:

```bash
# Raid 1 IDE config
part raid.11 --size 1000 --asprimary --ondrive=hda
part raid.12 --size 1000 --asprimary --ondrive=hda
part raid.13 --size 2000 --asprimary --ondrive=hda
part raid.14 --size 8000 --ondrive=hda
part raid.15 --size 16384 --grow --ondrive=hda
part raid.21 --size 1000 --asprimary --ondrive=hdc
part raid.22 --size 1000 --asprimary --ondrive=hdc
part raid.23 --size 2000 --asprimary --ondrive=hdc
part raid.24 --size 8000 --ondrive=hdc
part raid.25 --size 16384 --grow --ondrive=hdc

# You can add --spares=x
raid / --fstype ext3 --device md0 --level=RAID1 raid.11 raid.21
raid /safe --fstype ext3 --device md1 --level=RAID1 raid.12 raid.22
raid swap --fstype swap --device md2 --level=RAID1 raid.13 raid.23
raid /usr --fstype ext3 --device md3 --level=RAID1 raid.14 raid.24
raid pv.01 --fstype ext3 --device md4 --level=RAID1 raid.15 raid.25

# LVM configuration so that we can resize /var and /usr/local later
volgroup sysvg pv.01
logvol /var --vname=sysvg --size=8000 --name=var
logvol /var/freespace --vname=sysvg --size=8000 --name=freespacetouse
logvol /usr/local --vname=sysvg --size=1 --grow --name=usrlocal
```
This advanced example implements LVM over RAID, as well as the ability to resize various directories for future growth.

15.5. Package Selection

⚠️ Warning — do not install every available package

You can use a kickstart file to install every available package by specifying @Everything or simply * in the %packages section. However, using a kickstart file in this way will introduce package and file conflicts onto the installed system.

Use the %packages command to begin a kickstart file section that lists the packages you would like to install (this is for installations only, as package selection during upgrades is not supported).

You can specify packages by group or by their package names. The installation program defines several groups that contain related packages. Refer to the variant/repo/data/comps-*.xml file on the Fedora DVD for a list of groups. Each group has an id, user visibility value, name, description, and package list. If the group is selected for installation, the packages marked mandatory in the package list are always installed, the packages marked default are installed if they are not specifically excluded elsewhere, and the packages marked optional must be specifically included elsewhere even when the group is selected.

Specify groups, one entry to a line, starting with an @ symbol, a space, and then the full group name or group id as given in the comps.xml file. For example:

```
%packages
@ X Window System
@ Desktop
@ Sound and Video
```

Note that the Core and Base groups are always selected by default, so it is not necessary to specify them in the %packages section.

Specify individual packages by name, one entry to a line. You can use asterisks as wildcards to glob package names in entries. For example:

```
sqlite
curl
aspell
docbook*
```

The docbook* entry includes the packages docbook-dtds, docbook-simple, docbook-slides and others that match the pattern represented with the wildcard.

Use a leading dash to specify packages or groups to exclude from the installation. For example:

```
-@ Graphical Internet
-autofs
-ipa*fonts
```
Using a kickstart file to install every available package by specifying * will introduce package and file conflicts onto the installed system. Packages known to cause such problems are assigned to the @Conflicts (variant) group, where variant is Client, ComputeNode, Server or Workstation. If you specify * in a kickstart file, be sure to exclude @Conflicts (variant) or the installation will fail:

```
* -@Conflicts (Server)
```

Note that the Fedora Project does not support the use of * in a kickstart file, even if you exclude @Conflicts (variant).

The following options are available for the `%packages` option:

--nobase
Do not install the @Base group. Use this option to perform a minimal installation, for example, for a single-purpose server or desktop appliance.

--resolvedeps
The --resolvedeps option has been deprecated. Dependencies are now always resolved automatically.

--ignoredeps
The --ignoredeps option has been deprecated. Dependencies are resolved automatically every time now.

--ignoremissing
Ignore the missing packages and groups instead of halting the installation to ask if the installation should be aborted or continued. For example:

```
%packages --ignoremissing
```

## 15.6. Pre-installation Script

You can add commands to run on the system immediately after the ks.cfg has been parsed. This section must be placed towards the end of the kickstart file, after the kickstart commands described in Section 15.4, "Kickstart Options", and must start with the `%pre` command. If your kickstart file also includes a `%post` section, the order of the `%pre` and `%post` sections does not matter.

You can access the network in the `%pre` section; however, name service has not been configured at this point, so only IP addresses work.

Note that the pre-install script is not run in the change root environment.

--interpreter /usr/bin/python
Allows you to specify a different scripting language, such as Python. Replace /usr/bin/python with the scripting language of your choice.
15.6.1. Example

Here is an example %pre section:

```bash
#!/bin/sh
hds=""
mymedia=""
for file in /proc/ide/h* do
  mymedia=`cat $file/media`
  if [ $mymedia == "disk" ] ; then
    hds="$hds `basename $file`"
  fi
done
set $hds
numhd=`echo $#`
drive1=`echo $hds | cut -d' ' -f1`
drive2=`echo $hds | cut -d' ' -f2`
#Write out partition scheme based on whether there are 1 or 2 hard drives
if [ $numhd == "2" ] ; then
  #2 drives
  echo "#partitioning scheme generated in %pre for 2 drives" > /tmp/part-include
  echo "clearpart --all" >> /tmp/part-include
  echo "part /boot --fstype ext3 --size 75 --ondisk hda" >> /tmp/part-include
  echo "part / --fstype ext3 --size 1 --grow --ondisk hda" >> /tmp/part-include
  echo "part swap --recommended --ondisk $drive1" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 1 --grow --ondisk hdb" >> /tmp/part-include
else
  #1 drive
  echo "#partitioning scheme generated in %pre for 1 drive" > /tmp/part-include
  echo "clearpart --all" >> /tmp/part-include
  echo "part /boot --fstype ext3 --size 75" >> /tmp/part-include
  echo "part swap --recommended" >> /tmp/part-include
  echo "part / --fstype ext3 --size 2048" >> /tmp/part-include
  echo "part /home --fstype ext3 --size 2048 --grow" >> /tmp/part-include
fi
```

This script determines the number of hard drives in the system and writes a text file with a different partitioning scheme depending on whether it has one or two drives. Instead of having a set of partitioning commands in the kickstart file, include the line:

```bash
%include /tmp/part-include
```

The partitioning commands selected in the script are used.

### Note

The pre-installation script section of kickstart cannot manage multiple install trees or source media. This information must be included for each created ks.cfg file, as the pre-installation script occurs during the second stage of the installation process.

15.7. Post-installation Script

You have the option of adding commands to run on the system once the installation is complete. This section must be placed towards the end of the kickstart file, after the kickstart commands described in Section 15.4, "Kickstart Options", and must start with the %post command. If your kickstart file also includes a %pre section, the order of the %pre and %post sections does not matter.
This section is useful for functions such as installing additional software and configuring an additional nameserver.

**Note**

If you configured the network with static IP information, including a nameserver, you can access the network and resolve IP addresses in the `%post` section. If you configured the network for DHCP, the `/etc/resolv.conf` file has not been completed when the installation executes the `%post` section. You can access the network, but you cannot resolve IP addresses. Thus, if you are using DHCP, you must specify IP addresses in the `%post` section.

**Note**

The post-install script is run in a chroot environment; therefore, performing tasks such as copying scripts or RPMs from the installation media do not work.

**--nochroot**

Allows you to specify commands that you would like to run outside of the chroot environment.

The following example copies the file `/etc/resolv.conf` to the file system that was just installed.

```
%post --nochroot
    cp /etc/resolv.conf /mnt/sysimage/etc/resolv.conf
```

**--interpreter /usr/bin/python**

Allows you to specify a different scripting language, such as Python. Replace `/usr/bin/python` with the scripting language of your choice.

**--log /path/to/logfile**

Logs the output of the post-install script. Note that the path of the log file must take into account whether or not you use the **--nochroot** option. For example, without **--nochroot**:

```
%post --log=/root/ks-post.log
```

with **--nochroot**:

```
%post --nochroot --log=/mnt/sysimage/root/ks-post.log
```

### 15.7.1. Example

**Example 15.1. Run a script named runme from an NFS share:**

```
mkdir /mnt/temp
mount -o nolock 10.10.0.2:/usr/new-machines /mnt/temp
openvt -s -w -- /mnt/temp/runme
```
NFS file locking is not supported while in kickstart mode, therefore `-o nolock` is required when mounting an NFS mount.

15.8. Making the Kickstart File Available

A kickstart file must be placed in one of the following locations:

- On removable media, such as a floppy disk, optical disk, or USB flash drive
- On a hard drive
- On a network

Normally a kickstart file is copied to the removable media or hard drive, or made available on the network. The network-based approach is most commonly used, as most kickstart installations tend to be performed on networked computers.

Let us take a more in-depth look at where the kickstart file may be placed.

15.8.1. Creating Kickstart Boot Media

To perform a kickstart installation using removable media, the kickstart file must be named `ks.cfg` and must be located in the top-level directory of the disc.

Diskette-based booting is no longer supported in Fedora. Installations must use CD-ROM or flash memory products for booting. However, the kickstart file may still reside on a diskette's top-level directory, and must be named `ks.cfg`. Separate boot media will be required.

Refer to Section 3.3, “Making Minimal Boot Media” for instructions on creating boot media.

To perform a pen-based flash memory kickstart installation, the kickstart file must be named `ks.cfg` and must be located in the flash memory's top-level directory. Create the boot image first, and then copy the `ks.cfg` file.

Refer to Section 3.3, “Making Minimal Boot Media” for instructions on creating live USB media using the `Fedora-version-architecture-format.iso` image file that you can download from the Fedora Project site at `http://download.fedoraproject.org/`.

Note

Creation of USB flashdrives for booting is possible, but is heavily dependent on system hardware BIOS settings. Refer to your hardware manufacturer to see if your system supports booting to alternate devices.

15.8.2. Making the Kickstart File Available on the Network
Chapter 15. Kickstart Installations

Network installations using kickstart are quite common, because system administrators can quickly and easily automate the installation on many networked computers. In general, the approach most commonly used is for the administrator to have both a BOOTP/DHCP server and an NFS server on the local network. The BOOTP/DHCP server is used to give the client system its networking information, while the actual files used during the installation are served by the NFS server. Often, these two servers run on the same physical machine, but they are not required to.

Include the `ks` kernel boot option in the `append` line of a target in your `pxelinux.cfg/default` file to specify the location of a kickstart file on your network. The syntax of the `ks` option in a `pxelinux.cfg/default` file is identical to its syntax when used at the boot prompt. Refer to Section 15.10, “Starting a Kickstart Installation” for a description of the syntax and refer to Example 15.2, “Using the `ks` option in the `pxelinux.cfg/default` file” for an example of an `append` line.

If the `dhcpd.conf` file on the DHCP server is configured to point to `/tftpboot/pxelinux.0` on the BOOTP server (whether on the same physical machine or not), systems configured to boot over the network can load the kickstart file and commence installation.

Example 15.2. Using the `ks` option in the `pxelinux.cfg/default` file

For example, if `foo.ks` is a kickstart file available on an NFS share at `192.168.0.200:/export/kickstart/`, part of your `pxelinux.cfg/default` file might include:

```
label 1
    kernel Fedora17/vmlinuz
    append initrd=Fedora17/initrd.img ramdisk_size=10000 ks=nfs:192.168.0.200:/export/kickstart/foo.ks
```

15.9. Making the Installation Tree Available

The kickstart installation must access an installation tree. An installation tree is a copy of the binary Fedora DVD with the same directory structure.

If you are performing a DVD-based installation, insert the Fedora installation DVD into the computer before starting the kickstart installation.

If you are performing a hard drive installation, make sure the ISO images of the binary Fedora DVD are on a hard drive in the computer.

If you are performing a network-based (NFS, FTP, or HTTP) installation, you must make the installation tree or ISO image available over the network. Refer to Section 5.1, “Preparing for a Network Installation” for details.

15.10. Starting a Kickstart Installation
Important — Kickstart installations and firstboot

Firstboot does not run after a system is installed from a Kickstart file unless a desktop and the X Window System were included in the installation and graphical login was enabled. Either specify a user with the user option in the Kickstart file before installing additional systems from it (refer to Section 15.4, “Kickstart Options” for details) or log into the installed system with a virtual console as root and add users with the adduser command.

To begin a kickstart installation, you must boot the system from boot media you have made or the Fedora DVD, and enter a special boot command at the boot prompt. The installation program looks for a kickstart file if the ks command line argument is passed to the kernel.

DVD and local storage

The linux ks= command also works if the ks.cfg file is located on a vfat or ext2 file system on local storage and you boot from the Fedora DVD.

With Driver Disk

If you need to use a driver disk with kickstart, specify the dd option as well. For example, if installation requires a kickstart file on a local hard drive and also requires a driver disk, boot the system with:

```
linux ks=hd:partition:/path/ks.cfg dd
```

Boot CD-ROM

If the kickstart file is on a boot CD-ROM as described in Section 15.8.1, “Creating Kickstart Boot Media”, insert the CD-ROM into the system, boot the system, and enter the following command at the boot: prompt (where ks.cfg is the name of the kickstart file):

```
linux ks=cdrom:/ks.cfg
```

Other options to start a kickstart installation are as follows:

- **autostep**
  Make kickstart non-interactive.

- **debug**
  Start up pdb immediately.

- **dd**
  Use a driver disk.

- **dhcppclass=<class>**
  Sends a custom DHCP vendor class identifier. ISC’s dhcpcd can inspect this value using "option vendor-class-identifier".

- **dns=<dns>**
  Comma separated list of nameservers to use for a network installation.

- **driverdisk**
  Same as ‘dd’.
expert
   Turns on special features:
   • allows partitioning of removable media
   • prompts for a driver disk

gateway=<gw>
   Gateway to use for a network installation.

graphical
   Force graphical install. Required to have ftp/http use GUI.

isa
   Prompt user for ISA devices configuration.

ip=<ip>
   IP to use for a network installation, use ‘dhcp’ for DHCP.

ipv6=auto, ipv6= dhcp
   IPv6 configuration for the device. Use auto to specify automatic neighbor discovery or dhcp for a stateful configuration with DHCPv6. You cannot specify a static IPv6 address.

keymap=<keymap>
   Keyboard layout to use. Valid layouts include:
   • be-latin1 — Belgian
   • bg_bds-utf8 — Bulgarian
   • bg_pho-utf8 — Bulgarian (Phonetic)
   • br-abnt2 — Brazilian (ABNT2)
   • cf — French Canadian
   • croat — Croatian
   • cz-us-qwertz — Czech
   • cz-lat2 — Czech (qwerty)
   • de — German
   • de-latin1 — German (latin1)
   • de-latin1-nodeadkeys — German (latin1 without dead keys)
   • dvorak — Dvorak
   • dk — Danish
   • dk-latin1 — Danish (latin1)
   • es — Spanish
   • et — Estonian
   • fi — Finnish
• **fi-latin1** — Finnish (latin1)
• **fr** — French
• **fr-latin9** — French (latin9)
• **fr-latin1** — French (latin1)
• **fr-pc** — French (pc)
• **fr_CH** — Swiss French
• **fr_CH-latin1** — Swiss French (latin1)
• **gr** — Greek
• **hu** — Hungarian
• **hu101** — Hungarian (101 key)
• **is-latin1** — Icelandic
• **it** — Italian
• **it-ibm** — Italian (IBM)
• **it2** — Italian (it2)
• **jp106** — Japanese
• **ko** — Korean
• **la-latin1** — Latin American
• **mk-utf** — Macedonian
• **nl** — Dutch
• **no** — Norwegian
• **pl2** — Polish
• **pt-latin1** — Portuguese
• **ro** — Romanian
• **ru** — Russian
• **sr-cy** — Serbian
• **sr-latin** — Serbian (latin)
• **sv-latin1** — Swedish
• **sg** — Swiss German
• **sg-latin1** — Swiss German (latin1)
• **sk-qwerty** — Slovak (qwerty)
Chapter 15. Kickstart Installations

- slovene — Slovenian
- trq — Turkish
- uk — United Kingdom
- ua-utf — Ukrainian
- us-acentos — U.S. International
- us — U.S. English

The file `/usr/lib/python2.6/site-packages/system_config_keyboard/keyboard_models.py` on 32-bit systems or `/usr/lib64/python2.6/site-packages/system_config_keyboard/keyboard_models.py` on 64-bit systems also contains this list and is part of the `system-config-keyboard` package.

ks=nfs:<server>:/<path>
The installation program looks for the kickstart file on the NFS server `<server>`, as file `<path>`. The installation program uses DHCP to configure the Ethernet card. For example, if your NFS server is server.example.com and the kickstart file is in the NFS share `/mydir/ks.cfg`, the correct boot command would be `ks=nfs:server.example.com:/mydir/ks.cfg`.

ks=http://<server>:/<path>
The installation program looks for the kickstart file on the HTTP server `<server>`, as file `<path>`. The installation program uses DHCP to configure the Ethernet card. For example, if your HTTP server is server.example.com and the kickstart file is in the HTTP directory `/mydir/ks.cfg`, the correct boot command would be `ks=http://server.example.com/mydir/ks.cfg`.

ks=hd:<device>:/<file>
The installation program mounts the file system on `<device>` (which must be vfat or ext2), and looks for the kickstart configuration file as `<file>` in that file system (for example, `ks=hd:sda3:/mydir/ks.cfg`).

ks=bd:<biosdev>:/<path>
The installation program mounts the file system on the specified partition on the specified BIOS device `<biosdev>`, and looks for the kickstart configuration file specified in `<path>` (for example, `ks=bd:80p3:/mydir/ks.cfg`). Note this does not work for BIOS RAID sets.

ks=file:/<file>
The installation program tries to read the file `<file>` from the file system; no mounts are done. This is normally used if the kickstart file is already on the `initrd` image.

ks=cdrom:/<path>
The installation program looks for the kickstart file on CD-ROM, as file `<path>`.

ks
If `ks` is used alone, the installation program configures the Ethernet card to use DHCP. The kickstart file is read from NFS server specified by DHCP option server-name. The name of the kickstart file is one of the following:

- If DHCP is specified and the boot file begins with a `/`, the boot file provided by DHCP is looked for on the NFS server.
- If DHCP is specified and the boot file begins with something other than a `/`, the boot file provided by DHCP is looked for in the `/kickstart` directory on the NFS server.
• If DHCP did not specify a boot file, then the installation program tries to read the file `/kickstart/1.2.3.4-kickstart`, where 1.2.3.4 is the numeric IP address of the machine being installed.

**ksdevice=</device>**

The installation program uses this network device to connect to the network. You can specify the device in one of five ways:

• the device name of the interface, for example, eth0

• the MAC address of the interface, for example, 00:12:34:56:78:9a

• the keyword `link`, which specifies the first interface with its link in the **up** state

• the keyword `bootif`, which uses the MAC address that `pxelinux` set in the `BOOTIF` variable. Set IPAPPEND 2 in your `pxelinux.cfg` file to have `pxelinux` set the `BOOTIF` variable.

• the keyword `ibft`, which uses the MAC address of the interface specified by iBFT

For example, consider a system connected to an NFS server through the eth1 device. To perform a kickstart installation on this system using a kickstart file from the NFS server, you would use the command `ks=nfs:<server>:/<path> ksdevice=eth1` at the boot: prompt.

**kssendmac**

Adds HTTP headers to ks=http:// request that can be helpful for provisioning systems. Includes MAC address of all nics in CGI environment variables of the form: "X-RHN-Provisioning-MAC-0:eth0 01:23:45:67:89:ab".

**lang=</lang>**

Language to use for the installation. This should be a language which is valid to be used with the 'lang' kickstart command.

**loglevel=</level>**

Set the minimum level required for messages to be logged. Values for </level> are debug, info, warning, error, and critical. The default value is info.

**mediacheck**

Activates loader code to give user option of testing integrity of install source (if an ISO-based method).

**netmask=</nm>**

Netmask to use for a network installation.

**nofallback**

If GUI fails exit.

**nofb**

Do not load the VGA16 framebuffer required for doing text-mode installation in some languages.

**nofirewire**

Do not load support for firewire devices.

**noipv6**

Disable IPv6 networking during installation.
Chapter 15. Kickstart Installations

This option is not available during PXE installations

During installations from a PXE server, IPv6 networking might become active before anaconda processes the Kickstart file. If so, this option will have no effect during installation.

nomount
Don't automatically mount any installed Linux partitions in rescue mode.

nonet
Do not auto-probe network devices.

noparport
Do not attempt to load support for parallel ports.

nopass
Do not pass information about the keyboard and mouse from anaconda stage 1 (the loader) to stage 2 (the installer).

nopcmcia
Ignore PCMCIA controller in system.

noprobe
Do not automatically probe for hardware; prompt the user to allow anaconda to probe for particular categories of hardware.

noshell
Do not put a shell on tty2 during install.

repo=cdrom
Do a DVD based installation.

repo=ftp://<path>
Use <path> for an FTP installation.

repo=hd:<dev>://<path>
Use <path> on <dev> for a hard drive installation.

repo=http://<path>
Use <path> for an HTTP installation.

repo=nfs:<path>
Use <path> for an NFS installation.

rescue
Run rescue environment.

resolution=<mode>
Run installer in mode specified, ‘1024x768’ for example.

serial
Turns on serial console support.
Starting a Kickstart Installation

**skipddc**
Do not probe the Data Display Channel (DDC) of the monitor. This option provides a workaround if the DDC probe causes the system to stop responding.

**syslog=<host>[::<port>]**
Once installation is up and running, send log messages to the syslog process on <host>, and optionally, on port <port>. Requires the remote syslog process to accept connections (the \-r option).

**text**
Force text mode install.

---

**Important**

If you select text mode for a kickstart installation, make sure that you specify choices for the partitioning, bootloader, and package selection options. These steps are automated in text mode, and anaconda cannot prompt you for missing information. If you do not provide choices for these options, anaconda will stop the installation process.

---

**updates**
Prompt for storage device containing updates (bug fixes).

**updates=ftp://<path>**
Image containing updates over FTP.

**updates=http://<path>**
Image containing updates over HTTP.

**upgradeany**
Offer to upgrade any Linux installation detected on the system, regardless of the contents or the existence of the /etc/redhat-release file.

**vnc**
Enable vnc-based installation. You will need to connect to the machine using a vnc client application.

**vncconnect=<host>[::<port>]**
Connect to the vnc client named <host>, and optionally use port <port>.

Requires ‘vnc’ option to be specified as well.

**vncpassword=<password>**
Enable a password for the vnc connection. This will prevent someone from inadvertently connecting to the vnc-based installation.

Requires ‘vnc’ option to be specified as well.
**Kickstart Configurator**

*Kickstart Configurator* allows you to create or modify a kickstart file using a graphical user interface, so that you do not have to remember the correct syntax of the file.

*Kickstart Configurator* is not installed by default on Fedora 17. Run `su - yum install system-config-kickstart` or use your graphical package manager to install the software.

To launch *Kickstart Configurator*, boot your system into a graphical environment, then run `system-config-kickstart`, or click **Applications** → **System Tools** → **Kickstart** on the GNOME desktop or **Kickoff Application Launcher** → **Applications** → **System** → **Kickstart** on the KDE desktop.

As you are creating a kickstart file, you can click **File** → **Preview** at any time to review your current selections.

To start with an existing kickstart file, select **File** → **Open** and select the existing file.

### 16.1. Basic Configuration

![Figure 16.1. Basic Configuration](image)

Choose the language to use during the installation and as the default language to be used after installation from the **Default Language** menu.

Select the system keyboard type from the **Keyboard** menu.

From the **Time Zone** menu, choose the time zone to use for the system. To configure the system to use UTC, select **Use UTC clock**.
Enter the desired root password for the system in the **Root Password** text entry box. Type the same password in the **Confirm Password** text box. The second field is to make sure you do not mistype the password and then realize you do not know what it is after you have completed the installation. To save the password as an encrypted password in the file, select **Encrypt root password**. If the encryption option is selected, when the file is saved, the plain text password that you typed is encrypted and written to the kickstart file. Do not type an already encrypted password and select to encrypt it. Because a kickstart file is a plain text file that can be easily read, it is recommended that an encrypted password be used.

