



Mac OS X Server

Getting Started

For Version 10.4 or Later

🍏 Apple Computer, Inc.
© 2005 Apple Computer, Inc. All rights reserved.

The owner or authorized user of a valid copy of Mac OS X Server software may reproduce this publication for the purpose of learning to use such software. No part of this publication may be reproduced or transmitted for commercial purposes, such as selling copies of this publication or for providing paid-for support services.

Every effort has been made to ensure that the information in this manual is accurate. Apple Computer, Inc., is not responsible for printing or clerical errors.

Apple
1 Infinite Loop
Cupertino, CA 95014-2084
408-996-1010
www.apple.com

The Apple logo is a trademark of Apple Computer, Inc., registered in the U.S. and other countries. Use of the “keyboard” Apple logo (Option-Shift-K) for commercial purposes without the prior written consent of Apple may constitute trademark infringement and unfair competition in violation of federal and state laws.

Apple, the Apple logo, AirPort, AppleShare, AppleTalk, FireWire, iBook, iMac, iPod, Keychain, LaserWriter, Mac, Mac OS, Macintosh, Power Mac, Power Macintosh, Quartz, QuickTime, WebObjects, and Xserve are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. Apple Remote Desktop, eMac, Finder, Xcode, and Xgrid are trademarks of Apple Computer, Inc.

Adobe and PostScript are trademarks of Adobe Systems Incorporated.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

Other company and product names mentioned herein are trademarks of their respective companies. Mention of third-party products is for informational purposes only and constitutes neither an endorsement nor a recommendation. Apple assumes no responsibility with regard to the performance or use of these products.

034-2651-A/03-24-05

Contents

Preface	9 About This Guide
	9 What's New in Version 10.4
	9 High-Performance Computing
	9 User Access Management
	11 Server Administration
	11 Collaboration Services
	12 What's in This Guide
	12 Part I: Introduction to Mac OS X Server
	12 Part II: Installation and Initial Setup
	12 Glossary
	12 Using Onscreen Help
	13 The Mac OS X Server Suite
	14 Getting Documentation Updates
	14 Getting Additional Information

Part I Introduction to Mac OS X Server

Chapter 1	19 Mac OS X Server in Action
	20 Departments and Workgroups
	23 Small and Medium Businesses
	25 Higher-Education Facilities
	27 K–12 Labs and Classrooms
	29 Computational Clustering
	31 Data Centers
Chapter 2	33 Inside Mac OS X Server
	33 Core System Services
	34 Open Directory
	34 Using Mac OS X Server Directories
	34 Using Non-Apple Directories
	35 Directory Management
	35 Search Policies

36	Authentication
36	Single Sign-On
37	Discovery of Network Services
37	User Management
37	User Accounts
37	Group Accounts
38	Computer Lists
38	Home Directories
38	Macintosh User Management
40	Windows User Management
40	System Image Services
41	NetBoot
41	Network Install
41	Software Update Service
42	File Services
42	Sharing
43	Apple File Service
43	Windows Services
44	Network File System (NFS) Service
44	File Transfer Protocol (FTP)
45	Web-based Distributed Authoring and Versioning (WebDAV)
45	Print Service
46	Web Service
47	Mail Service
48	Network Services
48	DHCP
48	DNS
49	Firewall
49	NAT
49	VPN
50	Gateway Setup Assistant
50	IP Failover
51	Media Streaming and Broadcasting
51	Application Server Support
52	Apache Tomcat
52	JBoss
53	WebObjects
53	Collaboration Services
54	Integrating Into Existing Environments
54	High Availability
55	High-Performance Computing
55	Server Administration
56	Migrating and Upgrading