Choosing **Target Architecture** specifies which specific hardware architecture distribution is used during installation.

Choosing **Reboot system after installation** reboots your system automatically after the installation is finished.

Kickstart installations are performed in graphical mode by default. To override this default and use text mode instead, select the **Perform installation in text mode** option.

You can perform a kickstart installation in interactive mode. This means that the installation program uses all the options pre-configured in the kickstart file, but it allows you to preview the options in each screen before continuing to the next screen. To continue to the next screen, click the **Next** button after you have approved the settings or change them before continuing the installation. To select this type of installation, select the **Perform installation in interactive mode** option.

### 16.2. Installation Method

**Figure 16.2. Installation Method**
The **Installation Method** screen allows you to choose whether to perform a new installation or an upgrade. If you choose upgrade, the **Partition Information** and **Package Selection** options are disabled. They are not supported for kickstart upgrades.

Choose the type of kickstart installation or upgrade from the following options:

- **DVD** — Choose this option to install or upgrade from the Fedora DVD.
- **NFS** — Choose this option to install or upgrade from an NFS shared directory. In the text field for the NFS server, enter a fully-qualified domain name or IP address. For the NFS directory, enter the name of the NFS directory that contains the **variant** directory of the installation tree. For example, if the NFS server contains the directory `/mirrors/redhat/i386/Server/`, enter `/mirrors/redhat/i386/` for the NFS directory.
- **FTP** — Choose this option to install or upgrade from an FTP server. In the FTP server text field, enter a fully-qualified domain name or IP address. For the FTP directory, enter the name of the FTP directory that contains the **variant** directory. For example, if the FTP server contains the directory `/mirrors/redhat/i386/Server/`, enter `/mirrors/redhat/i386/Server/` for the FTP directory. If the FTP server requires a username and password, specify them as well.
- **HTTP** — Choose this option to install or upgrade from an HTTP server. In the text field for the HTTP server, enter the fully-qualified domain name or IP address. For the HTTP directory, enter the name of the HTTP directory that contains the **variant** directory. For example, if the HTTP server contains the directory `/mirrors/redhat/i386/Server/`, enter `/mirrors/redhat/i386/Server/` for the HTTP directory.
- **Hard Drive** — Choose this option to install or upgrade from a hard drive. Hard drive installations require the use of ISO images. Be sure to verify that the ISO images are intact before you start the installation. To verify them, use an `md5sum` program as well as the `linux mediacheck` boot option as discussed in Section 11.6.2, “Verifying boot media”. Enter the hard drive partition that contains the ISO images (for example, `/dev/hda1`) in the **Hard Drive Partition** text box. Enter the directory that contains the ISO images in the **Hard Drive Directory** text box.
16.3. Boot Loader Options

Please note that this screen will be disabled if you have specified a target architecture other than x86 / x86_64.

GRUB is the default boot loader for Fedora on x86 / x86_64 architectures. If you do not want to install a boot loader, select **Do not install a boot loader**. If you choose not to install a boot loader, make sure you create a boot diskette or have another way to boot your system, such as a third-party boot loader.

You must choose where to install the boot loader (the Master Boot Record or the first sector of the /boot partition). Install the boot loader on the MBR if you plan to use it as your boot loader.

To pass any special parameters to the kernel to be used when the system boots, enter them in the **Kernel parameters** text field. For example, if you have an IDE CD-ROM Writer, you can tell the kernel to use the SCSI emulation driver that must be loaded before using `cdrecord` by configuring `hdd=ide-scsi` as a kernel parameter (where `hdd` is the CD-ROM device).

You can password protect the GRUB boot loader by configuring a GRUB password. Select **Use GRUB password**, and enter a password in the **Password** field. Type the same password in the **Confirm Password** text field. To save the password as an encrypted password in the file, select **Encrypt GRUB password**. If the encryption option is selected, when the file is saved, the plain text password that you typed is encrypted and written to the kickstart file. If the password you typed was already encrypted, unselect the encryption option.

Whenever you are required to enter this password, you will also be asked for a username, which is **root**.

If **Upgrade an existing installation** is selected on the **Installation Method** page, select **Upgrade existing boot loader** to upgrade the existing boot loader configuration, while preserving the old entries.
16.4. Partition Information

Select whether or not to clear the Master Boot Record (MBR). Choose to remove all existing partitions, remove all existing Linux partitions, or preserve existing partitions.

To initialize the disk label to the default for the architecture of the system (for example, msdos for x86), select **Initialize the disk label** if you are installing on a brand new hard drive.

**Note**

Although anaconda and kickstart support Logical Volume Management (LVM), at present there is no mechanism for configuring this using the Kickstart Configurator.

16.4.1. Creating Partitions

To create a partition, click the **Add** button. The **Partition Options** window shown in Figure 16.5, "Creating Partitions" appears. Choose the mount point, file system type, and partition size for the new partition. Optionally, you can also choose from the following:

- In the **Additional Size Options** section, choose to make the partition a fixed size, up to a chosen size, or fill the remaining space on the hard drive. If you selected swap as the file system type, you can select to have the installation program create the swap partition with the recommended size instead of specifying a size.

- Force the partition to be created as a primary partition.

- Create the partition on a specific hard drive. For example, to make the partition on the first IDE hard disk (/dev/hda), specify hda as the drive. Do not include /dev in the drive name.
• Use an existing partition. For example, to make the partition on the first partition on the first IDE hard disk (/dev/hda1), specify hda1 as the partition. Do not include /dev in the partition name.

• Format the partition as the chosen file system type.

![Partition Options Window](image)

**Figure 16.5. Creating Partitions**

To edit an existing partition, select the partition from the list and click the **Edit** button. The same **Partition Options** window appears as when you chose to add a partition as shown in **Figure 16.5, “Creating Partitions”**, except it reflects the values for the selected partition. Modify the partition options and click **OK**.

To delete an existing partition, select the partition from the list and click the **Delete** button.

**16.4.1.1. Creating Software RAID Partitions**

To create a software RAID partition, use the following steps:

1. Click the **RAID** button.
2. Select **Create a software RAID partition**.

3. Configure the partitions as previously described, except select **Software RAID** as the file system type. Also, you must specify a hard drive on which to make the partition or specify an existing partition to use.

![Figure 16.6. Creating a Software RAID Partition](image)

Repeat these steps to create as many partitions as needed for your RAID setup. All of your partitions do not have to be RAID partitions.

After creating all the partitions needed to form a RAID device, follow these steps:

1. Click the **RAID** button.

2. Select **Create a RAID device**.

3. Select a mount point, file system type, RAID device name, RAID level, RAID members, number of spares for the software RAID device, and whether to format the RAID device.
4. Click **OK** to add the device to the list.

### 16.5. Network Configuration
If the system to be installed via kickstart does not have an Ethernet card, do not configure one on the Network Configuration page.

Networking is only required if you choose a networking-based installation method (NFS, FTP, or HTTP). Networking can always be configured after installation with the Network Administration Tool (system-config-network). Refer to the Fedora Deployment Guide for details.

For each Ethernet card on the system, click Add Network Device and select the network device and network type for the device. Select eth0 to configure the first Ethernet card, eth1 for the second Ethernet card, and so on.

### 16.6. Authentication
Chapter 16. Kickstart Configurator

In the Authentication section, select whether to use shadow passwords and MD5 encryption for user passwords. These options are highly recommended and chosen by default.

The Authentication Configuration options allow you to configure the following methods of authentication:

- NIS
- LDAP
- Kerberos 5
- Hesiod
- SMB
- Name Switch Cache

These methods are not enabled by default. To enable one or more of these methods, click the appropriate tab, click the checkbox next to Enable, and enter the appropriate information for the authentication method. Refer to the Fedora Deployment Guide for more information about the options.

16.7. Firewall Configuration

The Firewall Configuration window is similar to the screen in the installation program and the Security Level Configuration Tool.
If **Disable firewall** is selected, the system allows complete access to any active services and ports. No connections to the system are refused or denied.

Selecting **Enable firewall** configures the system to reject incoming connections that are not in response to outbound requests, such as DNS replies or DHCP requests. If access to services running on this machine is required, you can choose to allow specific services through the firewall.

Only devices configured in the **Network Configuration** section are listed as available **Trusted devices**. Connections from any devices selected in the list are accepted by the system. For example, if **eth1** only receives connections from internal system, you might want to allow connections from it.

If a service is selected in the **Trusted services** list, connections for the service are accepted and processed by the system.

In the **Other ports** text field, list any additional ports that should be opened for remote access. Use the following format: **port:protocol**. For example, to allow IMAP access through the firewall, specify **imap:tcp**. Numeric ports can also be specified explicitly; to allow UDP packets on port 1234 through the firewall, enter **1234:udp**. To specify multiple ports, separate them with commas.

### 16.7.1. SELinux Configuration

Kickstart can set SELinux to **enforcing**, **permissive** or **disabled** mode. Finer grained configuration is not possible at this time.

### 16.8. Display Configuration

If you are installing the X Window System, you can configure it during the kickstart installation by checking the **Configure the X Window System** option on the **Display Configuration** window as shown in **Figure 16.11, “X Configuration”**. If this option is not chosen, the X configuration options are disabled and the **skipx** option is written to the kickstart file.
Chapter 16. Kickstart Configurator

Figure 16.11. X Configuration

Select whether to start the Setup Agent the first time the installed system boots. The Setup Agent is disabled by default, but the setting can be changed to enabled or enabled in reconfiguration mode. Reconfiguration mode enables the language, mouse, keyboard, root password, security level, time zone, and networking configuration options in addition to the default ones.

16.9. Package Selection

Figure 16.12. Package Selection

The Package Selection window allows you to choose which package groups to install.
Package resolution is carried out automatically.

Currently, Kickstart Configurator does not allow you to select individual packages. To install individual packages, modify the %packages section of the kickstart file after you save it. Refer to Section 15.5, “Package Selection” for details.

16.10. Pre-Installation Script

You can add commands to run on the system immediately after the kickstart file has been parsed and before the installation begins. If you have configured the network in the kickstart file, the network is enabled before this section is processed. To include a pre-installation script, type it in the text area.

To specify a scripting language to use to execute the script, select the Use an interpreter option and enter the interpreter in the text box beside it. For example, /usr/bin/python2.6 can be specified for a Python script. This option corresponds to using %pre --interpreter /usr/bin/python2.6 in your kickstart file.

Only the most commonly used commands are available in the pre-installation environment:

arping, awk, basename, bash, bunzip2, bzcat, cat, chattr, chgrp, chmod, chown, chroot, chvt, clear, cp, cpio, cut, date, dd, df, dirname, dmesg, du, e2fsck, e2label, echo, egrep, eject, env, expr, false, fdisk, fgrep, find, fsck, fsck.ext2, fsck.ext3, ftp, grep, gunzip, gzip, hdparm, head, hostname, hwclock, ifconfig, insmod, ip, ipcalc, kill, killall, less, ln, load_policy, login, losetup, ls, lsattr, lsmod, lvm, md5sum, mkdir, mke2fs, mkfs.ext2, mkfs.ext3, mkinitfs, mkswap, mktemp, modprobe, more, mount, mt, mv, nslookup, openvt, pidof, ping, ps, pwd, readlink, rm, rmdir, rmmod, route, rpm, sed, sh, sha1sum, sleep, sort, swapoff, swapon, sync, tail, tar, tee, top, touch, true, tune2fs, umount, uniq, vconfig, vi, wc, wget, xargs, zcat.
Chapter 16. Kickstart Configurator

Important

Do not include the `%pre` command. It is added for you.

Note

The pre-installation script is run after the source media is mounted and stage 2 of the bootloader has been loaded. For this reason it is not possible to change the source media in the pre-installation script.

16.11. Post-Installation Script

You can also add commands to execute on the system after the installation is completed. If the network is properly configured in the kickstart file, the network is enabled, and the script can include commands to access resources on the network. To include a post-installation script, type it in the text area.

Important

Do not include the `%post` command. It is added for you.
For example, to change the message of the day for the newly installed system, add the following command to the \%post section:

```bash
echo "Hackers will be punished" > /etc/motd
```

**Note**

More examples can be found in Section 15.7.1, “Example”.

### 16.11.1. Chroot Environment

To run the post-installation script outside of the chroot environment, click the checkbox next to this option on the top of the Post-Installation window. This is equivalent to using the \--nochroot option in the \%post section.

To make changes to the newly installed file system, within the post-installation section, but outside of the chroot environment, you must prepend the directory name with `/mnt/sysimage/`.

For example, if you select Run outside of the chroot environment, the previous example must be changed to the following:

```bash
echo "Hackers will be punished" > /mnt/sysimage/etc/motd
```

### 16.11.2. Use an Interpreter

To specify a scripting language to use to execute the script, select the Use an interpreter option and enter the interpreter in the text box beside it. For example, `/usr/bin/python2.2` can be specified for a Python script. This option corresponds to using \%post --interpreter `/usr/bin/python2.2` in your kickstart file.

### 16.12. Saving the File

To review the contents of the kickstart file after you have finished choosing your kickstart options, select **File => Preview** from the pull-down menu.
To save the kickstart file, click the **Save to File** button in the preview window. To save the file without previewing it, select **File** => **Save File** or press **Ctrl+S**. A dialog box appears. Select where to save the file.

After saving the file, refer to **Section 15.10, “Starting a Kickstart Installation”** for information on how to start the kickstart installation.
Part III. After installation

This part of the *Fedora Installation Guide* covers finalizing the installation, as well as some installation-related tasks that you might perform at some time in the future. These include:

- using a Fedora installation disk to rescue a damaged system.
- upgrading to a new version of Fedora.
- removing Fedora from your computer.
Firstboot

**Important — Firstboot not available after text-mode installation**

Firstboot is only available on systems after a graphical installation or after a kickstart installation where a desktop and the X window system were installed and graphical login was enabled. If you performed a text-mode installation or a kickstart installation that did not include a desktop and the X window system, the Firstboot configuration tool does not appear.

**Firstboot** launches the first time that you start a new Fedora system. Use **Firstboot** to configure the system for use before you log in.

**Welcome**

There are a few more steps to take before your system is ready to use. The Setup Agent will now guide you through some basic configuration. Please click the "Forward" button in the lower right corner to continue.

![Fedora logo](image)

*Figure 17.1. Firstboot welcome screen*

Select **Forward** to start Firstboot.
17.1. License Agreement

This screen displays the overall licensing terms for Fedora. Each software package in Fedora is covered by its own license. All licensing guidelines for Fedora are located at http://fedoraproject.org/wiki/Legal/Licenses.

License Information

Thank you for installing Fedora. Fedora is a compilation of software packages, each under its own license. The compilation is made available under the GNU General Public License version 2. There are no restrictions on using, copying, or modifying this code. However, there are restrictions and obligations that apply to the redistribution of the code, either in its original or a modified form. Among other things, those restrictions/obligations pertain to the licensing of the redistribution, trademark rights, and export control.

If you would like to understand what those restrictions are, please visit http://fedoraproject.org/wiki/Legal/Licenses/LicenseAgreement.

Understood, please proceed.

If you agree to the terms of the licence, select Yes, I agree to the License Agreement and click Forward.

17.2. Create User

Create a user account for yourself with this screen. Always use this account to log in to your Fedora system, rather than using the root account.
Create User

You must create a "username" for regular (non-administrative) use of your system. To create a system "username", please provide the information requested below.

- **Full Name:**
- **Username:**
- **Password:**
- **Confirm Password:**

If you need to use network authentication, such as Kerberos or NIS, please click the Use Network Login button.

If you need more control when creating the user (specifying home directory, and/or UID), please click the Advanced button.

**Figure 17.3. Firstboot create user screen**

Enter a user name and your full name, and then enter your chosen password. Type your password once more in the **Confirm Password** box to ensure that it is correct.

Check the **Add to Administrators group** box if you would like administrative privileges. This will place you in the wheel group, which gives you access to all administrative functions, including installing and updating software, creating and altering configuration files, and administering other users.

To configure Fedora to use network services for authentication of user information, click **Use Network Login**. Refer to Section 17.2.1, "Authentication Configuration" for further details.

To create additional users or customise your first user account, click **Advanced** to open the **User Manager**.
In **User Manager** you can edit various properties, such as a private group for the user, the preferred login shell, and user and group IDs.

### Important — Create at least one user account

If you do not create at least one user account in this step, you will not be able to log in to the Fedora graphical environment. If you skipped this step during installation, refer to Section 10.4.3, “Booting into a Graphical Environment”.

### Note — Creating Extra User Accounts

To add additional user accounts to your system after the installation is complete, choose **System → Administration → Users & Groups**.

### 17.2.1. Authentication Configuration

If you clicked **Use Network Login** on the **Create User** screen, you must now specify how users are to be authenticated on the system. Use the drop-down menu to select from the following types of user database:
• **Local accounts only** (for use when the user database on the network is not accessible)

• **LDAP** (Lightweight Directory Access Protocol)

• **NIS** (Network Information Service)

• **Winbind** (for use with Microsoft Active Directory)

When you select the type of user database appropriate for your network, you must provide additional details relevant to that database type. For example, if you select **LDAP**, you must specify the **base distinguished name** for LDAP searches, and the address of the LDAP server. You must also select an **Authentication Method** relevant to the type of user database that you chose, for example, a Kerberos password, LDAP password, or NIS password.

The **Advanced Options** tab lets you enable other authentication mechanisms, including fingerprint readers, smart cards, and local access control in `/etc/security/access.conf`. 
Figure 17.6. Firstboot authentication Advanced Options screen

The **Password Options** tab lets you set format requirements for user passwords, including minimum length and required character classes such as lower case, upper case, and numbers.
17.3. Date and Time

Use this screen to adjust the date and time of the system clock. To change these settings after installation, click System → Administration → Date & Time.
Chapter 17. Firstboot

Figure 17.8. Firstboot date and time screen

Date and Time

Please set the date and time for the system.

Current date and time: Thu 18 Feb 2010 11:18:30 AM EST

☐ Synchronize date and time over the network

Manually set the date and time of your system:

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date: Sun Mon Tue Wed Thu Fri Sat</td>
<td></td>
</tr>
<tr>
<td>31</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
</tr>
<tr>
<td>14</td>
<td>15</td>
</tr>
<tr>
<td>21</td>
<td>22</td>
</tr>
<tr>
<td>28</td>
<td>1</td>
</tr>
<tr>
<td>7</td>
<td>8</td>
</tr>
</tbody>
</table>

Hour: 11
Minute: 14
Second: 57

Click the Synchronize date and time over the network checkbox to configure your system to use Network Time Protocol (NTP) servers to maintain the accuracy of the clock. NTP provides time synchronization service to computers on the same network. Many public NTP servers are available on the Internet.

17.4. Hardware Profile

Firstboot displays a screen that allows you to submit your hardware information anonymously to the Fedora Project. Developers use these hardware details to guide further support efforts. You can read more about this project and its development at http://smolts.org/.
Hardware Profile

Smolt is a hardware profiler for The Fedora Project. Submitting your profile is a great way to give back to the community as this information is used to help focus our efforts on popular hardware and platforms. Submissions are anonymous. Sending your profile will enable a monthly check-in.

![Hardware Profile Screen]

To opt in to this important work, select **Send Profile**. If you choose not to submit any profile data, do not change the default. Select **Finish** to continue to the login screen.

---

**Figure 17.9. Firstboot hardware profile screen**

To ensure the security of your system, run a package update after the installation completes. *Chapter 18, Your Next Steps* explains how to update your Fedora system.
Your Next Steps

18.1. Updating Your System

The Fedora Project releases updated software packages for Fedora throughout the support period of each version. Updated packages add new features, improve reliability, resolve bugs, or remove security vulnerabilities. To ensure the security of your system, update regularly, and as soon as possible after a security announcement is issued. Refer to Section 18.4, “Subscribing to Fedora Announcements and News” for information on the Fedora announcements services.

An update applet reminds you of updates when they are available. This applet is installed by default in Fedora. It checks for software updates from all configured repositories, and runs as a background service. It generates a notification message on the desktop if updates are found, and you can click the message to update your system’s software.

To update your system with the latest packages manually, use Update System:

1. Choose System → Administration → Update System.
2. To review the list of updated packages, select Review.
3. Click Update System to begin the update process.
4. If one or more updates require a system reboot, the update process displays a dialog with the option to Reboot Now. Either select this option to reboot the system immediately, or Cancel it and reboot the system at a more convenient time.
5. If a reboot is not required the update will conclude with a dialog that indicates that the System Update Completed and all selected updates have been successfully installed as well as a button to Close Update System.

To update packages from the command-line, use the yum utility. Type this command to begin a full update of your system with yum:

```
su -c 'yum update'
```
Chapter 18. Your Next Steps

Enter the root password when prompted.

Refer to http://docs.fedoraproject.org/yum/ for more information on yum.

### Network Connection Required

Ensure that your system has an active network connection before you run the Update Software tool, or the yum utility. The update process downloads information and packages from a network of servers.

If your Fedora system has a permanent network connection, you may choose to enable daily system updates. To enable automatic updates, follow the instructions on the webpage http://docs.fedoraproject.org/yum/sn-updating-your-system.html.

#### 18.2. Finishing an Upgrade

### System Updates Recommended

Once you have rebooted your system after performing an upgrade, you should also perform a manual system update. Consult Section 18.1, "Updating Your System" for more information.

If you chose to upgrade your system from a previous release rather than perform a fresh installation, you may want to examine the differences in the package set. Section 9.11.2, “Upgrading Using the Installer” advised you to create a package listing for your original system. You can now use that listing to determine how to bring your new system close to the original system state.

Most software repository configurations are stored in packages that end with the term release. Check the old package list for the repositories that were installed:

```bash
awk '{print $1}' ~/old-pkglist.txt | grep 'release$
```

If necessary, retrieve and install these packages from their original sources on the Internet. Follow the instructions at the originating site to install the repository configuration packages for use by yum and other software management tools on your Fedora system.

Then run the following commands to make a list of other missing software packages:

```bash
awk '{print $1}' ~/old-pkglist.txt | sort | uniq > ~/old-pkgnames.txt
rpm -qa --qf '%{NAME}
' sort | uniq > ~/new-pkgnames.txt
diff -u ~/old-pkgnames.txt ~/new-pkgnames.txt | grep '^-' | sed 's/^-.//' > /tmp/pkgs-to-install.txt
```

Now use the file /tmp/pkgs-to-install.txt with the yum command to restore most or all of your old software:

```bash
su -c 'yum install `cat /tmp/pkgs-to-install.txt`'
```
Missing Software

Due to changes in package complements between Fedora releases, it is possible this method may not restore all the software on your system. You can use the routines above to again compare the software on your system, and remedy any problems you find.

18.3. Switching to a Graphical Login

Important — Access to Software Repositories Might Be Required

To switch to a graphical environment, you might need to install extra software from a repository. You can access Fedora repositories through the Internet or use a Fedora installation DVD as a repository. Refer to Section 18.3.1, “Enabling Access to Software Repositories from the Command Line”.

If you installed using a text login and wish to switch to a graphical login, follow this procedure.

1. If you are not already root, switch users to the root account:

   ```
   su -
   ```

   Provide the administrator password when prompted.

2. If you have not already done so, install the X Window System and a graphical desktop environment. For example, to install the GNOME desktop environment, use this command:

   ```
   yum groupinstall "X Window System" Desktop
   ```

   To install the KDE desktop environment, use:

   ```
   yum groupinstall "X Window System" "KDE Desktop"
   ```

   This step may take some time as your Fedora system downloads and installs additional software. You may be asked to provide the installation media depending on your original installation source.

3. Run the following commands to change the run level:

   ```
   rm -f /etc/systemd/system/default.target
   ln -s /lib/systemd/system/graphical.target
   /etc/systemd/system/default.target
   ```

   Reboot the system using the `reboot` command. Your system will restart and present a graphical login.
If you encounter any problems with the graphical login, refer to Chapter 10, Troubleshooting Installation on an Intel or AMD System.

18.3.1. Enabling Access to Software Repositories from the Command Line

The usual way to install new software on a Fedora system is through a software repository. You can access Fedora repositories through the Internet, or use a Fedora installation DVD as a repository. The software that you access through online repositories is more up-to-date than what is available on an installation DVD. Furthermore, configuring a Fedora system to access online repositories is generally easier than configuring the system to use an installation DVD as a repository, as long as you have an existing, wired network connection available.

18.3.1.1. Enabling Access to Software Repositories Through the Internet

By default, every Fedora installation is already configured to access Fedora repositories through the Internet. Therefore, all you must do is ensure that the system can access the Internet. If you have an existing, wired network connection available, this process is straightforward:

1. If you are not already root, switch users to the root account:

   ```
   su -
   ```

2. Ensure that the system is plugged into your network. Note that your network might be as small as two devices — a computer and an external modem/router.

3. Run `system-config-network`. The network configuration tool starts and displays the Select Action screen.

4. Select Device configuration and press Enter. The network configuration tool displays the Select A Device screen with a list of network interfaces present on your system. The first interface is named eth0 by default.

5. Select a network interface to configure and press Enter. The network configuration tool takes you to the Network Configuration screen.

6. You can manually configure a static IP, gateway, and DNS servers on this screen or leave these fields blank to accept the default values. When you have chosen a configuration, select OK, and press Enter. The network configuration tool takes you back to the Select A Device screen.

7. Select Save and press Enter. The network configuration tool takes you back to the Select Action screen.

8. Select Save&Quit and press Enter. The network configuration tool saves your settings and exits.

9. Run `ifup interface`, where interface is the network interface that you configured with the network configuration tool. For example, run `ifup eth0` to start eth0.

Configuration of dial-up or wireless Internet connections is more complicated and beyond the scope of this guide.

18.3.1.2. Using a Fedora Installation DVD as a Software Repository

To use a Fedora installation DVD as a software repository, either in the form of a physical disc, or in the form of an ISO image file.
1. If you are using a physical DVD, insert the disc into your computer.

2. If you are not already root, switch users to the root account:

   su -

3. Create a mount point for the repository:

   mkdir -p /path/to/repo

   where /path/to/repo is a location for the repository, for example, /mnt/repo

4. Mount the DVD on the mount point that you just created. If you are using a physical disc, you need to know the device name of your DVD drive. You can find the names of any CD or DVD drives on your system with the command cat /proc/sys/dev/cdrom/info. The first CD or DVD drive on the system is typically named sr0. When you know the device name, mount the DVD:

   mount -r -t iso9660 /dev/device_name /path/to/repo

   For example: mount -r -t iso9660 /dev/sr0 /mnt/repo

   If you are using an ISO image file of a disc, mount the image file like this:

   mount -r -t iso9660 -o loop /path/to/image/file.iso /path/to/repo

   For example: mount -r -o loop /home/root/Downloads/Fedora17-Server-i386-DVD.iso /mnt/repo

   Note that you can only mount an image file if the storage device that holds the image file is itself mounted. For example, if the image file is stored on a hard drive that it not mounted automatically when the system boots, you must mount the hard drive before you mount an image file stored on that hard drive. Consider a hard drive named /dev/sdb that is not automatically mounted at boot time and which has an image file stored in a directory named Downloads on its first partition:

   mkdir /mnt/temp
   mount /dev/sdb1 /mnt/temp
   mkdir /mnt/repo
   mount -r -t iso9660 -o loop /mnt/temp/Downloads/Fedora-17-i386-DVD.iso /mnt/repo

   If you are not sure whether a storage device is mounted, run the mount command to obtain a list of current mounts. If you are not sure of the device name or partition number of a storage device, run fdisk -l and try to identify it in the output.

5. Create a new repo file in the /etc/yum.repos.d/ directory. The name of the file is not important, as long as it ends in .repo. For example, dvd.repo is an obvious choice.

   1. Choose a name for the repo file and open it as a new file with the vi text editor. For example:

      vi /etc/yum.repos.d/dvd.repo

   2. Press the I key to enter insert mode.

   3. Supply the details of the repository. For example:
Chapter 18. Your Next Steps

```bash
[dvd]
baseurl=file:///mnt/repo/Server
enabled=1
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-fedora-$basearch
```

The name of the repository is specified in square brackets — in this example, `[dvd]`. The name is not important, but you should choose something that is meaningful and recognizable.

The line that specifies the `baseurl` should contain the path to the mount point that you created previously, suffixed with `/Server` for a Fedora server installation DVD, or with `/Client` for a Fedora client installation DVD.

4. Press the `Esc` key to exit `insert` mode.

5. Type `:wq` and press the `Enter` key to save the file and exit the `vi` text editor.

6. After installing or upgrading software from the DVD, delete the repo file that you created.

18.4. Subscribing to Fedora Announcements and News

To receive information about package updates, subscribe to either the announcements mailing list, or the RSS feeds.

Fedora Project announcements mailing list

https://www.redhat.com/mailman/listinfo/fedora-announce-list

Fedora Project RSS feeds

http://fedoraproject.org/infofeed/

The announcements mailing list also provides you with news on the Fedora Project, and the Fedora community.

Security Announcements

Announcements with the keyword `[SECURITY]` in the title identify package updates that resolve security vulnerabilities.

18.5. Finding Documentation and Support

Members of the Fedora community provide support through mailing lists, Web forums and Linux User Groups (LUGs) across the world.

The Web site for the formally endorsed forums is http://forums.fedoraproject.org/.

The following resources provide information on many aspects of Fedora:

- The FAQ on the Fedora Project website
  http://fedoraproject.org/wiki/FAQ

- The documents available from the Fedora Documentation Project Web site
  http://docs.fedoraproject.org/
• The Linux Documentation Project (LDP)  
  http://www.tldp.org/

• The Red Hat Enterprise Linux documentation, much of which also applies to Fedora  
  http://www.redhat.com/docs/manuals/enterprise/

Many other organizations and individuals also provide tutorials and HOWTOs for Fedora on their Web sites.

18.6. Joining the Fedora Community
The Fedora Project is driven by the individuals that contribute to it. Community members provide support and documentation to other users, help to improve the software included in Fedora by testing, and develop new software alongside the programmers employed by Red Hat. The results of this work are available to all.

To make a difference, start here:

http://join.fedoraproject.org/
Chapter 19.

Basic System Recovery

When things go wrong, there are ways to fix problems. However, these methods require that you understand the system well. This chapter describes how to boot into rescue mode, single-user mode, and emergency mode, where you can use your own knowledge to repair the system.

19.1. Rescue Mode

19.1.1. Common Problems

You might need to boot into one of these recovery modes for any of the following reasons:

- You are unable to boot normally into Fedora (runlevel 3 or 5).
- You are having hardware or software problems, and you want to get a few important files off of your system's hard drive.
- You forgot the root password.

19.1.1.1. Unable to Boot into Fedora

This problem is often caused by the installation of another operating system after you have installed Fedora. Some other operating systems assume that you have no other operating system(s) on your computer. They overwrite the Master Boot Record (MBR) that originally contained the GRUB boot loader. If the boot loader is overwritten in this manner, you cannot boot Fedora unless you can get into rescue mode and reconfigure the boot loader.

Another common problem occurs when using a partitioning tool to resize a partition or create a new partition from free space after installation, and it changes the order of your partitions. If the partition number of your / partition changes, the boot loader might not be able to find it to mount the partition. To fix this problem, boot in rescue mode and modify the /etc/grub.d/10_linux file.

For instructions on how to reinstall the GRUB boot loader from a rescue environment, refer to Section 19.1.2.1, “Reinstalling the Boot Loader”.

19.1.1.2. Hardware/Software Problems

This category includes a wide variety of different situations. Two examples include failing hard drives and specifying an invalid root device or kernel in the boot loader configuration file. If either of these occur, you might not be able to reboot into Fedora. However, if you boot into one of the system recovery modes, you might be able to resolve the problem or at least get copies of your most important files.

19.1.1.3. Root Password

What can you do if you forget your root password? To reset it to a different password, boot into rescue mode or single-user mode, and use the passwd command to reset the root password.
Chapter 19. Basic System Recovery

19.1.2. Booting into Rescue Mode

Rescue mode provides the ability to boot a small Fedora environment entirely from CD-ROM, or some other boot method, instead of the system's hard drive.

As the name implies, rescue mode is provided to rescue you from something. During normal operation, your Fedora system uses files located on your system's hard drive to do everything — run programs, store your files, and more.

However, there may be times when you are unable to get Fedora running completely enough to access files on your system's hard drive. Using rescue mode, you can access the files stored on your system's hard drive, even if you cannot actually run Fedora from that hard drive.

To boot into rescue mode, you must be able to boot the system using one of the following methods:\footnote{Refer to the earlier sections of this guide for more details.}

- By booting the system from a boot CD-ROM or DVD.
- By booting the system from other installation boot media, such as USB flash devices.
- By booting the system from the Fedora installation DVD.

Once you have booted using one of the described methods, add the keyword \texttt{rescue} as a kernel parameter. For example, for an x86 system, type the following command at the installation boot prompt:

```
linux rescue
```

You are prompted to answer a few basic questions, including which language to use. It also prompts you to select where a valid rescue image is located. Select from \texttt{Local CD-ROM}, \texttt{Hard Drive}, \texttt{NFS image}, \texttt{FTP}, or \texttt{HTTP}. The location selected must contain a valid installation tree, and the installation tree must be for the same version of Fedora as the Fedora disk from which you booted. If you used a boot CD-ROM or other media to start rescue mode, the installation tree must be from the same tree from which the media was created. For more information about how to set up an installation tree on a hard drive, NFS server, FTP server, or HTTP server, refer to the earlier section of this guide.

If you select a rescue image that does not require a network connection, you are asked whether or not you want to establish a network connection. A network connection is useful if you need to backup files to a different computer or install some RPM packages from a shared network location, for example.

The following message is displayed:

The rescue environment will now attempt to find your Linux installation and mount it under the directory /mnt/sysimage. You can then make any changes required to your system. If you want to proceed with this step choose 'Continue'. You can also choose to mount your file systems read-only instead of read-write by choosing 'Read-only'. If for some reason this process fails you can choose 'Skip' and this step will be skipped and you will go directly to a command shell.

If you select \texttt{Continue}, it attempts to mount your file system under the directory /mnt/sysimage/. If it fails to mount a partition, it notifies you. If you select \texttt{Read-Only}, it attempts to mount your file
system under the directory `/mnt/sysimage/`, but in read-only mode. If you select **Skip**, your file system is not mounted. Choose **Skip** if you think your file system is corrupted.

Once you have your system in rescue mode, a prompt appears on VC (virtual console) 1 and VC 2 (use the **Ctrl-Alt-F1** key combination to access VC 1 and **Ctrl-Alt-F2** to access VC 2):

```
sh-3.00b#
```

If you selected **Continue** to mount your partitions automatically and they were mounted successfully, you are in single-user mode.

Even if your file system is mounted, the default root partition while in rescue mode is a temporary root partition, not the root partition of the file system used during normal user mode (runlevel 3 or 5). If you selected to mount your file system and it mounted successfully, you can change the root partition of the rescue mode environment to the root partition of your file system by executing the following command:

```
chroot /mnt/sysimage
```

This is useful if you need to run commands such as **rpm** that require your root partition to be mounted as `/`. To exit the **chroot** environment, type **exit** to return to the prompt.

If you selected **Skip**, you can still try to mount a partition or LVM2 logical volume manually inside rescue mode by creating a directory such as `/foo`, and typing the following command:

```
mount -t ext4 /dev/mapper/VolGroup00-LogVol02 /foo
```

In the above command, `/foo` is a directory that you have created and `/dev/mapper/VolGroup00-LogVol02` is the LVM2 logical volume you want to mount. If the partition is of type **ext2** or **ext3**, replace **ext4** with **ext2** or **ext3** respectively.

If you do not know the names of all physical partitions, use the following command to list them:

```
fdisks -l
```

If you do not know the names of all LVM2 physical volumes, volume groups, or logical volumes, use the following commands to list them:

```
pvdisplay
```

```
vgdisplay
```

```
lvdisplay
```

---

237
From the prompt, you can run many useful commands, such as:

- `ssh`, `scp`, and `ping` if the network is started
- `dump` and `restore` for users with tape drives
- `parted` and `fdisk` for managing partitions
- `rpm` for installing or upgrading software
- `vi` for editing text files

### 19.1.2.1. Reinstalling the Boot Loader

In many cases, the GRUB boot loader can mistakenly be deleted, corrupted, or replaced by other operating systems.

The following steps detail the process on how GRUB is reinstalled on the master boot record:

1. Boot the system from an installation boot medium.
2. Type `linux rescue` at the installation boot prompt to enter the rescue environment.
3. Type `chroot /mnt/sysimage` to mount the root partition.
4. Type `/sbin/grub-install bootpart` to reinstall the GRUB boot loader, where `bootpart` is the boot partition (typically, `/dev/sda`).
5. Review the `/etc/grub.d/10_linux` file, as additional entries may be needed in the `/etc/grub.d/40_custom` for GRUB to control additional operating systems.
6. Reboot the system.

### 19.1.3. Booting into Single-User Mode

One of the advantages of single-user mode is that you do not need a boot CD-ROM; however, it does not give you the option to mount the file systems as read-only or not mount them at all.

If your system boots, but does not allow you to log in when it has completed booting, try single-user mode.

In single-user mode, your computer boots to runlevel 1. Your local file systems are mounted, but your network is not activated. You have a usable system maintenance shell. Unlike rescue mode, single-user mode automatically tries to mount your file system. **Do not use single-user mode if your file system cannot be mounted successfully.** You cannot use single-user mode if the runlevel 1 configuration on your system is corrupted.

On an x86 system using GRUB, use the following steps to boot into single-user mode:

1. Press the `Esc` key at boot time to load the GRUB splash screen, then press any key to enter the GRUB interactive menu.
2. Select Fedora with the version of the kernel that you wish to boot and type `a` to append the line.
3. Go to the end of the line and type `single` as a separate word (press the `Spacebar` and then type `single`). Press `Enter` to exit edit mode.
19.1.4. Booting into Emergency Mode

In emergency mode, you are booted into the most minimal environment possible. The root file system
is mounted read-only and almost nothing is set up. The main advantage of emergency mode over
single-user mode is that the init files are not loaded. If init is corrupted or not working, you can still
mount file systems to recover data that could be lost during a re-installation.

To boot into emergency mode, use the same method as described for single-user mode in
Section 19.1.3, “Booting into Single-User Mode” with one exception, replace the keyword single with
the keyword emergency.

19.2. Using rescue mode to fix or work around driver problems

A malfunctioning or missing driver can prevent a system from booting normally. Rescue mode
provides an environment in which you can add, remove, or replace a driver even when the system
fails to boot. Wherever possible, we recommend that you use the RPM package manager to remove
malfunctioning drivers or to add updated or missing drivers. If you cannot remove a malfunctioning
driver for some reason, you can instead blacklist the driver so that it does not load at boot time.

Note that when you install a driver from a driver disc, the driver disc updates all initramfs images on
the system to use this driver. If a problem with a driver prevents a system from booting, you cannot
rely on booting the system from another initramfs image.

19.2.1. Using RPM to add, remove, or replace a driver

In rescue mode, you can use RPM to install, remove, or update packages from the installed system,
even though you did not boot the installed system. To remove a malfunctioning driver:

1. Boot the system into rescue mode with the linux rescue command at the boot prompt, or the
   linux rescue dd command if you need to load a third-party driver from a driver disc. Follow
   the instructions in Section 19.1.2, “Booting into Rescue Mode” and do not choose to mount the
   installed system as read only.

2. Change the root directory to /mnt/sysimage/:

   chroot /mnt/sysimage/

3. Use the rpm -e command to remove the driver package. For example, to remove the kmod-
   foobar driver package, run:

   rpm -e kmod-foobar

4. Exit the chroot environment:

   exit

Installing a driver is a similar process, but the RPM package that contains the driver must be available
on the system.

1. Boot the system into rescue mode with the linux rescue command at the boot prompt, or the
   linux rescue dd command if you need to load a third-party driver from a driver disc. Follow
Chapter 19. Basic System Recovery

the instructions in Section 19.1.2, "Booting into Rescue Mode" and do not choose to mount the installed system as read only.

2. Make the RPM package that contains the driver available. For example, mount a CD or USB flash drive and copy the RPM package to a location of your choice under /mnt/sysimage/, for example: /mnt/sysimage/root/drivers/.

3. Change the root directory to /mnt/sysimage:

   chroot /mnt/sysimage/

4. Use the rpm -ivh command to install the driver package. For example, to install the kmod-foobar driver package from /root/drivers/, run:

   rpm -ivh /root/drivers/kmod-foobar-1.2.04.17.el6.i686

   Note that /root/drivers/ in this chroot environment is /mnt/sysimage/root/drivers/ in the original rescue environment.

When you have finished removing and installing drivers, reboot the system.

19.2.2. Blacklisting a driver

As described in Section 19.1.2, "Booting into Rescue Mode", the rdblacklist kernel option blacklists a driver at boot time. To continue to blacklist the driver on subsequent boots, add the rdblacklist option to the line in /etc/grub.d/10_linux that describes your kernel. To blacklist the driver when the root device is mounted, add a blacklist entry in a file under /etc/modprobe.d/.

1. Boot the system into rescue mode with the command linux rescue rdblacklist=name_of_driver, where name_of_driver is the driver that you need to blacklist. Follow the instructions in Section 19.1.2, "Booting into Rescue Mode" and do not choose to mount the installed system as read only.

2. Open the /mnt/sysimage/etc/grub.d/10_linux file with the vi text editor:

   vi /mnt/sysimage/etc/grub.d/10_linux

3. Identify the default kernel used to boot the system. Each kernel is specified in the 10Linux file with a group of lines that begins menuentry. The default kernel is specified by the default parameter in /etc/default/grub. A value of 0 refers to the first menu entry in the custom script files in /etc/grub.d, a value of 1 refers to the second menu entry, and higher values refer to subsequent kernels in turn. Check the script prior to 10_linux, named 00_header, to ensure you specify the correct kernel.

4. Edit the linux line of the menu entry to include the option rdblacklist=name_of_driver, where name_of_driver is the driver that you need to blacklist. For example, to blacklist the driver named foobar:

   linux /vmlinuz-2.6.32-71.18-2.el6.i686 ro root=/dev/sda1 rhgb quiet rdblacklist=foob

5. Save the file and exit vi.

6. Create a new file under /etc/modprobe.d/ that contains the command blacklist name_of_driver. Give the file a descriptive name that will help you find it in future, and use the
filename extension `.conf`. For example, to continue to blacklist the driver `foobar` when the root device is mounted, run:

```bash
echo "blacklist foobar" >> /mnt/sysimage/etc/modprobe.d/blacklist-foobar.conf
```

7. Reboot the system. You no longer need to supply `rdbblacklist` manually as a kernel option until you next update the default kernel. If you update the default kernel before the problem with the driver has been fixed, you must edit `16_linux` again to ensure that the faulty driver is not loaded at boot time.
Upgrading Your Current System

This chapter explains the various methods available for upgrading your Fedora system.

20.1. Determining Whether to Upgrade or Re-Install

Before upgrading to Fedora 17 you should first bring your current version up to date. However, it is not then necessary to upgrade to intermediate versions. For example, you can upgrade from Fedora 14 to Fedora 17 directly.

*This recommended reinstallation method helps to ensure the best system stability possible.*

If you currently use Fedora 16, you can perform a traditional, installation program-based upgrade.

However, before you chose to upgrade your system, there are a few things you should keep in mind:

- Individual package configuration files may or may not work after performing an upgrade due to changes in various configuration file formats or layouts.
- Third party or ISV applications may not work correctly following the upgrade.
- If you have additional third-party package repositories (such as *rpmfusion*) enabled, note that software installed from those repositories may not function properly after a system upgrade. Fedora does not maintain third-party packages and cannot guarantee that such repositories are up-to-date.

Upgrading your system installs updated versions of the packages which are currently installed on your system.

The upgrade process preserves existing configuration files by renaming them with an .rpmsave extension (for example, *sendmail.cf.rpmsave*). The upgrade process also creates a log of its actions in */root/upgrade.log*.

**Warning**

As software evolves, configuration file formats can change. It is very important to carefully compare your original configuration files to the new files before integrating your changes.

**Note**

It is always a good idea to back up any data that you have on your systems. For example, if you are upgrading or creating a dual-boot system, you should back up any data you wish to keep on your hard drive(s). Mistakes do happen and can result in the loss of all of your data.

Some upgraded packages may require the installation of other packages for proper operation. If you choose to customize your packages to upgrade, you may be required to resolve dependency problems. Otherwise, the upgrade procedure takes care of these dependencies, but it may need to install additional packages which are not on your system.
Depending on how you have partitioned your system, the upgrade program may prompt you to add an additional swap file. If the upgrade program does not detect a swap file that equals twice your RAM, it asks you if you would like to add a new swap file. If your system does not have a lot of RAM (less than 256 MB), it is recommended that you add this swap file.

20.2. Upgrading Your System

In most cases, the simplest way to upgrade an existing Fedora installation is with the preupgrade tool. When a new version of Fedora is available, preupgrade downloads the packages necessary to upgrade your installation, and initiates the upgrade process.

Install preupgrade with your graphical package manager, or type yum install preupgrade at the command line and press Enter.

To run preupgrade, type preupgrade at the command line and press Enter.

You can also upgrade a Fedora installation by starting the installation process by any of the methods described in Chapter 9, Installing using anaconda. If the installer detects a previous Fedora installation on the system, it will ask you whether you want to upgrade that installation — refer to Section 9.11.1, “The Upgrade Dialog”

The Upgrade Examine screen appears if you have instructed the installation program to perform an upgrade.

Note

If the contents of your /etc/fedora-release file have been changed from the default, your Fedora installation may not be found when attempting an upgrade to Fedora 17.

You can relax some of the checks against this file by booting with the following boot command:

    linux upgradeany

Use the linux upgradeany command if your Fedora installation was not given as an option to upgrade.

To perform an upgrade, select Perform an upgrade of an existing installation. Click Next when you are ready to begin your upgrade.

To re-install your system, select Perform a new Fedora installation and refer to Chapter 9, Installing using anaconda for further instructions.
Removing Fedora

We respect your freedom to choose an operating system for your computer. This section explains how to uninstall Fedora.

⚠️ These instructions may destroy data!

If you have data from Fedora that you want to keep, back it up before you proceed. Write your data to CD, DVD, external hard disk, or other storage device.

As a precaution, also back up data from any other operating systems that are installed on the same computer. Mistakes do happen and can result in the loss of all your data.

If you back up data from Fedora to be used later in another operating system, make sure that the storage medium or device is readable by that other operating system. For example, without extra third-party software, Microsoft Windows cannot read an external hard drive that you have formatted with Fedora to use the ext2, ext3, or ext4 file system.

To uninstall Fedora from your x86-based system, you must remove the Fedora boot loader information from your master boot record (MBR) and remove any partitions that contain the operating system. The method for removing Fedora from your computer varies, depending on whether Fedora is the only operating system installed on the computer, or whether the computer is configured to dual-boot Fedora and another operating system.

These instructions cannot cover every possible computer configuration. If your computer is configured to boot three or more operating systems, or has a highly-customized partition scheme, use the following sections as a general guide to partition removal with the various tools described. In these situations, you will also need to learn to configure your chosen bootloader. See Appendix E, The GRUB Boot Loader for a general introduction to the subject, but detailed instructions are beyond the scope of this document.

Legacy versions of Microsoft operating systems

**Fdisk**, the disk partitioning tool provided with MS-DOS and Microsoft Windows, is unable to remove the file systems used by Fedora. MS-DOS and versions of Windows prior to Windows XP (except for Windows 2000) have no other means of removing or modifying partitions. Refer to Section 21.3, "Replacing Fedora with MS-DOS or legacy versions of Microsoft Windows" for alternative removal methods for use with MS-DOS and these versions of Windows.

21.1. Fedora is the only operating system on the computer

If Fedora is the only operating system on your computer, use the installation media for the replacement operating system to remove Fedora. Examples of installation media include the Windows XP installation CD, Windows Vista installation DVD, or the installation CD, CDs, or DVD of another Linux distribution.