Chapter 3

- 57 **Server Administration**
- 57 Using the Administration Tools
- 58 Computers You Can Use to Administer a Server
- 59 Setting Up an Administrator Computer
- 59 Using a Non-Mac OS X Computer for Administration
- 60 Installer
- 60 Server Assistant
- 60 Directory Access
- 61 Workgroup Manager
- 61 Opening and Authenticating in Workgroup Manager
- 62 Administering Accounts
- 63 Defining Managed Preferences
- 64 Working With Directory Data
- 65 Managing Sharing
- 66 Configuring Managed Network Views
- 67 Customizing the Workgroup Manager Environment
- 67 Server Admin
- 68 Opening and Authenticating in Server Admin
- 68 Working With Specific Servers
- 70 Administering Services
- 71 Controlling Access to Services
- 71 Using SSL for Remote Server Administration
- 72 Customizing the Server Admin Environment
- 72 Gateway Setup Assistant
- 73 System Image Management
- 73 Server Monitor
- 74 Media Streaming Management
- 75 Apple Remote Desktop
- 75 Command-Line Tools
- 76 Xgrid Admin
- 76 Working With Pre-Version 10.4 Computers From Version 10.4 Servers

Part II

Installation and Initial Setup

Chapter 4

- 79 **Installation and Setup Overview**
- 79 Planning
- 80 Installing Server Software
- 80 Upgrading and Migrating
- 81 Local Installation From the Server Install Discs
- 81 Remote Installation From the Server Install Discs
- 83 Automating Server Installation With a Disk Image
- 84 Initial Server Setup

- 84 Settings Established During Initial Server Setup
- 85 Setting Up Servers Interactively
- 86 Automating Server Setup
- 88 Setting Up Services
- 89 Keeping Current

Chapter 5

- 91 **Before You Begin**
- 91 Setting Up a Planning Team
- 92 Identifying the Servers You'll Need to Set Up
- 92 Determining Services to Host on Each Server
- 94 Define a Migration Strategy
- 94 Upgrading and Migrating From an Earlier Version of Mac OS X Server
- 94 Migrating From Windows NT
- 95 Defining an Integration Strategy
- 95 Defining Physical Infrastructure Requirements
- 96 Defining Server Setup Infrastructure Requirements
- 97 Making Sure Required Server Hardware Is Available
- 97 Minimizing the Need to Relocate Servers After Setup
- 98 Changing the Server's Host Name After Setup
- 98 Changing the Server's IP Address After Setup
- 98 Determining the Installation and Setup Strategy to Use
- 98 Collecting and Organizing Information

Chapter 6

- 99 **Installing Server Software**
- 100 Understanding System Requirements for Installing Mac OS X Server
- 100 Information You Need
- 100 Using the Server Installation Discs
- 100 Upgrading and Migrating
- 101 Preparing Discs for Installing Mac OS X Server
- 102 Hardware-Specific Instructions for Installing Mac OS X Server
- 102 Identifying Remote Servers When Installing Mac OS X Server
- 103 Connecting to the Network During Installation
- 103 Installing Server Software Interactively From the Install Discs
- 103 Using Installer to Install Locally From the Install Discs
- 104 Using Server Assistant to Install Remotely From the Install Discs
- 106 Installing Server Software on a Computer With Mac OS X Version 10.4 Preinstalled
- 106 Automating Server Software Installation With a Disk Image
- 107 Using the installer Command-Line Tool to Install Server Software
- 109 Installing Multiple Servers

Chapter 7

- 111 **Initial Server Setup**
- 112 Information You Need
- 112 Saving Setup Data