Note that some manufacturers of factory-built computers pre-installed with Microsoft Windows do not supply the Windows installation CD or DVD with the computer. The manufacturer may instead have
supplied their own “system restore disk”, or have included software with the computer that allowed you to create your own “system restore disk” when you first started the computer. In some cases, the system restore software is stored on a separate partition on the system’s hard drive. If you cannot identify the installation media for an operating system that was pre-installed on your computer, consult the documentation supplied with the machine, or contact the manufacturer.

When you have located the installation media for your chosen operating system:

1. Back up any data that you want to keep.

2. Shut down the computer.

3. Boot your computer with the installation disk for the replacement operating system.

4. Follow the prompts presented during the installation process. Windows, OS X, and most Linux installation disks allow you to manually partition your hard drive during the installation process, or will offer you the option to remove all partitions and start with a fresh partition scheme. At this point, remove any existing partitions that the installation software detects or allow the installer to remove the partitions automatically. “System restore” media for computers pre-installed with Microsoft Windows might create a default partition layout automatically without input from you.

**Warning**

If your computer has system restore software stored on a partition on a hard drive, take care when removing partitions while installing an operating system from other media. Under these circumstances, you could destroy the partition holding the system restore software.

### 21.2. Your computer dual-boots Fedora and another operating system

If your computer is configured to dual-boot Fedora and another operating system, removing Fedora without removing the partitions containing the other operating system and its data is more complicated. Specific instructions for a number of operating systems are set out below. To keep neither Fedora nor the other operating system, follow the steps described for a computer with only Fedora installed: Section 21.1, “Fedora is the only operating system on the computer”
21.2.1. Your computer dual-boots Fedora and a Microsoft Windows operating system


**Warning**

Once you commence this process, your computer may be left in an unbootable state until you complete the entire set of instructions. Carefully read the steps below before beginning the removal process. Consider opening these instructions on another computer or printing them so that you have access to them at all times during the process.

This procedure relies on the Windows Recovery Console that loads from the Windows installation disk, so you will not be able to complete the procedure without access to this disk. If you start this procedure and do not complete it, you could leave your computer in a condition where you cannot boot it. The "system restore disk" supplied with some factory-built computers that are sold with Windows pre-installed on them might not include the Windows Recovery Console.

During the process outlined in these instructions, the Windows Recovery Console will prompt you for the Administrator password for your Windows system. Do not follow these instructions unless you know the Administrator password for your system or are certain that an Administrator password has never been created, even by the computer manufacturer.

1. Remove the Fedora partitions
   a. Boot your computer into your Microsoft Windows environment.
   b. Click **Start**>**Run**, type `diskmgmt.msc` and press **Enter**. The Disk Management tool opens.
      The tool displays a graphical representation of your disk, with bars representing each partition. The first partition is usually labeled **NTFS** and corresponds to your **C:** drive. At least two Fedora partitions will be visible. Windows will not display a file system type for these partitions, but may allocate drive letters to some of them.
   c. Right-click on one of the Fedora partitions, then click **Delete Partition** and click **Yes** to confirm the deletion. Repeat this process for the other Fedora partitions on your system. As you delete partitions, Windows labels the space on the hard drive previously occupied by those partitions as **unallocated**.

2. Enable Windows to use the space on your hard drive vacated by Fedora (optional)
This step is not required to remove Fedora from your computer. However, if you skip this step, you will leave part of your hard drive’s storage capacity unusable by Windows. Depending on your configuration, this might be a significant portion of the storage capacity of the drive.

Decide whether to extend an existing Windows partition to use the extra space, or create a new Windows partition in that space. If you create a new Windows partition, Windows will allocate a new drive letter to it and will interact with it as if it is a separate hard drive.

**Extending an existing Windows partition**

- Click **Start>Run...**, type `diskpart` and press `Enter`. A command window appears.
- Type `list volume` and press `Enter`. `Diskpart` displays a list of the partitions on your system with a volume number, its drive letter, volume label, filesystem type, and size. Identify the Windows partition that you would like to use to occupy the space vacated on your hard drive by Fedora and take note of its volume number (for example, your Windows C: drive might be "Volume 0").
- Type `select volume N` (where `N` is the volume number for the Windows partition that you want to extend) and press `Enter`. Now type `extend` and press `Enter`. `Diskpart` now extends your chosen partition to fill the remaining space on your hard drive. It will notify you when the operation is complete.

**Adding a new Windows partition**

- In the **Disk Management** window, right-click on disk space that Windows labels as `unallocated` and select **New Partition** from the menu. The **New Partition Wizard** starts.
- Follow the prompts presented by the **New Partition Wizard**. If you accept the default options, the tool will create a new partition that fills all available space on the hard drive, assigns it the next available drive letter, and formats it with the NTFS file system.

3. **Restore the Windows bootloader**

- Insert the Windows installation disk and restart your computer. As your computer starts, the following message will appear on the screen for a few seconds:

```
Press any key to boot from CD
```
Your computer dual-boots Fedora and a Microsoft Windows operating system.

Press any key while the message is still showing and the Windows installation software will load.

b. When the Welcome to Setup screen appears, you can start the Windows Recovery Console. The procedure is slightly different on different versions of Windows:
   - On Windows 2000 and Windows Server 2000, press the R key, then the C key.

c. The Windows Recovery Console scans your hard drives for Windows installations, and assigns a number to each one. It displays a list of Windows installations and prompts you to select one. Type the number corresponding to the Windows installation that you want to restore.

d. The Windows Recovery Console prompts you for the Administrator password for your Windows installation. Type the Administrator password and press the Enter key. If there is no administrator password for this system, press only the Enter key.

e. At the prompt, type the command `fixmbr` and press the Enter. The `fixmbr` tool now restores the Master Boot Record for the system.

f. When the prompt reappears, type `exit` and press the Enter key.

g. Your computer will restart and boot your Windows operating system.

21.2.1.2. Windows Vista and Windows Server 2008

⚠️ Warning

Once you commence this process, your computer may be left in an unbootable state until you complete the entire set of instructions. Carefully read the steps below before beginning the removal process. Consider opening these instructions on another computer or printing them so that you have access to them at all times during the process.

This procedure relies on the Windows Recovery Environment that loads from the Windows installation disk and you will not be able to complete the procedure without access to this disk. If you start this procedure and do not complete it, you could leave your computer in a condition where you cannot boot it. The "system restore disk" supplied with some factory-built computers that are sold with Windows pre-installed on them might not include the Windows Recovery Environment.

1. Remove the Fedora partitions
   a. Boot your computer into your Microsoft Windows environment.
   b. Click Start then type `diskmgmt.msc` into the Start Search box and press Enter. The Disk Management tool opens.

   The tool displays a graphical representation of your disk, with bars representing each partition. The first partition is usually labeled NTFS and corresponds to your C: drive. At least two
Chapter 21. Removing Fedora

Fedora partitions will be visible. Windows will not display a file system type for these partitions, but may allocate drive letters to some of them.

c. Right-click on one of the Fedora partitions, then click Delete Partition and click Yes to confirm the deletion. Repeat this process for the other Fedora partitions on your system. As you delete partitions, Windows labels the space on the hard drive previously occupied by those partitions as unallocated.

2. Enable Windows to use the space on your hard drive vacated by Fedora (optional)

Note

This step is not required to remove Fedora from your computer. However, if you skip this step, you will leave part of your hard drive’s storage capacity unusable by Windows. Depending on your configuration, this might be a significant portion of the storage capacity of the drive.

Decide whether to extend an existing Windows partition to use the extra space, or create a new Windows partition in that space. If you create a new Windows partition, Windows will allocate a new drive letter to it and will interact with it as if it is a separate hard drive.

Extending an existing Windows partition
a. In the Disk Management window, right-click on the Windows partition that you want to extend and select Extend Volume from the menu. The Extend Volume Wizard opens.

b. Follow the prompts presented by the Extend Volume Wizard. If you accept the defaults that it offers you, the tool will extend the selected volume to fill all available space on the hard drive.

Adding a new Windows partition
a. In the Disk Management window, right-click on disk space that Windows labels as unallocated and select New Simple Volume from the menu. The New Simple Volume Wizard starts.

b. Follow the prompts presented by the New Simple Volume Wizard. If you accept the default options, the tool will create a new partition that fills all available space on the hard drive, assigns it the next available drive letter, and formats it with the NTFS file system.

3. Restore the Windows bootloader
a. Insert the Windows installation disk and restart your computer. As your computer starts, the following message will appear on the screen for a few seconds:

   Press any key to boot from CD or DVD

   Press any key while the message is still showing and the Windows installation software will load.

b. In the Install Windows dialog, select a language, time and currency format, and keyboard type. Click Next

c. Click Repair your computer.
d. The Windows Recovery Environment (WRE) shows you the Windows installations that it can detect on your system. Select the installation that you want to restore, then click Next.

e. Click Command prompt. A command window will open.

f. Type `bootrec /fixmbr` and press Enter.

g. When the prompt reappears, close the command window, then click Restart.

h. Your computer will restart and boot your Windows operating system.

**21.2.2. Your computer dual-boots Fedora and Mac OS X**

The procedure to remove Fedora from a system that dual-boots Fedora and Mac OS X varies depending on whether you have installed Boot Camp on your computer:

**You are not using Boot Camp on your computer**

1. Open the Disk Utility in `/Applications/Utilities`.

2. Select the entry on the left for the disk volume containing Fedora.

3. Click the Partition tab on the right side of the dialog.

4. Select the Fedora partitions and click the minus button below the partition layout diagram.

5. Resize your OS X partition to include the newly freed space.

**You are using Boot Camp on your computer**

1. Open the Boot Camp Assistant in `/Applications/Utilities`.

2. Select Create or remove a Windows partition and click Next.

3. If your computer has a single internal disk, click Restore.

4. If your computer has multiple internal disks, select the Linux disk, and then select Restore to a single Mac OS partition. Click Continue.

**21.2.3. Your computer dual-boots Fedora and a different Linux distribution**

Because of the differences between the many different Linux distributions, these instructions are a general guide only. Specific details vary according to the configuration of your particular system and the Linux distribution that dual-boots with Fedora.

1. Procedure 21.1. Remove Fedora partitions

   1. Boot your Fedora installation.

   2. As root or with `sudo`, run `mount`. Note the partitions that are mounted. In particular, note the partition that is mounted as the root of the filesystem. The output of `mount` on a system where the root of the filesystem is on a standard partition such as `/dev/sda2` might resemble:

```
/dev/sda2 on / type ext4 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:object_r:tmpfs_t:s0")
/dev/sda1 on /boot type ext4 (rw)
```
# Chapter 21. Removing Fedora

| none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw) |
| sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw) |

The output of `mount` on a system where the root of the filesystem is on a logical volume might resemble:

| /dev/mapper/VolGroup00-LogVol00 on / type ext4 (rw) |
| proc on /proc type proc (rw) |
| sysfs on /sys type sysfs (rw) |
| devpts on /dev/pts type devpts (rw,gid=5,mode=620) |
| tmpfs on /dev/shm type tmpfs (rw,rootcontext="system_u:object_r:tmpfs_t:s0") |
| /dev/sda1 on /boot type ext4 (rw) |
| none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw) |
| sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw) |

3. Ensure that any data on this system that you still require is backed up to another system or storage location.

4. Shut down the system and boot the Linux distribution that you want to keep on the system.

5. As root or with `sudo`, run `mount`. If any of the partitions that you previously noted as used for Fedora are mounted, review the contents of these partitions. If you no longer require the contents of these partitions, unmount them with the `umount` command.

6. Remove any unwanted and unnecessary partitions, for example, with `fdisk` for standard partitions, or `lvremove` and `vgremove` to remove logical volumes and volume groups.

2. **Remove Fedora entries from your bootloader**

## Example only

These instructions assume that your system uses the **GRUB** bootloader. If you use a different bootloader (such as **LILO**) consult the documentation for that software to identify and remove Fedora entries from its list of boot targets and to ensure that your default operating system is correctly specified.

a. At the command line, type `su` - and press **Enter**. When the system prompts you for the root password, type the password and press **Enter**.

b. Type `gedit /etc/grub.d/10_linux` and press **Enter**. This opens the **10_linux** file in the **gedit** text editor.

c. A typical Fedora entry in the **10_linux** file consists of four lines:

```plaintext
Example 21.1. Example Fedora entry in **10_linux**

menuentry "Fedora (2.6.32.130.el6.i686)"

set root=(hd0,1)

linux /vmlinuz-2.6.32.130.el6.i686 ro root=UUID=04a07c13-e6bf-6d5a-b207-002689545705 rhgb quiet

initrd /initrd-2.6.32.130.el6.i686.img
```
Depending on the configuration of your system, there may be multiple Fedora entries in
10_linux, each corresponding to a different version of the Linux kernel. Delete each of the
Fedora entries from these files.

Save the updated 10_linux file and close gedit.

d. Type gedit etc/default/grub and press Enter.

e. The file etc/default/grub contains a line that specifies the default operating system to
boot, in the format default=\textit{N} where \textit{N} is a number equal to or greater than 0. If \textit{N} is set to
0, GRUB will boot the first operating system in the list. If \textit{N} is set to 1, it will boot the second
operating system, and so forth. Alternatively, the default value can be the full menu entry.

Identify the entry for the operating system that you want GRUB to boot by default and note its
place in the order within the list.

Make sure that the default= line contains the number \textit{one below} the number of your chosen
default operating system in the list.

Save the updated grub file and close gedit. If you have Fedora entries in the other script files
in the /etc/grub.d directory, use this procedure to remove them in the same way.

3. Make space available to your operating system

\begin{itemize}
\item \textbf{If you do not use LVM}
\begin{itemize}
\item Boot your computer from Linux live media, and install \texttt{parted} if it is not already present.
\item As root or with \texttt{sudo}, run \texttt{parted disk}, where \texttt{disk} is the device name of the disk that
contains a partition that you want to resize, for example, /dev/sda.
\end{itemize}
\end{itemize}
c. At the `parted` prompt, enter `print`. The `parted` tool displays information about the partitions on your system, including their partition numbers, their sizes, and their positions on the disk.

d. At the `parted` prompt, enter `resize number start end`, where `number` is the partition number, `start` is the location on the disk at which the partition begins, and `end` is the location on the disk at which you want the partition to end. Use the start position that you previously obtained with the `print` command, and refer to the `parted` documentation for different ways to specify the end parameter.

e. When `parted` finishes resizing the partition, enter `quit` at the `parted` prompt.

f. Run `e2fsck partition`, where `partition` is the partition that you just resized. For example, if you just resized `/dev/sda3`, enter `e2fsck /dev/sda3`.

Linux now checks the file system of the newly-resized partition.

g. When the file system check finishes, type `resize2fs partition` at a command line and press `Enter`, where `partition` is the partition that you just resized. For example, if you just resized `/dev/sda3`, type `resize2fs /dev/sda3`.

Linux now resizes your file system to fill the newly-resized partition.

h. Restart your computer. The extra space is now available to your Linux installation.

• If you use LVM

  a. Boot your computer from Linux live media and install `fdisk` and `lvm2` if they are not already present.

  b. Create a new partition in the free space on the disk

    i. As root or with `sudo`, run `fdisk disk`, where `disk` is the device name of the disk where you want to create new space, for example, `/dev/sda`.

    ii. At the prompt `Command (m for help):`, enter `n` to create a new partition. Refer to the `fdisk` documentation for options.

  c. Change the partition type identifier

    i. At the prompt `Command (m for help):`, enter `t` to change a partition type.

    ii. At the prompt `Partition number (1-4):`, type the number of the partition that you just created. For example, if you just created partition `/dev/sda3`, type the number `3` and press `Enter`. This identifies the partition whose type `fdisk` will change.

    iii. At the prompt `Hex code (type L to list codes):`, enter `8e` to create a Linux LVM partition.

    iv. At the prompt `Command (m for help):`, enter `w` to write the changes to disk and exit `fdisk`.

  d. Expand the volume group

    i. At the command prompt, type `lvm` and press `Enter` to start the `lvm2` tool.

    ii. At the `lvm>` prompt, type `pvcreate partition` and press `Enter`, where `partition` is the partition that you recently created. For example, `pvcreate /dev/sda3`. This creates `/dev/sda3` as a physical volume in LVM.
Replacing Fedora with MS-DOS or legacy versions of Microsoft Windows

iii. At the `lvm>` prompt, type `vgextend VolumeGroup partition` and press `Enter`, where `VolumeGroup` is the LVM volume group on which Linux is installed and `partition` is the partition that you recently created. For example, if Linux is installed on `/dev/VolumeGroup00`, you would type `vgextend /dev/VolumeGroup00 /dev/sda3` to extend that volume group to include the physical volume at `/dev/sda3`.

iv. At the `lvm>` prompt, type `lvextend -l +100%FREE LogVol` and press `Enter`, where `LogVol` is the logical volume that contains your Linux filesystem. For example, to extend `LogVol00` to fill the newly-available space in its volume group, `VolGroup00`, type `lvextend -l +100%FREE /dev/VolGroup00/LogVol00`.

v. At the `lvm>` prompt, type `exit` and press `Enter` to exit `lvm2`.

vi. Type `e2fsck LogVol` at the command line and press `Enter`, where `LogVol` is the logical volume that you just resized. For example, if you just resized `/dev/VolumeGroup00/LogVol00`, you would type `e2fsck /dev/VolumeGroup00/LogVol00`.

Linux now checks the file system of the newly-resized logical volume.

e. When the file system check finishes, type `resize2fs LogVol` at a command line and press `Enter`, where `LogVol` is the partition that you just resized. For example, if you just resized `/dev/VolumeGroup00/LogVol00`, you would type `resize2fs /dev/VolumeGroup00/LogVol00`.

Linux now resizes your file system to fill the newly-resized logical volume.

f. Restart your computer. The extra space is now available to your Linux installation.

21.3. Replacing Fedora with MS-DOS or legacy versions of Microsoft Windows

In DOS and Windows, use the Windows `fdisk` utility to create a new MBR with the *undocumented* flag `/mbr`. This ONLY rewrites the MBR to boot the primary DOS partition. The command should look like the following:

```
fdisk /mbr
```

If you need to remove Linux from a hard drive and have attempted to do this with the default DOS (Windows) `fdisk`, you will experience the *Partitions exist but they do not exist* problem. The best way to remove non-DOS partitions is with a tool that understands partitions other than DOS.

To begin, insert the Fedora DVD and boot your system. When the boot prompt appears, type: `linux rescue`. This starts the rescue mode program.

You are prompted for your keyboard and language requirements. Enter these values as you would during the installation of Fedora.

Next, a screen appears telling you that the program attempts to find a Fedora install to rescue. Select `Skip` on this screen.

After selecting `Skip`, you are given a command prompt where you can access the partitions you would like to remove.

First, type the command `list-harddrives`. This command lists all hard drives on your system that are recognizable by the installation program, as well as their sizes in megabytes.
Warning

Be careful to remove only the necessary Fedora partitions. Removing other partitions could result in data loss or a corrupted system environment.

To remove partitions, use the partitioning utility `parted`. Start `parted`, where `/dev/hda` is the device on which to remove the partition:

```
parted /dev/hda
```

Using the `print` command, view the current partition table to determine the minor number of the partition to remove:

```
print
```

The `print` command also displays the partition's type (such as linux-swap, ext2, ext3, ext4 and so on). Knowing the type of the partition helps you in determining whether to remove the partition.

Remove the partition with the command `rm`. For example, to remove the partition with minor number 3:

```
rm 3
```

Important

The changes start taking place as soon as you press [Enter], so review the command before committing to it.

After removing the partition, use the `print` command to confirm that it is removed from the partition table.

Once you have removed the Linux partitions and made all of the changes you need to make, type `quit` to quit `parted`.

After quitting `parted`, type `exit` at the boot prompt to exit rescue mode and reboot your system, instead of continuing with the installation. The system should reboot automatically. If it does not, you can reboot your computer using `Control+Alt+Delete`.
Part IV. Technical appendixes

The appendixes in this section do not contain instructions that tell you how to install Fedora. Instead, they provide technical background that you might find helpful to understand the options that Fedora offers you at various points in the installation process.
Appendix A. An Introduction to Disk Partitions

Note

This appendix is not necessarily applicable to non-x86-based architectures. However, the general concepts mentioned here may apply.

This appendix is not necessarily applicable to non-x86-based architectures. However, the general concepts mentioned here may apply.

If you are reasonably comfortable with disk partitions, you could skip ahead to Section A.1.4, “Making Room For Fedora”, for more information on the process of freeing up disk space to prepare for a Fedora installation. This section also discusses the partition naming scheme used by Linux systems, sharing disk space with other operating systems, and related topics.

A.1. Hard Disk Basic Concepts

Hard disks perform a very simple function — they store data and reliably retrieve it on command.

When discussing issues such as disk partitioning, it is important to know a bit about the underlying hardware. Unfortunately, it is easy to become bogged down in details. Therefore, this appendix uses a simplified diagram of a disk drive to help explain what is really happening when a disk drive is partitioned. Figure A.1, “An Unused Disk Drive”, shows a brand-new, unused disk drive.

Figure A.1. An Unused Disk Drive

Not much to look at, is it? But if we are talking about disk drives on a basic level, it is adequate. Say that we would like to store some data on this drive. As things stand now, it will not work. There is something we need to do first.

A.1.1. It is Not What You Write, it is How You Write It

Experienced computer users probably got this one on the first try. We need to format the drive. Formatting (usually known as "making a file system") writes information to the drive, creating order out of the empty space in an unformatted drive.
Appendix A. An Introduction to Disk Partitions

Figure A.2. Disk Drive with a File System

As Figure A.2, “Disk Drive with a File System”, implies, the order imposed by a file system involves some trade-offs:

• A small percentage of the drive’s available space is used to store file system-related data and can be considered as overhead.

• A file system splits the remaining space into small, consistently-sized segments. For Linux, these segments are known as *blocks*. ¹

Given that file systems make things like directories and files possible, these trade-offs are usually seen as a small price to pay.

It is also worth noting that there is no single, universal file system. As Figure A.3, “Disk Drive with a Different File System”, shows, a disk drive may have one of many different file systems written on it. As you might guess, different file systems tend to be incompatible; that is, an operating system that supports one file system (or a handful of related file system types) may not support another. This last statement is not a hard-and-fast rule, however. For example, Fedora supports a wide variety of file systems (including many commonly used by other operating systems), making data interchange between different file systems easy.

Figure A.3. Disk Drive with a Different File System

Of course, writing a file system to disk is only the beginning. The goal of this process is to actually store and retrieve data. Let us take a look at our drive after some files have been written to it.

Figure A.4. Disk Drive with Data Written to It

As Figure A.4, “Disk Drive with Data Written to It”, shows, some of the previously-empty blocks are now holding data. However, by just looking at this picture, we cannot determine exactly how many files reside on this drive. There may only be one file or many, as all files use at least one block and some

¹ Blocks really are consistently sized, unlike our illustrations. Keep in mind, also, that an average disk drive contains thousands of blocks. But for the purposes of this discussion, please ignore these minor discrepancies.
files use multiple blocks. Another important point to note is that the used blocks do not have to form a contiguous region; used and unused blocks may be interspersed. This is known as *fragmentation*. Fragmentation can play a part when attempting to resize an existing partition.

As with most computer-related technologies, disk drives changed over time after their introduction. In particular, they got bigger. Not larger in physical size, but bigger in their capacity to store information. And, this additional capacity drove a fundamental change in the way disk drives were used.

### A.1.2. Partitions: Turning One Drive Into Many

As disk drive capacities soared, some people began to wonder if having all of that formatted space in one big chunk was such a great idea. This line of thinking was driven by several issues, some philosophical, some technical. On the philosophical side, above a certain size, it seemed that the additional space provided by a larger drive created more clutter. On the technical side, some file systems were never designed to support anything above a certain capacity. Or the file systems *could* support larger drives with a greater capacity, but the overhead imposed by the file system to track files became excessive.

The solution to this problem was to divide disks into *partitions*. Each partition can be accessed as if it was a separate disk. This is done through the addition of a *partition table*.

#### Note

While the diagrams in this chapter show the partition table as being separate from the actual disk drive, this is not entirely accurate. In reality, the partition table is stored at the very start of the disk, before any file system or user data. But for clarity, they are separate in our diagrams.

![Figure A.5. Disk Drive with Partition Table](image)

As *Figure A.5, “Disk Drive with Partition Table”* shows, the partition table is divided into four sections or four *primary* partitions. A primary partition is a partition on a hard drive that can contain only one logical drive (or section). Each section can hold the information necessary to define a single partition, meaning that the partition table can define no more than four partitions.

Each partition table entry contains several important characteristics of the partition:

- The points on the disk where the partition starts and ends
- Whether the partition is "active"
- The partition's type

Let us take a closer look at each of these characteristics. The starting and ending points actually define the partition's size and location on the disk. The "active" flag is used by some operating
systems’ boot loaders. In other words, the operating system in the partition that is marked “active” is booted.

The partition’s type can be a bit confusing. The type is a number that identifies the partition’s anticipated usage. If that statement sounds a bit vague, that is because the meaning of the partition type is a bit vague. Some operating systems use the partition type to denote a specific file system type, to flag the partition as being associated with a particular operating system, to indicate that the partition contains a bootable operating system, or some combination of the three.

By this point, you might be wondering how all this additional complexity is normally used. Refer to Figure A.6, “Disk Drive With Single Partition”, for an example.

In many cases, there is only a single partition spanning the entire disk, essentially duplicating the method used before partitions. The partition table has only one entry used, and it points to the start of the partition.

We have labeled this partition as being of the “DOS” type. Although it is only one of several possible partition types listed in Table A.1, “Partition Types”, it is adequate for the purposes of this discussion.

Table A.1, “Partition Types”, contains a listing of some popular (and obscure) partition types, along with their hexadecimal numeric values.

<table>
<thead>
<tr>
<th>Partition Type</th>
<th>Value</th>
<th>Partition Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Empty</td>
<td>00</td>
<td>Novell Netware 386</td>
<td>65</td>
</tr>
<tr>
<td>DOS 12-bit FAT</td>
<td>01</td>
<td>PIC/IX</td>
<td>75</td>
</tr>
<tr>
<td>XENIX root</td>
<td>02</td>
<td>Old MINIX</td>
<td>80</td>
</tr>
<tr>
<td>XENIX usr</td>
<td>03</td>
<td>Linux/MINIX</td>
<td>81</td>
</tr>
<tr>
<td>DOS 16-bit &lt;=32M</td>
<td>04</td>
<td>Linux swap</td>
<td>82</td>
</tr>
<tr>
<td>Extended</td>
<td>05</td>
<td>Linux native</td>
<td>83</td>
</tr>
<tr>
<td>DOS 16-bit &gt;=32</td>
<td>06</td>
<td>Linux extended</td>
<td>85</td>
</tr>
<tr>
<td>OS/2 HPFS</td>
<td>07</td>
<td>Amoeba</td>
<td>93</td>
</tr>
<tr>
<td>AIX</td>
<td>08</td>
<td>Amoeba BBT</td>
<td>94</td>
</tr>
<tr>
<td>AIX bootable</td>
<td>09</td>
<td>BSD/386</td>
<td>a5</td>
</tr>
<tr>
<td>OS/2 Boot Manager</td>
<td>0a</td>
<td>OpenBSD</td>
<td>a6</td>
</tr>
<tr>
<td>Win95 FAT32</td>
<td>0b</td>
<td>NEXTSTEP</td>
<td>a7</td>
</tr>
<tr>
<td>Win95 FAT32 (LBA)</td>
<td>0c</td>
<td>BSDI fs</td>
<td>b7</td>
</tr>
<tr>
<td>Win95 FAT16 (LBA)</td>
<td>0e</td>
<td>BSDI swap</td>
<td>b8</td>
</tr>
<tr>
<td>Win95 Extended (LBA)</td>
<td>0f</td>
<td>Syrinx</td>
<td>c7</td>
</tr>
</tbody>
</table>
A.1.3. Partitions within Partitions — An Overview of Extended Partitions

Of course, over time it became obvious that four partitions would not be enough. As disk drives continued to grow, it became more and more likely that a person could configure four reasonably-sized partitions and still have disk space left over. There needed to be some way of creating more partitions.

Enter the extended partition. As you may have noticed in *Table A.1, “Partition Types”*, there is an “Extended” partition type. It is this partition type that is at the heart of extended partitions.

When a partition is created and its type is set to “Extended,” an extended partition table is created. In essence, the extended partition is like a disk drive in its own right — it has a partition table that points to one or more partitions (now called logical partitions, as opposed to the four primary partitions) contained entirely within the extended partition itself. *Figure A.7, “Disk Drive With Extended Partition”*, shows a disk drive with one primary partition and one extended partition containing two logical partitions (along with some unpartitioned free space).

![Figure A.7. Disk Drive With Extended Partition](image)

As this figure implies, there is a difference between primary and logical partitions — there can only be four primary partitions, but there is no fixed limit to the number of logical partitions that can exist. However, due to the way in which partitions are accessed in Linux, you should avoid defining more than 12 logical partitions on a single disk drive.

Now that we have discussed partitions in general, let us review how to use this knowledge to install Fedora.

A.1.4. Making Room For Fedora

---

<table>
<thead>
<tr>
<th>Partition Type</th>
<th>Value</th>
<th>Partition Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Venix 80286</td>
<td>40</td>
<td>CP/M</td>
<td>db</td>
</tr>
<tr>
<td>Novell</td>
<td>51</td>
<td>DOS access</td>
<td>e1</td>
</tr>
<tr>
<td>PReP Boot</td>
<td>41</td>
<td>DOS R/O</td>
<td>e3</td>
</tr>
<tr>
<td>GNU HURD</td>
<td>63</td>
<td>DOS secondary</td>
<td>f2</td>
</tr>
<tr>
<td>Novell Netware 286</td>
<td>64</td>
<td>BBT</td>
<td>ff</td>
</tr>
</tbody>
</table>
The following list presents some possible scenarios you may face when attempting to repartition your hard disk:

- Unpartitioned free space is available
- An unused partition is available
- Free space in an actively used partition is available

Let us look at each scenario in order.

**Note**

Keep in mind that the following illustrations are simplified in the interest of clarity and do not reflect the exact partition layout that you encounter when actually installing Fedora.

### A.1.4.1. Using Unpartitioned Free Space

In this situation, the partitions already defined do not span the entire hard disk, leaving unallocated space that is not part of any defined partition. Figure A.8, “Disk Drive with Unpartitioned Free Space”, shows what this might look like.

![Figure A.8. Disk Drive with Unpartitioned Free Space](image)

In Figure A.8, “Disk Drive with Unpartitioned Free Space”, 1 represents an undefined partition with unallocated space and 2 represents a defined partition with allocated space.

If you think about it, an unused hard disk also falls into this category. The only difference is that all the space is not part of any defined partition.

In any case, you can create the necessary partitions from the unused space. Unfortunately, this scenario, although very simple, is not very likely (unless you have just purchased a new disk just for Fedora). Most pre-installed operating systems are configured to take up all available space on a disk drive (refer to Section A.1.4.3, “Using Free Space from an Active Partition”).

Next, we will discuss a slightly more common situation.

### A.1.4.2. Using Space from an Unused Partition

In this case, maybe you have one or more partitions that you do not use any longer. Perhaps you have dabbled with another operating system in the past, and the partition(s) you dedicated to it never seem to be used anymore. Figure A.9, “Disk Drive With an Unused Partition”, illustrates such a situation.
In Figure A.9, “Disk Drive With an Unused Partition”, 1 represents an unused partition and 2 represents reallocating an unused partition for Linux.

If you find yourself in this situation, you can use the space allocated to the unused partition. You first must delete the partition and then create the appropriate Linux partition(s) in its place. You can delete the unused partition and manually create new partitions during the installation process.

A.1.4.3. Using Free Space from an Active Partition

This is the most common situation. It is also, unfortunately, the hardest to handle. The main problem is that, even if you have enough free space, it is presently allocated to a partition that is already in use. If you purchased a computer with pre-installed software, the hard disk most likely has one massive partition holding the operating system and data.

Aside from adding a new hard drive to your system, you have two choices:

Destructive Repartitioning

Basically, you delete the single large partition and create several smaller ones. As you might imagine, any data you had in the original partition is destroyed. This means that making a complete backup is necessary. For your own sake, make two backups, use verification (if available in your backup software), and try to read data from your backup before you delete the partition.

Warning

If there was an operating system of some type installed on that partition, it needs to be reinstalled as well. Be aware that some computers sold with pre-installed operating systems may not include the CD-ROM media to reinstall the original operating system. The best time to notice if this applies to your system is before you destroy your original partition and its operating system installation.

After creating a smaller partition for your existing operating system, you can reinstall any software, restore your data, and start your Fedora installation. Figure A.10, “Disk Drive Being Destructively Repartitioned” shows this being done.
Appendix A. An Introduction to Disk Partitions

Figure A.10. Disk Drive Being Destructively Repartitioned

In Figure A.10, “Disk Drive Being Destructively Repartitioned”, 1 represents before and 2 represents after.

Warning

As Figure A.10, “Disk Drive Being Destructively Repartitioned”, shows, any data present in the original partition is lost without proper backup!

Non-Destructive Repartitioning

Here, you run a program that does the seemingly impossible: it makes a big partition smaller without losing any of the files stored in that partition. Many people have found this method to be reliable and trouble-free. What software should you use to perform this feat? There are several disk management software products on the market. Do some research to find the one that is best for your situation.

While the process of non-destructive repartitioning is rather straightforward, there are a number of steps involved:

- Compress and backup existing data
- Resize the existing partition
- Create new partition(s)

Next we will look at each step in a bit more detail.

A.1.4.3.1. Compress existing data

As Figure A.11, “Disk Drive Being Compressed”, shows, the first step is to compress the data in your existing partition. The reason for doing this is to rearrange the data such that it maximizes the available free space at the "end" of the partition.

Figure A.11. Disk Drive Being Compressed

In Figure A.11, “Disk Drive Being Compressed”, 1 represents before and 2 represents after.
This step is crucial. Without it, the location of your data could prevent the partition from being resized to the extent desired. Note also that, for one reason or another, some data cannot be moved. If this is the case (and it severely restricts the size of your new partition(s)), you may be forced to destructively repartition your disk.

A.1.4.3.2. Resize the existing partition

Figure A.12, "Disk Drive with Partition Resized", shows the actual resizing process. While the actual result of the resizing operation varies depending on the software used, in most cases the newly freed space is used to create an unformatted partition of the same type as the original partition.

In Figure A.12, "Disk Drive with Partition Resized", 1 represents before and 2 represents after.

It is important to understand what the resizing software you use does with the newly freed space, so that you can take the appropriate steps. In the case we have illustrated, it would be best to delete the new DOS partition and create the appropriate Linux partition(s).

A.1.4.3.3. Create new partition(s)

As the previous step implied, it may or may not be necessary to create new partitions. However, unless your resizing software is Linux-aware, it is likely that you must delete the partition that was created during the resizing process. Figure A.13, "Disk Drive with Final Partition Configuration", shows this being done.

In Figure A.13, "Disk Drive with Final Partition Configuration", 1 represents before and 2 represents after.

Note

The following information is specific to x86-based computers only.
As a convenience to our customers, we provide the \texttt{parted} utility. This is a freely available program that can resize partitions.

If you decide to repartition your hard drive with \texttt{parted}, it is important that you be familiar with disk storage and that you perform a backup of your computer data. You should make two copies of all the important data on your computer. These copies should be to removable media (such as tape, CD-ROM, or diskettes), and you should make sure they are readable before proceeding.

Should you decide to use \texttt{parted}, be aware that after \texttt{parted} runs you are left with two partitions: the one you resized, and the one \texttt{parted} created out of the newly freed space. If your goal is to use that space to install Fedora, you should delete the newly created partition, either by using the partitioning utility under your current operating system or while setting up partitions during installation.

\textbf{A.1.5. Partition Naming Scheme}

Linux refers to disk partitions using a combination of letters and numbers which may be confusing, particularly if you are used to the "C drive" way of referring to hard disks and their partitions. In the DOS/Windows world, partitions are named using the following method:

- Each partition's type is checked to determine if it can be read by DOS/Windows.
- If the partition's type is compatible, it is assigned a "drive letter." The drive letters start with a "C" and move on to the following letters, depending on the number of partitions to be labeled.
- The drive letter can then be used to refer to that partition as well as the file system contained on that partition.

Fedora uses a naming scheme that is more flexible and conveys more information than the approach used by other operating systems. The naming scheme is file-based, with file names in the form of \texttt{/dev/xxN}.

Here is how to decipher the partition naming scheme:

\texttt{/dev/}

This is the name of the directory in which all device files reside. Since partitions reside on hard disks, and hard disks are devices, the files representing all possible partitions reside in \texttt{/dev/}.

\texttt{xx}

The first two letters of the partition name indicate the type of device on which the partition resides, usually either \texttt{hd} (for IDE disks) or \texttt{sd} (for SCSI disks).

\texttt{y}

This letter indicates which device the partition is on. For example, \texttt{/dev/hda} (the first IDE hard disk) or \texttt{/dev/sdb} (the second SCSI disk).

\texttt{N}

The final number denotes the partition. The first four (primary or extended) partitions are numbered \texttt{1} through \texttt{4}. Logical partitions start at \texttt{5}. So, for example, \texttt{/dev/hda3} is the third primary or extended partition on the first IDE hard disk, and \texttt{/dev/sdb6} is the second logical partition on the second SCSI hard disk.
A.1.6. Disk Partitions and Other Operating Systems

If your Fedora partitions are sharing a hard disk with partitions used by other operating systems, most of the time you will have no problems. However, there are certain combinations of Linux and other operating systems that require extra care.

A.1.7. Disk Partitions and Mount Points

One area that many people new to Linux find confusing is the matter of how partitions are used and accessed by the Linux operating system. In DOS/Windows, it is relatively simple: Each partition gets a “drive letter.” You then use the correct drive letter to refer to files and directories on its corresponding partition.

This is entirely different from how Linux deals with partitions and, for that matter, with disk storage in general. The main difference is that each partition is used to form part of the storage necessary to support a single set of files and directories. This is done by associating a partition with a directory through a process known as mounting. Mounting a partition makes its storage available starting at the specified directory (known as a mount point).

For example, if partition /dev/hda5 is mounted on /usr/, that would mean that all files and directories under /usr/ physically reside on /dev/hda5. So the file /usr/share/doc/FAQ/faq/Linux-FAQ would be stored on /dev/hda5, while the file /etc/gdm/custom.conf would not.

Continuing our example, it is also possible that one or more directories below /usr/ would be mount points for other partitions. For instance, a partition (say, /dev/hda7) could be mounted on /usr/local/, meaning that /usr/local/man/whatis would then reside on /dev/hda7 rather than /dev/hda5.

A.1.8. How Many Partitions?

At this point in the process of preparing to install Fedora, you must give some consideration to the number and size of the partitions to be used by your new operating system. The question of “how many partitions” continues to spark debate within the Linux community and, without any end to the debate in sight, it is safe to say that there are probably as many partition layouts as there are people debating the issue.

Keeping this in mind, we recommend that, unless you have a reason for doing otherwise, you should at least create the following partitions: swap, /boot/, and / (root).
Appendix A. An Introduction to Disk Partitions

For more information, refer to Section 9.14.5, “Recommended Partitioning Scheme”.
Appendix B. ISCSI disks

Internet Small Computer System Interface (iSCSI) is a protocol that allows computers to communicate with storage devices by SCSI requests and responses carried over TCP/IP. Because iSCSI is based on the standard SCSI protocols, it uses some terminology from SCSI. The device on the SCSI bus to which requests get sent (and which answers these requests) is known as the target and the device issuing requests is known as the initiator. In other words, an iSCSI disk is a target and the iSCSI software equivalent of a SCSI controller or SCSI Host Bus Adapter (HBA) is called an initiator. This appendix only covers Linux as an iSCSI initiator: how Linux uses iSCSI disks, but not how Linux hosts iSCSI disks.

Linux has a software iSCSI initiator in the kernel that takes the place and form of a SCSI HBA driver and therefore allows Linux to use iSCSI disks. However, as iSCSI is a fully network-based protocol, iSCSI initiator support needs more than just the ability to send SCSI packets over the network. Before Linux can use an iSCSI target, Linux must find the target on the network and make a connection to it. In some cases, Linux must send authentication information to gain access to the target. Linux must also detect any failure of the network connection and must establish a new connection, including logging in again if necessary.

The discovery, connection, and logging in is handled in userspace by the iscsiadm utility, and the error handling is also handled in userspace by iscsid.

Both iscsiadm and iscsid are part of the iscsi-initiator-utils package under Fedora.

B.1. iSCSI disks in anaconda

Anaconda can discover (and then log in to) iSCSI disks in two ways:

1. When anaconda starts, it checks if the BIOS or add-on boot ROMs of the system support iSCSI Boot Firmware Table (iBFT), a BIOS extension for systems which can boot from iSCSI. If the BIOS supports iBFT, anaconda will read the iSCSI target information for the configured boot disk from the BIOS and log in to this target, making it available as an installation target.

2. If you select the Specialized Storage Devices option during installation, the storage device selection screen presents you with an Add Advanced Target button. If you click this button, you can add iSCSI target information like the discovery IP address. Anaconda probes the given IP address and logs in to any targets that it finds. See Section 9.5.1.1, “Advanced Storage Options” for the details that you can specify for iSCSI targets.

While anaconda uses iscsiadm to find and log into iSCSI targets, iscsiadm automatically stores any information about these targets in the iscsiadm iSCSI database. Anaconda then copies this database to the installed system and marks any iSCSI targets not used for / so that the system will automatically log in to them when it starts. If / is placed on an iSCSI target, initrd will log into this target and anaconda does not include this target in start up scripts to avoid multiple attempts to log into the same target.

If / is placed on an iSCSI target, anaconda sets NetworkManager to ignore any network interfaces that were active during the installation process. These interfaces will also be configured by initrd when the system starts. If NetworkManager were to reconfigure these interfaces, the system would lose its connection to /.

B.2. iSCSI disks during start up

iSCSI-related events might occur at a number of points while the system starts:
Appendix B. iSCSI disks

1. The init script in the initrd will log in to iSCSI targets used for / (if any). This is done using the iscsistart utility (which can do this without requiring iscsid to run).

2. When the root filesystem has been mounted and the various service initscripts get run, the iscsid initscript will get called. This script will then start iscsid if any iSCSI targets are used for /, or if any targets in the iSCSI database are marked to be logged in to automatically.

3. After the classic network service script has been run (or would have been run if enabled) the iscsi initscript will run. If the network is accessible, this will log in to any targets in the iSCSI database which are marked to be logged in to automatically. If the network is not accessible, this script will exit quietly.

4. When using NetworkManager to access the network (instead of the classic network service script), NetworkManager will call the iscsi initscript. See: /etc/NetworkManager/dispatcher.d/04-iscsi

**Important**

Because NetworkManager is installed in /usr, you cannot use it to configure network access if /usr is on network-attached storage such as an iSCSI target.

If iscsid is not needed as the system starts, it will not start automatically. If you start iscsiadm, iscsiadm will start iscsid in turn.
Appendix C. Disk Encryption

C.1. What is block device encryption?
Block device encryption protects the data on a block device by encrypting it. To access the device’s decrypted contents, a user must provide a passphrase or key as authentication. This provides additional security beyond existing OS security mechanisms in that it protects the device’s contents even if it has been physically removed from the system.

C.2. Encrypting block devices using dm-crypt/LUKS

Linux Unified Key Setup (LUKS) is a specification for block device encryption. It establishes an on-disk format for the data, as well as a passphrase/key management policy.

LUKS uses the kernel device mapper subsystem via the dm-crypt module. This arrangement provides a low-level mapping that handles encryption and decryption of the device’s data. User-level operations, such as creating and accessing encrypted devices, are accomplished through the use of the cryptsetup utility.

C.2.1. Overview of LUKS

- What LUKS does:
  - LUKS encrypts entire block devices
  - LUKS is thereby well-suited for protecting the contents of mobile devices such as:
    - Removable storage media
    - Laptop disk drives
  - The underlying contents of the encrypted block device are arbitrary.
    - This makes it useful for encrypting swap devices.
    - This can also be useful with certain databases that use specially formatted block devices for data storage.
  - LUKS uses the existing device mapper kernel subsystem.
    - This is the same subsystem used by LVM, so it is well tested.
  - LUKS provides passphrase strengthening.
    - This protects against dictionary attacks.
  - LUKS devices contain multiple key slots.
    - This allows users to add backup keys/passphrases.

- What LUKS does not do:
  - LUKS is not well-suited for applications requiring many (more than eight) users to have distinct access keys to the same device.
  - LUKS is not well-suited for applications requiring file-level encryption.

More detailed information about LUKS is available from the project website at http://code.google.com/p/cryptsetup/.
Appendix C. Disk Encryption

C.2.2. How will I access the encrypted devices after installation? (System Startup)
During system startup you will be presented with a passphrase prompt. After the correct passphrase has been provided the system will continue to boot normally. If you used different passphrases for multiple encrypted devices you may need to enter more than one passphrase during the startup.

Tip
Consider using the same passphrase for all encrypted block devices in a given system. This will simplify system startup and you will have fewer passphrases to remember. Just make sure you choose a good passphrase!

C.2.3. Choosing a Good Passphrase
While dm-crypt/LUKS supports both keys and passphrases, the anaconda installer only supports the use of passphrases for creating and accessing encrypted block devices during installation.

LUKS does provide passphrase strengthening but it is still a good idea to choose a good (meaning "difficult to guess") passphrase. Note the use of the term "passphrase", as opposed to the term "password". This is intentional. Providing a phrase containing multiple words to increase the security of your data is important.

C.3. Creating Encrypted Block Devices in Anaconda
You can create encrypted devices during system installation. This allows you to easily configure a system with encrypted partitions.

To enable block device encryption, check the "Encrypt System" checkbox when selecting automatic partitioning or the "Encrypt" checkbox when creating an individual partition, software RAID array, or logical volume. After you finish partitioning, you will be prompted for an encryption passphrase. This passphrase will be required to access the encrypted devices. If you have pre-existing LUKS devices and provided correct passphrases for them earlier in the install process the passphrase entry dialog will also contain a checkbox. Checking this checkbox indicates that you would like the new passphrase to be added to an available slot in each of the pre-existing encrypted block devices.

Tip
Checking the "Encrypt System" checkbox on the "Automatic Partitioning" screen and then choosing "Create custom layout" does not cause any block devices to be encrypted automatically.
What Kinds of Block Devices Can Be Encrypted?

Most types of block devices can be encrypted using LUKS. From anaconda you can encrypt partitions, LVM physical volumes, LVM logical volumes, and software RAID arrays.

C.3.2. Saving Passphrases

If you use a kickstart file during installation, you can automatically save the passphrases used during installation to an encrypted file (an escrow packet) on the local file system. To use this feature, you must have an X.509 certificate available at a location that anaconda can access. To specify the URL of this certificate, add the \(--escrowcert\) parameter to any of the \(\text{autopart, logvol, part or raid}\) commands. During installation, the encryption keys for the specified devices are saved in files in /\root, encrypted with the certificate.

You can save escrow packets during installation only with the use of a kickstart file — refer to Chapter 15, Kickstart Installations for more detail. You cannot save an escrow packet during an interactive installation, although you can create one on an installed system with the \text{volume_key} tool. The \text{volume_key} tool also allows you to use the information stored in an escrow packet to restore access to an encrypted volume. Refer to the \text{volume_key} manpage for more information.

C.3.3. Creating and Saving Backup Passphrases

If you use a kickstart file during installation, anaconda can add a randomly generated backup passphrase to each block device on the system and save each passphrase to an encrypted file on the local file system. Specify the URL of this certificate with the \(--escrowcert\) parameter as described in Section C.3.2, “Saving Passphrases”, followed by the \(--backuppassphrase\) parameter for each of the kickstart commands that relate to the devices for which you want to create backup passphrases.

Note that this feature is available only while performing a kickstart installation. Refer to Chapter 15, Kickstart Installations for more detail.

C.4. Creating Encrypted Block Devices on the Installed System After Installation

Encrypted block devices can be created and configured after installation, using either the following method or Disk Utility.

C.4.1. Create the block devices

Create the block devices you want to encrypt by using \text{parted, pvcreate, lvcreate} and \text{mdadm}.

C.4.2. Optional: Fill the device with random data

Filling <device> (e.g: \text{/dev/sda3}) with random data before encrypting it greatly increases the strength of the encryption. The downside is that it can take a very long time.
Appendix C. Disk Encryption

### Warning

The commands below will destroy any existing data on the device.

- The best way, which provides high quality random data but takes a long time (several minutes per gigabyte on most systems):

  `dd if=/dev/urandom of=<device>`

- Fastest way, which provides lower quality random data:

  `badblocks -c 10240 -s -w -t random -v <device>`

#### C.4.3. Format the device as a dm-crypt/LUKS encrypted device

### Warning

The command below will destroy any existing data on the device.

`cryptsetup luksFormat <device>`

#### Note

For more information, read the `cryptsetup(8)` man page.

After supplying the passphrase twice the device will be formatted for use. To verify, use the following command:

`cryptsetup isLuks <device> && echo Success`

To see a summary of the encryption information for the device, use the following command:

`cryptsetup luksDump <device>`

#### C.4.4. Create a mapping to allow access to the device's decrypted contents

To access the device's decrypted contents, a mapping must be established using the kernel `devicemapper`.
Create filesystems on the mapped device, or continue to build complex storage structures using the mapped device

It is useful to choose a meaningful name for this mapping. LUKS provides a UUID (Universally Unique Identifier) for each device. This, unlike the device name (e.g: /dev/sda3), is guaranteed to remain constant as long as the LUKS header remains intact. To find a LUKS device's UUID, run the following command:

```
cryptsetup luksUUID <device>
```

An example of a reliable, informative and unique mapping name would be `luks-<uuid>`, where `<uuid>` is replaced with the device's LUKS UUID (e.g: `luks-50ec957a-5b5a-47ee-85e6-f8085bb97a8`). This naming convention might seem unwieldy but is it not necessary to type it often.

```
cryptsetup luksOpen <device> <name>
```

There should now be a device node, /dev/mapper/<name>, which represents the decrypted device. This block device can be read from and written to like any other unencrypted block device.

To see some information about the mapped device, use the following command:

```
dmsetup info <name>
```

**Tip**

For more information, read the `dmsetup(8)` man page.

**C.4.5. Create filesystems on the mapped device, or continue to build complex storage structures using the mapped device**

Use the mapped device node (/dev/mapper/<name>) as any other block device. To create an ext2 filesystem on the mapped device, use the following command:

```
mke2fs /dev/mapper/<name>
```

To mount this filesystem on /mnt/test, use the following command:

**Important**

The directory /mnt/test must exist before executing this command.

```
mount /dev/mapper/<name> /mnt/test
```

**C.4.6. Add the mapping information to /etc/crypttab**

In order for the system to set up a mapping for the device, an entry must be present in the /etc/crypttab file. If the file doesn't exist, create it and change the owner and group to root (root:root) and change the mode to 0744. Add a line to the file with the following format:
Appendix C. Disk Encryption

The <device> field should be given in the form "UUID=<luks_uuid>", where <luks_uuid> is the LUKS uuid as given by the command \texttt{cryptsetup luksUUID <device>}. This ensures the correct device will be identified and used even if the device node (eg: /dev/sda5) changes.

\textbf{Tip}

For details on the format of the /etc/crypttab file, read the \texttt{crypttab(5)} man page.

\section*{C.4.7. Add an entry to /etc/fstab}

Add an entry to /etc/fstab. This is only necessary if you want to establish a persistent association between the device and a mountpoint. Use the decrypted device, /dev/mapper/<name> in the /etc/fstab file.

In many cases it is desirable to list devices in /etc/fstab by UUID or by a filesystem label. The main purpose of this is to provide a constant identifier in the event that the device name (eg: /dev/sda4) changes. LUKS device names in the form of /dev/mapper/luks-<luks_uuid> are based only on the device's LUKS UUID, and are therefore guaranteed to remain constant. This fact makes them suitable for use in /etc/fstab.

\textbf{Tip}

For details on the format of the /etc/fstab file, read the \texttt{fstab(5)} man page.

\section*{C.5. Common Post-Installation Tasks}

The following sections are about common post-installation tasks.

\subsection*{C.5.1. Set a randomly generated key as an additional way to access an encrypted block device}

These sections are about generating keys and adding keys.

\subsubsection*{C.5.1.1. Generate a key}

This will generate a 256-bit key in the file \$HOME/keyfile.

\begin{verbatim}
  dd if=/dev/urandom of=$HOME/keyfile bs=32 count=1
  chmod 600 $HOME/keyfile
\end{verbatim}

\subsubsection*{C.5.1.2. Add the key to an available keyslot on the encrypted device}

\begin{verbatim}
  cryptsetup luksAddKey <device> ~/keyfile
\end{verbatim}
Add a new passphrase to an existing device

### C.5.2. Add a new passphrase to an existing device

```bash
cryptsetup luksAddKey <device>
```

After being prompted for any one of the existing passphrases for authentication, you will be prompted to enter the new passphrase.

### C.5.3. Remove a passphrase or key from a device

```bash
cryptsetup luksRemoveKey <device>
```

You will be prompted for the passphrase you wish to remove and then for any one of the remaining passphrases for authentication.
Appendix D. Understanding LVM

LVM (Logical Volume Management) partitions provide a number of advantages over standard partitions. LVM partitions are formatted as physical volumes. One or more physical volumes are combined to form a volume group. Each volume group’s total storage is then divided into one or more logical volumes. The logical volumes function much like standard partitions. They have a file system type, such as ext4, and a mount point.

The /boot Partition and LVM

On most architectures, the boot loader cannot read LVM volumes. You must make a standard, non-LVM disk partition for your /boot partition.

However, on System z, the zipl boot loader supports /boot on LVM logical volumes with linear mapping.

To understand LVM better, imagine the physical volume as a pile of blocks. A block is simply a storage unit used to store data. Several piles of blocks can be combined to make a much larger pile, just as physical volumes are combined to make a volume group. The resulting pile can be subdivided into several smaller piles of arbitrary size, just as a volume group is allocated to several logical volumes.

An administrator may grow or shrink logical volumes without destroying data, unlike standard disk partitions. If the physical volumes in a volume group are on separate drives or RAID arrays then administrators may also spread a logical volume across the storage devices.

You may lose data if you shrink a logical volume to a smaller capacity than the data on the volume requires. To ensure maximum flexibility, create logical volumes to meet your current needs, and leave excess storage capacity unallocated. You may safely grow logical volumes to use unallocated space, as your needs dictate.

LVM and the Default Partition Layout

By default, the installation process creates / and swap partitions within LVM volumes, with a separate /boot partition.
Appendix E. The GRUB Boot Loader

When a computer running Linux is turned on, the operating system is loaded into memory by a special program called a *boot loader*. A boot loader usually exists on the system's primary hard drive (or other media device) and has the sole responsibility of loading the Linux kernel with its required files or (in some cases) other operating systems into memory.

E.1. Boot Loaders and System Architecture

Each architecture capable of running Fedora uses a different boot loader. The following table lists the boot loaders available for each architecture:

<table>
<thead>
<tr>
<th>Architecture</th>
<th>Boot Loaders</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMD® AMD64</td>
<td>GRUB</td>
</tr>
<tr>
<td>IBM® eServer™ System p™</td>
<td>yaboot</td>
</tr>
<tr>
<td>IBM® System z®</td>
<td>z/IPL</td>
</tr>
<tr>
<td>x86</td>
<td>GRUB</td>
</tr>
</tbody>
</table>

This appendix discusses commands and configuration options for the GRUB boot loader included with Fedora for the x86 architecture.

**Important — Supported file systems**

The GRUB bootloader in Fedora 17 supports only the ext2, ext3, and ext4 (recommended) file systems. You cannot use any other file system for `/boot`, such as Btrfs, XFS, or VFAT.

E.2. GRUB

The *GNU GRand Unified Boot loader* (GRUB) is a program which enables the selection of the installed operating system or kernel to be loaded at system boot time. It also allows the user to pass arguments to the kernel.

E.2.1. GRUB and the boot process on BIOS-based x86 systems

This section describes the specific role GRUB plays when booting a BIOS-based x86 system. For a look at the overall boot process, refer to *Section F.2, “A Detailed Look at the Boot Process”*. GRUB consists of the following images:

- **boot.img**: the first image to load in GRUB on BIOS-based x86 systems, which is written to either a master boot record (MBR) or the boot sector of a partition. Because a PC boot sector is 512 bytes, the size of this image is exactly 512 bytes.

---

1. For more on the system BIOS and the MBR, refer to *Section F.2.1.1, “BIOS-based x86 systems”*. 

---

283
BIOS cannot read partition tables or file systems. It initializes the hardware, reads the MBR, then depends entirely on boot.img to continue the boot process. This image is similar to Stage 1 in GRUB Legacy.

- **diskboot.img**: the first sector of the core image once the system boots from a hard disk. It reads the remaining parts of the core image to memory before initializing the kernel.

- **cdboot.img**: the first sector of the core image once the system is booted from a CD-ROM drive, similar to diskboot.img.

- **core.img**: GRUB's core image, built dynamically by the grub-mkimage program using the kernel image and a list of modules. It typically has sufficient modules to access /boot/grub2, and loads the rest from the file system at run-time.

- **kernel.img**: the location of GRUB's basic run-time functions. Although built into all core images, it is rarely used directly.

- ***.mod**: the remainder of GRUB is located in dynamically loadable modules. These modules load automatically or are built into the core image if they are essential, or can be initialized manually by the insmod command.

The method used to boot Linux is called *direct loading* because the boot loader loads the operating system directly. There is no intermediary between the boot loader and the kernel.

The boot process used by other operating systems may differ. For example, the Microsoft® Windows® operating system, as well as other operating systems, are loaded using *chain loading*. Under this method, the MBR points to the first sector of the partition holding the operating system, where it finds the files necessary to actually boot that operating system.

GRUB supports both direct and chain loading boot methods, allowing it to boot almost any operating system.

**Warning**

During installation, Microsoft's DOS and Windows installation programs completely overwrite the MBR, destroying any existing boot loaders. If creating a dual-boot system, it is best to install the Microsoft operating system first.

### E.2.2. GRUB and the boot process on UEFI-based x86 systems

This section describes the specific role GRUB plays when booting a UEFI-based x86 system. For a look at the overall boot process, refer to Section F.2, "A Detailed Look at the Boot Process".

GRUB loads itself into memory in the following stages:

1. The UEFI-based platform reads the partition table on the system storage and mounts the EFI System Partition (ESP), a VFAT partition labeled with a particular globally unique identifier (GUID). The ESP contains EFI applications such as bootloaders and utility software, stored in directories specific to software vendors. Viewed from within the Fedora 17 file system, the ESP is /boot/efi/, and EFI software provided by Red Hat is stored in /boot/efi/EFI/redhat/.
2. The `/boot/efi/EFI/redhat/` directory contains `grub.efi`, a version of GRUB compiled for the EFI firmware architecture as an EFI application. In the simplest case, the EFI boot manager selects `grub.efi` as the default bootloader and reads it into memory.

If the ESP contains other EFI applications, the EFI boot manager might prompt you to select an application to run, rather than load `grub.efi` automatically.

3. GRUB determines which operating system or kernel to start, loads it into memory, and transfers control of the machine to that operating system.

Because each vendor maintains its own directory of applications in the ESP, chain loading is not normally necessary on UEFI-based systems. The EFI boot manager can load any of the operating system bootloaders that are present in the ESP.

### E.2.3. Features of GRUB

GRUB contains several features that make it preferable to other boot loaders available for the x86 architecture. Below is a partial list of some of the more important features:

- **GRUB provides a true command-based, pre-OS environment on x86 machines.** This feature affords the user maximum flexibility in loading operating systems with specified options or gathering information about the system. For years, many non-x86 architectures have employed pre-OS environments that allow system booting from a command line.

- **GRUB supports Logical Block Addressing (LBA) mode.** LBA places the addressing conversion used to find files in the hard drive's firmware, and is used on many IDE and all SCSI hard devices. Before LBA, boot loaders could encounter the 1024-cylinder BIOS limitation, where the BIOS could not find a file after the 1024 cylinder head of the disk. LBA support allows GRUB to boot operating systems from partitions beyond the 1024-cylinder limit, so long as the system BIOS supports LBA mode. Most modern BIOS revisions support LBA mode.

- **GRUB can read ext2 partitions.** This functionality allows GRUB to access its configuration file, `/boot/grub2/grub.cfg`, every time the system boots, eliminating the need for the user to write a new version of the first stage boot loader to the MBR when configuration changes are made. The only time a user needs to reinstall GRUB on the MBR is if the physical location of the `/boot/` partition is moved on the disk. For details on installing GRUB to the MBR, refer to Section E.3, "Installing GRUB".

### E.3. Installing GRUB

If GRUB was not installed during the installation process, it can be installed afterward. Once installed, it automatically becomes the default boot loader.

Before installing GRUB, make sure to use the latest GRUB package available or use the GRUB package from the installation DVD. For instructions on installing packages, refer to the chapter titled *Package Management with RPM* in the *Fedora Deployment Guide*.

Once the GRUB package is installed, open a root shell prompt and run the command `grub-install <location>`, where `<location>` is the location that the GRUB Stage 1 boot loader should be installed. For example, the following command installs GRUB to the MBR of the master IDE device on the primary IDE bus:
The next time the system boots, the GRUB graphical boot loader menu appears before the kernel loads into memory.

**Important — GRUB and RAID**

GRUB cannot construct a software RAID. Therefore, the `/boot` directory must reside on a single, specific disk partition. The `/boot` directory cannot be striped across multiple disks, as in a level 0 RAID. To use a level 0 RAID on your system, place `/boot` on a separate partition outside the RAID.

Similarly, because the `/boot` directory must reside on a single, specific disk partition, GRUB cannot boot the system if the disk holding that partition fails or is removed from the system. This is true even if the disk is mirrored in a level 1 RAID.

Note that these issues apply only to RAID that is implemented in software, where the individual disks that make up the array are still visible as individual disks on the system. These issues do not apply to hardware RAID where multiple disks are represented as a single device.

**E.4. GRUB Terminology**

One of the most important things to understand before using GRUB is how the program refers to devices, such as hard drives and partitions. This information is particularly important when configuring GRUB to boot multiple operating systems.

**E.4.1. Device Names**

When referring to a specific device with GRUB, do so using the following format (note that the parentheses and comma are very important syntactically):

\[
(<\text{type-of-device}><\text{bios-device-number}>,<\text{partition-number}>)
\]

The `<type-of-device>` specifies the type of device from which GRUB boots. The two most common options are `hd` for a hard disk or `fd` for a 3.5 diskette. A lesser used device type is also available called `nd` for a network disk. Instructions on configuring GRUB to boot over the network are available online at [http://www.gnu.org/software/grub/manual/](http://www.gnu.org/software/grub/manual/).

The `<bios-device-number>` is the BIOS device number. The primary IDE hard drive is numbered 0 and a secondary IDE hard drive is numbered 1. This syntax is roughly equivalent to that used for devices by the kernel. For example, the `a` in `hda` for the kernel is analogous to the `0` in `hd0` for GRUB, the `b` in `hdb` is analogous to the `1` in `hd1`, and so on.

The `<partition-number>` specifies the number of a partition on a device. Unlike the `<bios-device-number>`, most types of partitions are numbered starting at 1. However, BSD partitions are specified using letters, with `a` corresponding to 1, `b` corresponding to 2, and so on.
Note

The numbering system for devices under GRUB always begins with 0, not 1. Failing to make this distinction is one of the most common mistakes made by new users.

GRUB2 features new partition numbering

Fedora 17 incorporates GRUB2, which numbers partitions and devices differently. Instead of 0, partition numbering begins at 1. However, device numbering still begins at 0.

To give an example, if a system has more than one hard drive, GRUB refers to the first hard drive as (hd0) and the second as (hd1). Likewise, GRUB refers to the first partition on the first drive as (hd0,1) and the third partition on the second hard drive as (hd1,3).

In general the following rules apply when naming devices and partitions under GRUB:

- It does not matter if system hard drives are IDE or SCSI, all hard drives begin with the letters hd. The letters fd are used to specify 3.5 diskettes.
- To specify an entire device without respect to partitions, leave off the comma and the partition number. This is important when telling GRUB to configure the MBR for a particular disk. For example, (hd0) specifies the MBR on the first device and (hd3) specifies the MBR on the fourth device.
- If a system has multiple drive devices, it is very important to know how the drive boot order is set in the BIOS. This is a simple task if a system has only IDE or SCSI drives, but if there is a mix of devices, it becomes critical that the type of drive with the boot partition be accessed first.

E.4.2. File Names and Blocklists

When typing commands to GRUB that reference a file, such as a menu list, it is necessary to specify an absolute file path immediately after the device and partition numbers.

The following illustrates the structure of such a command:

\[(<device-type><device-number>,<partition-number>)/<path/to/file>\]

In this example, replace <device-type> with hd, fd, or nd. Replace <device-number> with the integer for the device. Replace </path/to/file> with an absolute path relative to the top-level of the device.

It is also possible to specify files to GRUB that do not actually appear in the file system, such as a chain loader that appears in the first few blocks of a partition. To load such files, provide a blocklist that specifies block by block where the file is located in the partition. Since a file is often comprised of several different sets of blocks, blocklists use a special syntax. Each block containing the file is specified by an offset number of blocks, followed by the number of blocks from that offset point. Block offsets are listed sequentially in a comma-delimited list.
The following is a sample blocklist:

```
0+50, 100+25, 200+1
```

This sample blocklist specifies a file that starts at the first block on the partition and uses blocks 0 through 49, 100 through 124, and 200.

Knowing how to write blocklists is useful when using GRUB to load operating systems which require chain loading. It is possible to leave off the offset number of blocks if starting at block 0. As an example, the chain loading file in the first partition of the first hard drive would have the following name:

```
(hd0,1)+1
```

The following shows the `chainloader` command with a similar blocklist designation at the GRUB command line after setting the correct device and partition as root:

```
chainloader +1
```

### E.4.3. The Root File System and GRUB

The use of the term *root file system* has a different meaning in regard to GRUB. It is important to remember that GRUB's root file system has nothing to do with the Linux root file system.

The GRUB root file system is the top level of the specified device. For example, the image file `(/hd1,1)/grub/splash.xpm.gz` is located within the `/grub/` directory at the top-level (or root) of the `(hd1,1)` partition (which is actually the `/boot/` partition for the system).

Next, the `linux` command is executed with the location of the kernel file as an option. Once the Linux kernel boots, it sets up the root file system that Linux users are familiar with. The original GRUB root file system and its mounts are forgotten; they only existed to boot the kernel file.

Refer to the `root` and `linux` commands in Section E.6, “GRUB Commands” for more information.

### E.5. GRUB Interfaces

GRUB features three interfaces which provide different levels of functionality. Each of these interfaces allows users to boot the Linux kernel or another operating system.

The interfaces are as follows:

---

**Note**

The following GRUB interfaces can only be accessed by pressing any key within the three seconds of the GRUB menu bypass screen.
**Menu Interface**

This is the default interface shown when GRUB is configured by the installation program. A menu of operating systems or preconfigured kernels are displayed as a list, ordered by name. Use the arrow keys to select an operating system or kernel version and press the *Enter* key to boot it. If you do nothing on this screen, then after the time out period expires GRUB will load the default option.

Press the *e* key to enter the entry editor interface or the *c* key to load a command line interface.

Refer to *Section E.7, “GRUB Menu Configuration File”* for more information on configuring this interface.

**Menu Entry Editor Interface**

To access the menu entry editor, press the *e* key from the boot loader menu. The GRUB commands for that entry are displayed here, and users may alter these command lines before booting the operating system by adding a command line (*o* inserts a new line after the current line and *O* inserts a new line before it), editing one (*e*), or deleting one (*d*).

After all changes are made, the *b* key executes the commands and boots the operating system. The *Esc* key discards any changes and reloads the standard menu interface. The *c* key loads the command line interface.

**Note**

For information about changing runlevels using the GRUB menu entry editor, refer to *Section E.8, “Changing Runlevels at Boot Time”*.

**Command Line Interface**

The command line interface is the most basic GRUB interface, but it is also the one that grants the most control. The command line makes it possible to type any relevant GRUB commands followed by the *Enter* key to execute them. This interface features some advanced shell-like features, including *Tab* key completion based on context, and *Ctrl* key combinations when typing commands, such as *Ctrl+a* to move to the beginning of a line and *Ctrl+e* to move to the end of a line. In addition, the arrow, *Home*, *End*, and *Delete* keys work as they do in the *bash* shell.

Refer to *Section E.6, “GRUB Commands”* for a list of common commands.

### E.5.1. Interfaces Load Order

When GRUB loads its second stage boot loader, it first searches for its configuration file. Once found, the menu interface bypass screen is displayed. If a key is pressed within three seconds, GRUB builds a menu list and displays the menu interface. If no key is pressed, the default kernel entry in the GRUB menu is used.

If the configuration file cannot be found, or if the configuration file is unreadable, GRUB loads the command line interface, allowing the user to type commands to complete the boot process.

If the configuration file is not valid, GRUB prints out the error and asks for input. This helps the user see precisely where the problem occurred. Pressing any key reloads the menu interface, where it is then possible to edit the menu option and correct the problem based on the error reported by GRUB. If the correction fails, GRUB reports an error and reloads the menu interface.
E.6. GRUB Commands

GRUB allows a number of useful commands in its command line interface. Some of the commands accept options after their name; these options should be separated from the command and other options on that line by space characters.

The following is a list of useful commands:

- **boot** — Boots the operating system or chain loader that was last loaded.

- **chainloader <path/to/file>** — Loads the specified file as a chain loader. If the file is located on the first sector of the specified partition, use the blocklist notation, +1, instead of the file name.

  The following is an example chainloader command:

  ```
  chainloader +1
  ```

- **displaymem** — Displays the current use of memory, based on information from the BIOS. This is useful to determine how much RAM a system has prior to booting it.

- **initrd <path/to/initrd>** — Enables users to specify an initial RAM disk to use when booting. An initrd is necessary when the kernel needs certain modules in order to boot properly, such as when the root partition is formatted with the ext3 or ext4 file system.

  The following is an example initrd command:

  ```
  initrd /initrd-2.6.8-1.523.img
  ```

- **install <stage-1> <install-disk> <stage-2> p config-file** — Installs GRUB to the system MBR.

  - **<stage-1>** — Signifies a device, partition, and file where the first boot loader image can be found, such as (hd1,1)/grub/stage1.

  - **<install-disk>** — Specifies the disk where the stage 1 boot loader should be installed, such as (hd0).

  - **<stage-2>** — Passes the stage 2 boot loader location to the stage 1 boot loader, such as (hd1,1)/grub/stage2.

  - **p <config-file>** — This option tells the install command to look for the menu configuration file specified by <config-file>, such as (hd0,1)/grub/grub.conf.

**Warning**

The install command overwrites any information already located on the MBR.
• `linux <path/to/linux> <option-1> <option-N>` — Specifies the kernel file to load when booting the operating system. Replace `<path/to/linux>` with an absolute path from the partition specified by the root command. Replace `<option-1>` with options for the Linux kernel, such as `set root=/dev/VolGroup00/LogVol00` to specify the device on which the root partition for the system is located. Multiple options can be passed to the kernel in a space separated list.

The following is an example `kernel` command:

```
linux /vmlinuz-2.6.8-1.523 ro root=/dev/VolGroup00/LogVol00
```

The option in the previous example specifies that the root file system for Linux is located on the `hda5` partition.

• `set root=(<device-type><device-number>,<partition>)` — Configures the root partition for GRUB, such as `(hd1,1)`, and mounts the partition.

The following is an example `root` command:

```
set root=(hd0,1)
```

Other commands are also available; type `help --all` for a full list of commands. For a description of all GRUB commands, refer to the documentation available online at [http://www.gnu.org/software/grub/manual/](http://www.gnu.org/software/grub/manual/).

### E.7. GRUB Menu Configuration File

The configuration file (`/boot/grub2/grub.cfg`), which is used to create the list of operating systems to boot in GRUB's menu interface, essentially allows the user to select a pre-set group of commands to execute. The commands given in [Section E.6, “GRUB Commands”](#) can be used, as well as some special commands that are only available in the configuration file. Changes to `grub.cfg` are enacted by editing `etc/default/grub` and files in the `etc/grub.d` directory, particularly `10_linux` and `40_custom`, and then running the `grub2-mkconfig` command with root privileges.

### E.7.1. Configuration File Structure

The GRUB menu interface configuration file is `/boot/grub2/grub.cfg`. The commands to set the global preferences for the menu interface are placed at the top of the file, followed by stanzas for each operating kernel or operating system listed in the menu.

The following is a very basic GRUB menu configuration file designed to boot Fedora:

```
menuentry 'Fedora Linux, with Linux 3.1.0-0.rc6.git0.3.fc16.x86_64'
  set root=(hd0,1)
  linux /vmlinuz-2.6.27.19-170.2.35.fc10.1686 ro root=UUID=04a07c13-e6bf-6d5a-b207-002689545705 rhgb quiet
  initrd /initramfs-3.1.0-0.rc6.git0.3.fc16.x86_64.img
```

Configuring a GRUB menu configuration file to boot multiple operating systems is beyond the scope of this chapter. Consult [Section E.9, “Additional Resources”](#) for a list of additional resources.
E.7.2. Configuration File Directives

The following are directives commonly used in the GRUB menu configuration file:

- **chainloader <path/to/file>** — Loads the specified file as a chain loader. Replace `<path/to/file>` with the absolute path to the chain loader. If the file is located on the first sector of the specified partition, use the blocklist notation, `+1`.

- **color <normal-color> <selected-color>** — Allows specific colors to be used in the menu, where two colors are configured as the foreground and background. Use simple color names such as `red/black`. For example:

```
color red/black green/blue
```

- **default=<integer>** — Replace `<integer>` with the default entry title number to be loaded if the menu interface times out.

- **fallback=<integer>** — Replace `<integer>` with the entry title number to try if the first attempt fails.

- **hiddenmenu** — Prevents the GRUB menu interface from being displayed, loading the default entry when the timeout period expires. The user can see the standard GRUB menu by pressing the `Esc` key.

- **initrd <path/to/initrd>** — Enables users to specify an initial RAM disk to use when booting. Replace `<path/to/initrd>` with the absolute path to the initial RAM disk.

- **linux <path/to/linux> <option-1> ... <option-N>** — Specifies the kernel file to load when booting the operating system. Replace `<path/to/linux>` with an absolute path from the partition specified by the root directive. Multiple options can be passed to the kernel when it is loaded. These options include:
  - **rhgb** *(Red Hat graphical boot)* — displays an animation during the boot process, rather than lines of text.
  - **quiet** — suppresses all but the most important messages in the part of the boot sequence before the graphical boot animation begins.

- **password=<password>** — Prevents a user who does not know the password from editing the entries for this menu option.

Optionally, it is possible to specify an alternate menu configuration file after the `password=<password>` directive. In this case, GRUB restarts the second stage boot loader and uses the specified alternate configuration file to build the menu. If an alternate menu configuration file is left out of the command, a user who knows the password is allowed to edit the current configuration file.

For more information about securing GRUB, refer to the chapter titled *Workstation Security* in the *Fedora Deployment Guide*.

- **map** — Swaps the numbers assigned to two hard drives. For example:

```
map (hd0) (hd3)
```
Changing Runlevels at Boot Time

map (hd3) (hd0)

assigns the number 0 to the fourth hard drive, and the number 3 to the first hard drive. This option is especially useful if you configure your system with an option to boot a Windows operating system, because the Windows boot loader must find the Windows installation on the first hard drive.

For example, if your Windows installation is on the fourth hard drive, the following entry in `grub.conf` will allow the Windows boot loader to load Windows correctly:

```
title Windows
map (hd0) (hd3)
map (hd3) (hd0)
rootnoverify (hd3,0)
chainloader +1
```

- **menuentry "title"** — Specifies a title to be used with a particular group of commands used to load a kernel or operating system.
- **root \(<device-type><device-number>,<partition>\)** — Configures the root partition for GRUB, such as \((hd1,1)\), and mounts the partition.
- **rootnoverify \(<device-type><device-number>,<partition>\)** — Configures the root partition for GRUB, just like the `root` command, but does not mount the partition.
- **timeout=\<integer>** — Specifies the interval, in seconds, that GRUB waits before loading the entry designated in the `default` command.
- **splashimage=\<path-to-image>** — Specifies the location of the splash screen image to be used when GRUB boots.

To add human-readable comments to the menu configuration file, begin the line with the hash mark character (#).

E.8. Changing Runlevels at Boot Time

Under Fedora, it is possible to change the default runlevel at boot time.

To change the runlevel of a single boot session, use the following instructions:

- At boot time, press the Esc key to reach the GRUB splash screen, then press any key to enter the GRUB menu (within the first three seconds).
- Press the a key to append to the `linux` command.
- Add `<space>`\<runlevel> at the end of the boot options line to boot to the desired runlevel. For example, the following entry would initiate a boot process into runlevel 3:

```
grub append> ro root=/dev/VolGroup00/LogVol00 rhgb quiet 3
```

E.9. Additional Resources

This chapter is only intended as an introduction to GRUB. Consult the following resources to discover more about how GRUB works.
E.9.1. Installed Documentation

• `/usr/share/doc/grub-<version-number>/` — This directory contains good information about using and configuring GRUB, where `<version-number>` corresponds to the version of the GRUB package installed.

• `info grub` — The GRUB info page contains a tutorial, a user reference manual, a programmer reference manual, and a FAQ document about GRUB and its usage.

E.9.2. Useful Websites

• `http://www.gnu.org/software/grub/`\(^2\) — The home page of the GNU GRUB project. This site contains information concerning the state of GRUB development and an FAQ.
Appendix F. Boot Process, Init, and Shutdown

An important and powerful aspect of Fedora is the open, user-configurable method it uses for starting the operating system. Users are free to configure many aspects of the boot process, including specifying the programs launched at boot-time. Similarly, system shutdown gracefully terminates processes in an organized and configurable way, although customization of this process is rarely required.

Understanding how the boot and shutdown processes work not only allows customization, but also makes it easier to troubleshoot problems related to starting or shutting down the system.

F.1. The Boot Process

Below are the basic stages of the boot process:

1. The system loads and runs a boot loader. The specifics of this process depend on the system architecture. For example:
   - BIOS-based x86 systems run a first-stage boot loader from the MBR of the primary hard disk that, in turn, loads an additional boot loader, GRUB.
   - UEFI-based x86 systems mount an EFI System Partition that contains a version of the GRUB boot loader. The EFI boot manager loads and runs GRUB as an EFI application.

2. The boot loader loads the kernel into memory, which in turn loads any necessary modules and mounts the root partition read-only.

3. The kernel transfers control of the boot process to the /sbin/init program.

4. The /sbin/init program loads all services and user-space tools, and mounts all partitions listed in /etc/fstab.

5. The user is presented with a login screen for the freshly booted Linux system.

Because configuration of the boot process is more common than the customization of the shutdown process, the remainder of this chapter discusses in detail how the boot process works and how it can be customized to suite specific needs.

F.2. A Detailed Look at the Boot Process

The beginning of the boot process varies depending on the hardware platform being used. However, once the kernel is found and loaded by the boot loader, the default boot process is identical across all architectures. This chapter focuses primarily on the x86 architecture.

F.2.1. The firmware interface

F.2.1.1. BIOS-based x86 systems
The Basic Input/Output System (BIOS) is a firmware interface that controls not only the first step of the boot process, but also provides the lowest level interface to peripheral devices. On x86 systems equipped with BIOS, the program is written into read-only, permanent memory and is always available for use. When the system boots, the processor looks at the end of system memory for the BIOS program, and runs it.

Once loaded, the BIOS tests the system, looks for and checks peripherals, and then locates a valid device with which to boot the system. Usually, it checks any optical drives or USB storage devices present for bootable media, then, failing that, looks to the system's hard drives. In most cases, the order of the drives searched while booting is controlled with a setting in the BIOS, and it looks on the master IDE on the primary IDE bus or for a SATA device with a boot flag set. The BIOS then loads into memory whatever program is residing in the first sector of this device, called the Master Boot Record (MBR). The MBR is only 512 bytes in size and contains machine code instructions for booting the machine, called a boot loader, along with the partition table. Once the BIOS finds and loads the boot loader program into memory, it yields control of the boot process to it.

This first-stage boot loader is a small machine code binary on the MBR. Its sole job is to locate the second stage boot loader (GRUB) and load the first part of it into memory.

**F.2.1.2. UEFI-based x86 systems**

The Unified Extensible Firmware Interface (UEFI) is designed, like BIOS, to control the boot process (through boot services) and to provide an interface between system firmware and an operating system (through runtime services). Unlike BIOS, it features its own architecture, independent of the CPU, and its own device drivers. UEFI can mount partitions and read certain file systems.

When an x86 computer equipped with UEFI boots, the interface searches the system storage for a partition labeled with a specific globally unique identifier (GUID) that marks it as the EFI System Partition (ESP). This partition contains applications compiled for the EFI architecture, which might include bootloaders for operating systems and utility software. UEFI systems include an EFI boot manager that can boot the system from a default configuration, or prompt a user to choose an operating system to boot. When a bootloader is selected, manually or automatically, UEFI reads it into memory and yields control of the boot process to it.

**F.2.2. The Boot Loader**

**F.2.2.1. The GRUB boot loader for x86 systems**

The system loads GRUB into memory, as directed by either a first-stage bootloader in the case of systems equipped with BIOS, or read directly from an EFI System Partition in the case of systems equipped with UEFI.

GRUB has the advantage of being able to read ext2, ext3, and ext4 partitions and load its configuration file — `/boot/grub2/grub.cfg` (for BIOS) or `/boot/efi/EFI/redhat/grub.cfg` (for UEFI) — at boot time. Refer to Section E.7, "GRUB Menu Configuration File" for information on how to edit this file.

---

1 GRUB reads ext3 and ext4 file systems as ext2, disregarding the journal file.
Once the second stage boot loader is in memory, it presents the user with a graphical screen showing the different operating systems or kernels it has been configured to boot (when you update the kernel, the boot loader configuration file is updated automatically). On this screen a user can use the arrow keys to choose which operating system or kernel they wish to boot and press **Enter**. If no key is pressed, the boot loader loads the default selection after a configurable period of time has passed.

Once the second stage boot loader has determined which kernel to boot, it locates the corresponding kernel binary in the `/boot/` directory. The kernel binary is named using the following format — `/boot/vmlinuz-<kernel-version>` file (where `<kernel-version>` corresponds to the kernel version specified in the boot loader's settings).

For instructions on using the boot loader to supply command line arguments to the kernel, refer to *Appendix E, The GRUB Boot Loader*. For information on changing the runlevel at the boot loader prompt, refer *Section E.8, “Changing Runlevels at Boot Time”*

The boot loader then places one or more appropriate **initramfs** images into memory. The **initramfs** is used by the kernel to load drivers and modules necessary to boot the system. This is particularly important if SCSI hard drives are present or if the systems use the ext3 or ext4 file system.

Once the kernel and the **initramfs** image(s) are loaded into memory, the boot loader hands control of the boot process to the kernel.

For a more detailed overview of the GRUB boot loader, refer to *Appendix E, The GRUB Boot Loader*.

### F.2.2.2. Boot Loaders for Other Architectures

Once the kernel loads and hands off the boot process to the `init` command, the same sequence of events occurs on every architecture. So the main difference between each architecture’s boot process is in the application used to find and load the kernel.

For example, the IBM eServer pSeries architecture uses **yaboot**, and the IBM System z systems use the z/IPL boot loader.

### F.2.3. The Kernel

When the kernel is loaded, it immediately initializes and configures the computer's memory and configures the various hardware attached to the system, including all processors, I/O subsystems, and storage devices. It then looks for the compressed **initramfs** image(s) in a predetermined location in memory, decompresses it directly to `/sysroot/` via `cpio`, and loads all necessary drivers. Next, it initializes virtual devices related to the file system, such as LVM or software RAID, before completing the **initramfs** processes and freeing up all the memory the disk image once occupied.

The kernel then creates a root device, mounts the root partition read-only, and frees any unused memory.
At this point, the kernel is loaded into memory and operational. However, since there are no user applications that allow meaningful input to the system, not much can be done with the system.

To set up the user environment, the kernel executes the `/sbin/init` program.

### F.2.4. The `/sbin/init` Program

The `/sbin/init` program (also called `init`) coordinates the rest of the boot process and configures the environment for the user.

When the `init` command starts, it becomes the parent or grandparent of all of the processes that start up automatically on the system. First, it runs the `/etc/rc.d/rc.sysinit` script, which sets the environment path, starts swap, checks the file systems, and executes all other steps required for system initialization. For example, most systems use a clock, so `rc.sysinit` reads the `/etc/sysconfig/clock` configuration file to initialize the hardware clock. Another example is if there are special serial port processes which must be initialized, `rc.sysinit` executes the `/etc/rc.serial` file.

The `init` command then processes the jobs in the `/etc/event.d` directory, which describe how the system should be set up in each SysV init runlevel. Runlevels are a state, or mode, defined by the services listed in the SysV `/etc/rc.d/rc<x>.d/` directory, where `<x>` is the number of the runlevel. For more information on SysV init runlevels, refer to Section F.4, “SysV Init Runlevels”.

Next, the `init` command sets the source function library, `/etc/rc.d/init.d/functions`, for the system, which configures how to start, kill, and determine the PID of a program.

The `init` program starts all of the background processes by looking in the appropriate `rc` directory for the runlevel specified as the default in `/etc/inittab`. The `rc` directories are numbered to correspond to the runlevel they represent. For instance, `/etc/rc.d/rc5.d/` is the directory for runlevel 5.

When booting to runlevel 5, the `init` program looks in the `/etc/rc.d/rc5.d/` directory to determine which processes to start and stop.

Below is an example listing of the `/etc/rc.d/rc5.d/` directory:

```
K05innd -> ../init.d/innd
K05saslauthd -> ../init.d/saslauthd
K10dc_server -> ../init.d/dc_server
K10psacct -> ../init.d/psacct
K10radiusd -> ../init.d/radiusd
K12dc_client -> ../init.d/dc_client
K12Freenw - > ../init.d/Freenw
K12mailman -> ../init.d/mailman
K12mysqld -> ../init.d/mysqld
K15httpd -> ../init.d/httpd
K20netdump-server -> ../init.d/netdump-server
K20rstatd -> ../init.d/rstatd
K20rusersd -> ../init.d/rusersd
K20rwhod -> ../init.d/rwhod
K24irda -> ../init.d/irda
K25squid -> ../init.d/squid
K28amd -> ../init.d/amd
K30spamassassin -> ../init.d/spamassassin
K34dhcrelay -> ../init.d/dhcrelay
K34yppasswdd -> ../init.d/yppasswdd
K35dhcpd -> ../init.d/dhcpd
K35smb -> ../init.d/smb
K35vncserver -> ../init.d/vncserver
```
As illustrated in this listing, none of the scripts that actually start and stop the services are located in the /etc/rc.d/rc5.d/ directory. Rather, all of the files in /etc/rc.d/rc5.d/ are symbolic links pointing to scripts located in the /etc/rc.d/init.d/ directory. Symbolic links are used in each of the rc directories so that the runlevels can be reconfigured by creating, modifying, and deleting the symbolic links without affecting the actual scripts they reference.

The name of each symbolic link begins with either a K or an S. The K links are processes that are killed on that runlevel, while those beginning with an S are started.

The init command first stops all of the K symbolic links in the directory by issuing the /etc/rc.d/init.d/ <command> stop command, where <command> is the process to be killed. It then starts all of the S symbolic links by issuing /etc/rc.d/init.d/ <command> start.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>After the system is finished booting, it is possible to log in as root and execute these same scripts to start and stop services. For instance, the command /etc/rc.d/init.d/httpd stop stops the Apache HTTP Server.</td>
</tr>
</tbody>
</table>

Each of the symbolic links are numbered to dictate start order. The order in which the services are started or stopped can be altered by changing this number. The lower the number, the earlier it is started. Symbolic links with the same number are started alphabetically.

<table>
<thead>
<tr>
<th>Note</th>
</tr>
</thead>
<tbody>
<tr>
<td>One of the last things the init program executes is the /etc/rc.d/rc.local file. This file is useful for system customization. Refer to Section F.3, “Running Additional Programs at Boot Time” for more information about using the rc.local file.</td>
</tr>
</tbody>
</table>

After the init command has progressed through the appropriate rc directory for the runlevel, Upstart forks an /sbin/mingetty process for each virtual console (login prompt) allocated to the runlevel by the job definition in the /etc/event.d directory. Runlevels 2 through 5 have all six virtual consoles, while runlevel 1 (single user mode) has one, and runlevels 0 and 6 have none. The /sbin/mingetty process opens communication pathways to tty devices, sets their modes, prints the login prompt, accepts the user's username and password, and initiates the login process.

In runlevel 5, Upstart runs a script called /etc/X11/prefdm. The prefdm script executes the preferred X display manager — gdm, kdm, or xdm, depending on the contents of the /etc/sysconfig/desktop file.

Once finished, the system operates on runlevel 5 and displays a login screen.

---

2 Refer to the Fedora Deployment Guide for more information about tty devices.
3 Refer to the Fedora Deployment Guide for more information about display managers.
F.2.5. Job definitions

Previously, the sysvinit package provided the init daemon for the default configuration. When the system started, this init daemon ran the /etc/inittab script to start system processes defined for each runlevel. The default configuration now uses an event-driven init daemon provided by the Upstart package. Whenever particular events occur, the init daemon processes jobs stored in the /etc/event.d directory. The init daemon recognizes the start of the system as such an event.

Each job typically specifies a program, and the events that trigger init to run or to stop the program. Some jobs are constructed as tasks, which perform actions and then terminate until another event triggers the job again. Other jobs are constructed as services, which init keeps running until another event (or the user) stops it.

For example, the /etc/events.d/tty2 job is a service to maintain a virtual terminal on tty2 from the time that the system starts until the system shuts down, or another event (such as a change in runlevel) stops the job. The job is constructed so that init will restart the virtual terminal if it stops unexpectedly during that time:

```
# tty2 - getty
#
# This service maintains a getty on tty2 from the point the system is
# started until it is shut down again.

start on stopped rc2
start on stopped rc3
start on stopped rc4
start on started prefdm

stop on runlevel 0
stop on runlevel 1
stop on runlevel 6

respawn
exec /sbin/mingetty tty2
```

F.3. Running Additional Programs at Boot Time

The /etc/rc.d/rc.local script is executed by the init command at boot time or when changing runlevels. Adding commands to the bottom of this script is an easy way to perform necessary tasks like starting special services or initialize devices without writing complex initialization scripts in the /etc/rc.d/init.d/ directory and creating symbolic links.

The /etc/rc.serial script is used if serial ports must be setup at boot time. This script runs setserial commands to configure the system's serial ports. Refer to the setserial man page for more information.

F.4. SysV Init Runlevels

The SysV init runlevel system provides a standard process for controlling which programs init launches or halts when initializing a runlevel. SysV init was chosen because it is easier to use and more flexible than the traditional BSD-style init process.

The configuration files for SysV init are located in the /etc/rc.d/ directory. Within this directory, are the rc, rc.local, rc.sysinit, and, optionally, the rc.serial scripts as well as the following directories:
The *init.d/* directory contains the scripts used by the */sbin/init* command when controlling services. Each of the numbered directories represent the six runlevels configured by default under Fedora.

### F.4.1. Runlevels

The idea behind SysV init runlevels revolves around the idea that different systems can be used in different ways. For example, a server runs more efficiently without the drag on system resources created by the X Window System. Or there may be times when a system administrator may need to operate the system at a lower runlevel to perform diagnostic tasks, like fixing disk corruption in runlevel 1.

The characteristics of a given runlevel determine which services are halted and started by *init*. For instance, runlevel 1 (single user mode) halts any network services, while runlevel 3 starts these services. By assigning specific services to be halted or started on a given runlevel, *init* can quickly change the mode of the machine without the user manually stopping and starting services.

The following runlevels are defined by default under Fedora:

- **0** — Halt
- **1** — Single-user text mode
- **2** — Not used (user-definable)
- **3** — Full multi-user text mode
- **4** — Not used (user-definable)
- **5** — Full multi-user graphical mode (with an X-based login screen)
- **6** — Reboot

In general, users operate Fedora at runlevel 3 or runlevel 5 — both full multi-user modes. Users sometimes customize runlevels 2 and 4 to meet specific needs, since they are not used.

The default runlevel for the system is listed in */etc/init.tab*. To find out the default runlevel for a system, look for the line similar to the following near the bottom of */etc/init.tab*:

```
id:5:initdefault:
```

The default runlevel listed in this example is five, as the number after the first colon indicates. To change it, edit */etc/init.tab* as root.
### Warning

Be very careful when editing `/etc/inittab`. Simple typos can cause the system to become unbootable. If this happens, either use a boot diskette, enter single-user mode, or enter rescue mode to boot the computer and repair the file.

For more information on single-user and rescue mode, refer to the chapter titled *Basic System Recovery* in the *Fedora Deployment Guide*.

It is possible to change the default runlevel at boot time by modifying the arguments passed by the boot loader to the kernel. For information on changing the runlevel at boot time, refer to *Section E.8, “Changing Runlevels at Boot Time”*.

### F.4.2. Runlevel Utilities

One of the best ways to configure runlevels is to use an *initscript utility*. These tools are designed to simplify the task of maintaining files in the SysV init directory hierarchy and relieves system administrators from having to directly manipulate the numerous symbolic links in the subdirectories of `/etc/rc.d/`.

Fedora provides three such utilities:

- `/sbin/chkconfig` — The `/sbin/chkconfig` utility is a simple command line tool for maintaining the `/etc/rc.d/init.d/` directory hierarchy.

- `/usr/sbin/ntsysv` — The ncurses-based `/sbin/ntsysv` utility provides an interactive text-based interface, which some find easier to use than `chkconfig`.

- Services Configuration Tool — The graphical Services Configuration Tool (`system-config-services`) program is a flexible utility for configuring runlevels.

Refer to the chapter titled *Controlling Access to Services* in the *Fedora Deployment Guide* for more information regarding these tools.

### F.5. Shutting Down

To shut down Fedora, the root user may issue the `/sbin/shutdown` command. The `shutdown` man page has a complete list of options, but the two most common uses are:

```
/sbin/shutdown -h now
```

and

```
/sbin/shutdown -r now
```

After shutting everything down, the `-h` option halts the machine, and the `-r` option reboots.
PAM console users can use the `reboot` and `halt` commands to shut down the system while in runlevels 1 through 5. For more information about PAM console users, refer to the Fedora Deployment Guide.

If the computer does not power itself down, be careful not to turn off the computer until a message appears indicating that the system is halted.

Failure to wait for this message can mean that not all the hard drive partitions are unmounted, which can lead to file system corruption.
Appendix G. Logging the Installation

Anaconda tracks all of its activities in logs. This includes:

- Changing installation steps. The steps roughly correspond to the different screens in the graphical installer.
- Detection and manipulation of storage devices.
- Installation media detection.
- Network initialization.
- Kernel messages
- Calls to critical methods within anaconda.
- Calls to external programs.

G.1. Log files and formats

G.1.1. Logging on the installed system

During the installation, logs are stored in the /tmp directory. After the installation, the files can be found in the /var/log/anaconda directory. Another set of logs is stored in the /root directory of the target filesystem, and can be found at /mnt/sysimage/root during the installation. Some logs are also written to the virtual terminals.

Table G.1. anaconda log files

<table>
<thead>
<tr>
<th>Filename</th>
<th>TTY</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>anaconda.log</td>
<td>/dev/tty3</td>
<td>General installation information, including the step changes.</td>
</tr>
<tr>
<td>storage.log</td>
<td>/dev/tty3</td>
<td>Detection and manipulation of storage devices, including RAID, LVM, and partitioning actions.</td>
</tr>
<tr>
<td>program.log</td>
<td></td>
<td>Calls to external programs, and their output.</td>
</tr>
<tr>
<td>syslog</td>
<td>/dev/tty4</td>
<td>Messages from the kernel and external programs, such as NetworkManager.</td>
</tr>
<tr>
<td>yum.log</td>
<td></td>
<td>Yum’s internal log.</td>
</tr>
</tbody>
</table>

G.2. Remote logging with rsyslog

<table>
<thead>
<tr>
<th>Filename</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>install.log</td>
<td>The log of the package installation process</td>
</tr>
<tr>
<td>install.log.syslog</td>
<td>Messages from installation chroot logged through the system's syslog. Mostly information about users and groups created during yum’s package installation.</td>
</tr>
</tbody>
</table>
G.3. Remote logging via virtio
Appendix H. Other Technical Documentation

To learn more about anaconda, the Fedora installation program, visit the project Web page: http://www.fedoraproject.org/wiki/Anaconda.

Both anaconda and Fedora systems use a common set of software components. For detailed information on key technologies, refer to the Web sites listed below:

Boot Loader
Fedora uses the GRUB boot loader. Refer to http://www.gnu.org/software/grub/ for more information.

Disk Partitioning
Fedora uses parted to partition disks. Refer to http://www.gnu.org/software/parted/ for more information.

Storage Management
Logical Volume Management (LVM) provides administrators with a range of facilities to manage storage. By default, the Fedora installation process formats drives as LVM volumes. Refer to http://www.tldp.org/HOWTO/LVM-HOWTO/ for more information.

Audio Support
The Linux kernel used by Fedora incorporates PulseAudio audio server. For more information about PulseAudio, refer to the project documentation: http://www.pulseaudio.org/wiki/Documentation.

Graphics System
Both the installation system and Fedora use the Xorg suite to provide graphical capabilities. Components of Xorg manage the display, keyboard and mouse for the desktop environments that users interact with. Refer to http://www.x.org/ for more information.

Remote Displays
Fedora and anaconda include VNC (Virtual Network Computing) software to enable remote access to graphical displays. For more information about VNC, refer to the documentation on the RealVNC Web site: http://www.realvnc.com/documentation.html.

Command-line Interface
By default, Fedora uses the GNU bash shell to provide a command-line interface. The GNU Core Utilities complete the command-line environment. Refer to http://www.gnu.org/software/bash/bash.html for more information on bash. To learn more about the GNU Core Utilities, refer to http://www.gnu.org/software/coreutils/.

Remote System Access
Fedora incorporates the OpenSSH suite to provide remote access to the system. The SSH service enables a number of functions, which include access to the command-line from other systems, remote command execution, and network file transfers. During the installation process anaconda may use the scp feature of OpenSSH to transfer crash reports to remote systems. Refer to the OpenSSH Web site for more information: http://www.openssh.com/.

Access Control
SELinux provides Mandatory Access Control (MAC) capabilities that supplement the standard Linux security features. Refer to the SELinux Project Pages for more information: http://docs.fedoraproject.org/selinux-guide.
Appendix H. Other Technical Documentation

Firewall
The Linux kernel used by Fedora incorporates the netfilter framework to provide firewall features. The Netfilter project website provides documentation for both netfilter, and the iptables administration facilities: http://netfilter.org/documentation/index.html.

Software Installation
Fedora uses yum to manage the RPM packages that make up the system. Refer to http://docs.fedoraproject.org/yum/ for more information.

Virtualization
Virtualization provides the capability to simultaneously run multiple operating systems on the same computer. Fedora also includes tools to install and manage the secondary systems on a Fedora host. You may select virtualization support during the installation process, or at any time thereafter. Refer to the Fedora Virtualization Guide available from http://docs.fedoraproject.org/ for more information.
Appendix I. Contributors and production methods

I.1. Contributors

- **Fabian Affolter**\(^1\) (translator - German)
- **Amanpreet Singh Alam**\(^2\) (translator - Punjabi)
- Jean-Paul Aubry (translator - French)
- David Barzilay (translator - Brazilian Portuguese)
- **Domingo Becker**\(^3\) (translator - Spanish)
- Subhransu Behera (translator - Oriya)
- Michal Bentkowski (translator - Polish)
- Rahul Bhalerao (translator - Marathi)
- Runa Bhattacharjee (translator - Bengali (India))
- **Teta Bilianou**\(^4\) (translator - Greek)
- Vitor Vilas Boas (translator - Brazilian Portuguese)
- Lucas Brausch (translator - German)
- **Hector Daniel Cabrera**\(^5\) (translator - Spanish)
- **David Cantrell**\(^6\) (writer - VNC installation)
- Guido Caruso (translator - Italian)
- Guillaume Chardin (translator - French)
- **Nikos Charonitakis**\(^7\) (translator - Greek)
- Chester Cheng (translator - Chinese (Traditional))
- **Tom K. C. Chiu**\(^8\) (translator - Chinese (Traditional))
- Glaucia Cintra (translator - Brazilian Portuguese)
- Fabien Decroux (translator - French)

---

\(^1\) [http://fedoraproject.org/wiki/User:Fab](http://fedoraproject.org/wiki/User:Fab)
\(^2\) [http://fedoraproject.org/wiki/AmanAlam](http://fedoraproject.org/wiki/AmanAlam)
\(^3\) [http://fedoraproject.org/wiki/User:Beckerde](http://fedoraproject.org/wiki/User:Beckerde)
\(^4\) [http://fedoraproject.org/wiki/TetaBilianou](http://fedoraproject.org/wiki/TetaBilianou)
\(^6\) [https://fedoraproject.org/wiki/DavidCantrell](https://fedoraproject.org/wiki/DavidCantrell)
\(^7\) [http://fedoraproject.org/wiki/NikosCharonitakis](http://fedoraproject.org/wiki/NikosCharonitakis)
\(^8\) [http://fedoraproject.org/wiki/Tomchiukc](http://fedoraproject.org/wiki/Tomchiukc)
Appendix I. Contributors and production methods

- **Hans De Goede** (writer - iSCSI)
- Claudio Rodrigo Pereyra Diaz (translator - Spanish)
- **Piotr Drąg** (translator - Polish)
- **Damien Durand** (translator - French)
- **Stuart Ellis** (writer, editor)
- **Ali Fakoor** (translator - Persian)
- Felix I (translator - Tamil)
- Tony Fu (translator - Chinese (Simplified))
- **Paul W. Fields** (writer, editor)
- Paul Gampe (translator - Japanese)
- Sree Ganesh (translator - Telugu)
- **Dimitris Glezos** (translator - Greek)
- **Guillermo Gómez** (translator - Spanish)
- **Igor Gorbounov** (translator - Russian)
- **Rui Gouveia** (translator - Portuguese)
- Kiyoto James Hashida (translator - Japanese)
- Severin Heiniger (translator - German)
- Xi Huang (translator - Chinese (Simplified))
- Ryuichi Hyugabaru (translator - Japanese)
- Jayaradha N (translator - Tamil)
- Chris Johnson (writer)
- Eunju Kim (translator - Korean)
- Michelle J Kim (translator - Korean)
- **Miloš Komarčević** (translator - Serbian)
• Alexey Kostyuk (translator - Russian)
• Daniela Kugelmann (translator - German)
• Rüdiger Landmann20 (writer, editor)
• Magnus Larsson21 (translator - Swedish)
• Christopherus Laurentius22 (translator - Indonesian)
• Florent Le Coz (translator - French)
• Erick Lemon (writer)
• Andy Liu (translator - Chinese (Traditional))
• Wei Liu (translator - Chinese (Simplified))
• Yelitza Louze (translator - Spanish)
• Gan Lu (translator - Chinese (Simplified))
• Jens Maucher23 (translator - German)
• Igor Miletić24 (translator - Serbian)
• Noriko Mizumoto (translator - Japanese)
• Jeremy W. Mooney (writer)
• Enikő Nagy (translator - Hungarian)
• Igor Nestorović (translator - Serbian)
• David Nalley25 (writer, editor)
• John Nguyen (writer)
• Manuel Ospina (translator - Spanish)
• Janis Ozolins (translator - Latvian)
• Ankit Patel (translator - Gujarati)
• Davidson Paulo26 (translator - Brazilian Portuguese)
• Ani Peter (translator - Malayalam)
• Amitakhya Phukan27 (translator - Assamese)

20 https://fedoraproject.org/wiki/User:Rlandmann
21 http://translate.fedoraproject.org/people/raada
22 https://fedoraproject.org/wiki/ChristopherusLaurentius
23 https://fedoraproject.org/wiki/User:Jensm
24 http://fedoraproject.org/wiki/IgorMiletic
26 http://fedoraproject.org/wiki/User:Dpaulo
27 https://translate.fedoraproject.org/people/aphukan
Appendix I. Contributors and production methods

- **Silvio Pierro**\(^{28}\) (translator - Italian)
- **Micha Pietsch**\(^{29}\) (translator - German)
- José Nuno Pires (translator - Portuguese)
- Piotr Podgórski (translator - Polish)
- Yulia Poyarkova (translator - Russian)
- Shankar Prasad (translator - Kannada)
- Rajesh Ranjan (translator - Hindi)
- **Jack Reed**\(^{30}\) (writer, editor)
- **Tommy Reynolds**\(^{31}\) (writer)
- Tim Richert (translator - German)
- **Dominik Sandjaja**\(^{32}\) (translator - German)
- **Sharuzzaman Ahmat Raslan**\(^{33}\) (translator - Malay)
- **Mohsen Saeedi**\(^{34}\) (translator - Persian)
- **Tian Shixiong**\(^{35}\) (translator - Chinese (Simplified))
- Audrey Simons (translator - French)
- Keld Simonsen (translator - Danish)
- **Jared K. Smith**\(^{36}\) (writer, editor)
- Espen Stefansen (translator - Norwegian Bokmål)
- **Sulyok Péter**\(^{37}\) (translator - Hungarian)
- **Sümegi Zoltán**\(^{38}\) (translator - Hungarian)
- **Francesco Tombolini**\(^{39}\) (translator - Italian)
- Timo Trinks (translator - German)
- **Dimitris Typaldos**\(^{40}\) (translator - Greek)

\(^{28}\) https://fedoraproject.org/wiki/User:Perplex
\(^{29}\) https://fedoraproject.org/wiki/User:Barney
\(^{30}\) https://fedoraproject.org/wiki/User:jjr
\(^{31}\) https://fedoraproject.org/wiki/TommyReynolds
\(^{32}\) http://fedoraproject.org/wiki/DominikSandjaja
\(^{33}\) http://translate.fedoraproject.org/people/szaman
\(^{34}\) https://fedoraproject.org/wiki/User:Saeedi
\(^{35}\) https://fedoraproject.org/wiki/User:Tiansworld
\(^{36}\) https://fedoraproject.org/wiki/User:Jsmith
\(^{37}\) https://fedoraproject.org/wiki/User:Peti
\(^{38}\) https://fedoraproject.org/wiki/User:Zolt73
\(^{39}\) https://fedoraproject.org/wiki/User:Tombo
\(^{40}\) http://fedoraproject.org/wiki/DimitriosTypaldos
Production methods

Writers produce the Install Guide directly in DocBook XML in a revision control repository. They collaborate with other subject matter experts during the beta release phase of Fedora to explain the installation process. The editorial team ensures consistency and quality of the finished guide. At this point, the team of translators produces other language versions of the release notes, and then they become available to the general public as part of Fedora. The publication team also makes the guide, and subsequent errata, available via the Web.
Appendix J. Revision History

Revision 1.0-0  Thu Apr 26 2012  Jack Reed jreed@redhat.com
Updates for Fedora 17
Index

Symbols

/boot/ partition
   recommended partitioning, 98

/root/install.log
   install log file location, 115

/var/ partition
   recommended partitioning, 98

A

adding partitions, 90
   file system type, 92
anacdum.txt, 117
Anaconda, 307
anacconda.log, 117
architecture, 4
   determining, 4
array (see RAID)
automatic partitioning, 82, 82

B

Basic Input/Output System (see BIOS)
   BIOS
      definition of, 295
      (see also boot process)
   BIOS (Basic Input/Output System), 31
BitTorrent, 4
   seeding, 4
boot loader, 81, 103
   (see also GRUB)
   configuration, 103
   GRUB, 103
   installing on boot partition, 106
   MBR, 106
   password, 105
   upgrading, 81
boot loader password, 105
boot loaders, 283
   (see also GRUB)
   definition of, 283
   types of
      GRUB, 283
      yaboot, 283
      z/IPL, 283
boot options, 35
   mediacheck, 35
   serial mode, 35
   UTF-8, 35
   text mode, 35
boot process, 295, 295
   (see also boot loaders)
   chain loading, 283, 284
direct loading, 283, 284
   for x86, 295
   stages of, 295, 295
   /sbin/init command, 298
   boot loader, 296
   EFI shell, 296
   kernel, 297
booting
   emergency mode, 239
   installation program
      x86, AMD64 and Intel 64, 33
      rescue mode, 236
      single-user mode, 238

C
canceling the installation, 39
CD/DVD media
   booting, 31
   downloading, 3
      (see also ISO images)
   making, 7
      (see also ISO images)
   Chain loading, 51, 78, 86, 106
   chkconfig, 303
      (see also services)
clock, 74
clock, 74, 74
   GRUB, 103
   hardware, 29
   time, 74
   time zone, 74
custom consoles, virtual, 45

D

DHCP (Dynamic Host Configuration Protocol), 61
Disk Partitioner
   adding partitions, 90
disk partitioning, 82
disk space, 20
drivers
   adding
      rescue mode, 239
   removing
      rescue mode, 239
   replacing
      rescue mode, 239

DVD
   ATAPI, 39
   IDE, 39
   installation from, 39
   SCSI, 39
Index

E
- EFI shell, 296
  (see also boot process)
- emergency mode, 239

Encryption
  - Backup passphrases
    - Creating backup passphrases, 275
    - Saving backup passphrases, 275
  - Passphrases
    - Saving passphrases, 275
- ext2 (see file systems)
- ext3 (see file systems)
- ext4 (see file systems)
- extended partitions, 263
- Extensible Firmware Interface shell (see EFI shell)

F
- FCoE
  - installation, 52
- feedback
  - contact information for this manual, xiii
- file system
  - formats, overview of, 259
- file system types, 92
- file systems
  - ext2, 39
  - ext3, 39
  - ext4, 39
  - vfat, 39
- firewall
  - documentation, 308
- Firstboot, 217
  - via Kickstart, 165
- FTP
  - installation, 23, 41

G
- GRUB, 103, 283, 296
  (see also boot loaders)
  - additional resources, 293
    - installed documentation, 294
    - useful websites, 294
  - alternatives to, 108
  - boot process, 283, 284
- Changing Runlevels at Boot Time, 293
- changing runlevels with, 288
- commands, 290
- configuration, 103
- configuration file
  - /boot/grub/grub.conf, 291
  - structure, 291
  - definition of, 283
- documentation, 307
- features, 285
- installing, 285
- interfaces, 288
  - command line, 288
  - menu, 288
  - menu entry editor, 288
  - order of, 289
  - menu configuration file, 291
    - directives, 292
    - role in boot process, 296
    - terminology, 286
    - devices, 286
    - files, 287
    - root file system, 288
- grub.conf, 291
  (see also GRUB)

H
- halt, 303
  (see also shutdown)
- Hard disk
  - initializing, 78
  - hard disk
    - basic concepts, 259
    - extended partitions, 263
    - file system formats, 259
    - partition introduction, 261
    - partition types, 262
    - partitioning of, 259
  - hard drive installation, 39
    - preparing for, 25
  - hardware
    - compatibility, 19
    - configuration, 29
  - hostname, 61
  - HTTP
    - installation, 23, 41

I
- init command, 298
  (see also boot process)
- configuration files
  - /etc/inittab, 301
- role in boot process, 298
  (see also boot process)
- runlevels
  - directories for, 301
  - runlevels accessed by, 302
- SysV init
  - definition of, 301
- install log file
  - /root/install.log, 115
installation
  aborting, 39
  disk space, 20
  DVD, 39
  FTP, 23, 41
  GUI, 43
  hard drive, 25, 39
  HTTP, 23, 41
  keyboard navigation, 44
  kickstart (see kickstart installations)
  mediacheck, 35
method
  DVD, 21
  hard drive, 21
  NFS image, 21
  selecting, 20
  URL, 21
  network, 23
  NFS, 23, 40
  server information, 40
partitioning, 87
program
  graphical user interface, 44
  starting, 32
  virtual consoles, 45
serial mode, 35
  UTF-8, 35
starting, 39
text mode, 35
installation method
  selecting, 39
installation program
  x86, AMD64 and Intel 64
  booting, 33
installing packages, 108
IPv4, 61
iscsi
  installation, 52
ISO images
  downloading, 1, 3

K
kernel
  role in boot process, 297
kernel options, 36
keyboard
  configuration, 46
  navigating the installation program using, 44
keymap
  selecting language, 45
  selecting type of keyboard, 46
Kickstart, 136
kickstart
  how the file is found, 190

Kickstart Configurator, 199
%post script, 212
%pre script, 211
authentication options, 207
basic options, 199
boot loader, 202
boot loader options, 202
Display configuration, 209
firewall configuration, 208
installation method selection, 200
interactive, 200
keyboard, 199
language, 199
network configuration, 206
package selection, 210
partitioning, 203
  software RAID, 204
preview, 199
reboot, 200
root password, 199
  encrypt, 199
saving, 213
SELinux configuration, 209
text mode installation, 200
time zone, 199
kickstart file
  %include, 184
  %post, 187
  %pre, 186
  auth, 160
  authconfig, 160
  autopart, 158
  autostep, 160
  bootloader, 162
  CD-ROM-based, 189
clearpart, 162
cmdline, 163
creating, 158
device, 164
diskette-based, 189
driverdisk, 164
firewall, 164
firstboot, 165
flash-based, 189
format of, 157
graphical, 165
halt, 165
ignoredisk, 159
include contents of another file, 184
install, 165
installation methods, 165
iscsi, 166
iscsiname, 167
keyboard, 167
Index

lang, 169
langsamental, 169
logging, 170
logvol, 169
mediacheck, 171, 171, 180
mouse, 171
network, 171
network-based, 189, 190
options, 158
  partitioning examples, 184
package selection specification, 185
part, 174
partition, 174
post-installation configuration, 187
poweroff, 178
pre-installation configuration, 186
raid, 178
reboot, 179
rootpw, 180
selinux, 180
services, 181
shutdown, 181
skipx, 181
sshpw, 181
text, 182
timezone, 182
upgrade, 182
user, 182
vnc, 183
volgroup, 183
what it looks like, 157
xconfig, 183
zerombr, 184
kickstart installations, 157
CD-ROM-based, 189
diskette-based, 189
file format, 157
file locations, 189
flash-based, 189
installation tree, 190
LVM, 169
network-based, 189, 190
starting, 190, 191
  from a boot CD-ROM, 191

understanding, 281
volume group, 281
with kickstart, 169

M
master boot record, 103
Master Boot Record, 235 (see MBR)
reinstalling, 238
MBR
definition of, 295, 295
  (see also boot loaders)
  (see also boot process)
  installing boot loader on, 106
memory testing mode, 139
mirror, 3
modem, 61
mount points
  partitions and, 269
Multipath devices
  Mixing with non-multipath devices, 86

N
network
  installations
    FTP, 41
    HTTP, 41
    NFS, 40
network installation
  preparing for, 23
NFS
  installation, 23, 40
NTFS partitions
  resizing, 2
NTP (Network Time Protocol), 74, 223
ntsysv, 303
  (see also services)

O
OpenSSH, 307
  (see also SSH)
OS/2 boot manager, 106
OS/400, 283
  (see also boot loaders)

P
package groups, 113
packages
  groups, 108
    selecting, 108
  installing, 108
    selecting, 108
parted partitioning utility, 268
partition
extended, 263
partitioning, 87
  automatic, 82
  basic concepts, 259
  creating new, 90
    file system type, 92
  destructive, 265
  extended partitions, 263
  how many partitions, 261, 269
  introduction to, 261
  making room for partitions, 263
  mount points and, 269
  naming partitions, 268
  non-destructive, 266
  numbering partitions, 268
  other operating systems, 269
  primary partitions, 261
  recommended, 98
  types of partitions, 262
  using free space, 264
  using in-use partition, 265
  using unused partition, 264
Partitioning , 87
  adding partitions
    file system type, 92
Passphrases
  Block device encryption passphrases
    Creating backup block device encryption passphrases, 275
    Saving backup block device encryption passphrases, 275
    Saving block device encryption passphrases, 275
password
  boot loader, 105
  setting root, 75
program.log, 117
programs
  running at boot time, 301
PulseAudio, 307
PXE (Pre-boot eXecution Environment), 36
PXE installations
  boot message, custom, 150
  configuration, 147
  overview, 146
  performing, 151
  setting up the network server, 146
R
RAID
  hardware, 19
  kickstart installations, 178
    Kickstart Configurator, 204
  software, 19
  system unbootable after disk failure, 286
  trouble booting from drive attached to RAID card, 117
rc.local
  modifying, 301
rc.serial , 301
(see also setserial command)
re-installation, 243
removing
  Fedora
    from x86-based systems, 245
rescue discs, 140
rescue mode, 108, 140
  definition of, 236
  utilities available, 237
root / partition
  recommended partitioning, 98
root password, 75
runlevel 1, 238
runlevels (see init command)
  changing with GRUB, 288
  configuration of, 303
  (see also services)
S
scp, 307
(see also SSH)
screenshots
  during installation, 45
selecting
  packages, 108
SELinux
  documentation, 307
serial console, 132
serial ports (see setserial command)
services
  configuring with chkconfig , 303
  configuring with ntsysv , 303
  configuring with Services Configuration Tool , 303
Services Configuration Tool , 303
(see also services)
setserial command
  configuring, 301
shutdown, 303
(see also halt)
single-user mode, 238
ssh
  starting ssh at boot time, 135
SSH (Secure SHell)
  documentation, 307
starting
  installation, 32, 39
steps
booting with CD-ROM or DVD, 21
disk space, 20
hardware compatibility, 19
storage devices
  basic storage devices, 47
  specialized storage devices, 47
storage.log, 117
swap file
  upgrade, 244
swap partition
  recommended partitioning, 98
syslog, 117, 135
system recovery, 235
  adding drivers, 239
  common problems, 235
  forgetting the root password, 235
  hardware/software problems, 235
  reinstalling the boot loader, 238
  unable to boot into Fedora, 235
  removing drivers, 239
  replacing drivers, 239
system-config-kickstart (see Kickstart Configurator)
SysV init (see init command)

T
text interface, 132
tftp, 150
time zone
  configuration, 74
traceback messages
  saving traceback messages without removable media, 119, 119
troubleshooting, 117
  after the installation, 122
  Apache HTTP Server stops responding during startup, 127
  booting into a graphical environment, 124
  booting into GNOME or KDE, 124
  booting into the X Window System, 124
  graphical GRUB screen, 122
  GRUB command line, 123
  logging in, 125
  printers, 126
  RAM not recognized, 126
  Sendmail stops responding during startup, 127
  X (X Window System), 124
  X server crashes, 125
beginning the installation, 118
  frame buffer, disabling, 118
  GUI installation method unavailable, 118
  booting, 117
  RAID cards, 117
signal 11 error, 118
during the installation, 119
  completing partitions, 122
  No devices found to install Fedora error message, 119
  partition tables, 122, 122
  saving traceback messages without removable media, 119
  using remaining hard drive space, 122
DVD failure
  DVD verification, 35

U
UEFI (Unified Extensible Firmware Interface), 31
  uninstalling
    from x86-based systems, 245
Update System, 227, 227
upgrade, 243
  adding a swap file, 244
USB flash media
  downloading, 3
  making, 7
USB media
  booting, 31
user interface, graphical
  installation program, 44

V
vfat (see file systems)
virtual consoles, 45
Virtualization
  documentation, 308
VNC (Virtual Network Computing), 134
  documentation, 307
  enabling, 134
  installing client, 134
  listening mode, 135

X
Xorg, 307

Y
yaboot, 283
  (see also boot loaders)
yum, 227
  documentation, 308
yum.log, 117

Z
z/IPL, 283
  (see also boot loaders)