116	Specifying Initial Open Directory Usage
119	Connecting to the Network During Initial Server Setup
119	Configuring Servers With Multiple Ethernet Ports
119	Using Interactive Server Setup
120	Setting Up a Local Server Interactively
120	Postponing Local Server Setups Following Installation
120	Setting Up a Remote Server Interactively
121	Setting Up Multiple Remote Servers Interactively in a Batch
123	Setting Up Multiple Remote Servers Interactively One at a Time
124	Using Automatic Server Setup
124	Setting Up Servers Automatically Using Data Saved in a File
127	Setting Up Servers Automatically Using Data Saved in a Directory
130	Determining the Status of Setups
130	Using the Destination Pane for Setup Status Information
130	Handling Setup Failures
131	Handling Setup Warnings
131	Getting Upgrade Installation Status Information
131	Setting Up Services
131	Setting Up Open Directory
132	Setting Up User Management
132	Setting Up File Services
133	Setting Up Print Service
133	Setting Up Web Service
134	Setting Up Mail Service
134	Setting Up Network Services
135	Setting Up System Image and Software Update Services
135	Setting Up Media Streaming and Broadcasting
135	Setting Up an Application Server
136	Setting Up a WebObjects Server
136	Setting Up Collaboration Service

Appendix A	137 Mac OS X Server Worksheet
-------------------	--------------------------------------

Appendix B	149 Setup Example
	149 Mac OS X Server in a Small Business
	150 How to Set Up the Server

Glossary	157
-----------------	------------

Index	169
--------------	------------

About This Guide

This guide provides an orientation to the features and initial setup of Mac OS X Server version 10.4.

The guide will help you prepare your server to start serving your users and your business needs.

What's New in Version 10.4

Mac OS X Server version 10.4 offers major enhancements in the following key areas:

- High-performance computing
- User access management
- Server administration
- Collaboration services

High-Performance Computing

Mac OS X Server offers a high-performance, cost-effective approach to computationally intensive activities:

- **Xgrid service.** Xgrid computational service lets you achieve supercomputer performance levels by distributing computations over collections of dedicated or shared Mac OS X computers. The Xgrid cluster controller provides centralized access to the distributed computing pool, referred to as a computational cluster.
- **64-bit computing.** Support for 64-bit processing includes 64-bit addressable memory and the ability to run 64- and 32-bit applications simultaneously.
- **Accelerated networking.** Link aggregation lets you configure several physical network links as a single logical link to improve the capacity of network connections. You can also take advantage of jumbo frames and IP over FireWire to optimize network transmissions.

User Access Management

Numerous new features in version 10.4 enhance your ability to both facilitate and manage user access to services:

- **Access Control Lists (ACLs).** ACLs give you a way to craft share point, folder, and file access permissions with a high degree of precision. A wide range of permissions can be assigned to individual users and to groups, which can be nested. In addition, you can use inheritance to propagate permissions through a file system hierarchy.
- **Nested groups.** A nested group is a group that's a member of another group. Nesting groups lets you manage groups of users at both a global level (when you want to influence all members of a group) and at a smaller, more focused level (when you want to influence only certain members of a group).
- **Unified locking.** Mac OS X Server unifies file locking across AFP and SMB/CIFS protocols. This feature lets users working on multiple platforms simultaneously share files without worrying about file corruption.
- **Service access.** You can specify which users and groups can use services hosted by a server.
- **Pervasive Kerberos support.** The following services on Mac OS X Server now support Kerberos authentication: AFP, mail, File Transfer Protocol (FTP), Secure Shell (SSH), login window, LDAPv3, Virtual Private Network (VPN), screen saver, and Apache (via the SPNEGO protocol).
- **Network browsing.** You can set up managed network views, which are custom views that users see when they select the Network icon in the sidebar of a Finder window. A managed network view is one or more network neighborhoods, which appear in the Finder as folders. Each folder contains a list of resources that an administrator has associated with the view. Managed network views offer a meaningful way to present network resources. You can create multiple views for different client computers. And because the views are stored using Open Directory, a computer's network view is automatically available when a user logs in.
- **Site-to-site VPN.** Site-to-site VPN connects two networks. It offers a secure connection that's easy to establish when it's necessary to set up a network at another site, as when a business expands. Site-to-site VPN makes both networks appear as one to users working at either site.
- **Mobility.** Users with portable computers can use trusted binding to make sure that servers accessed as they move around are trustworthy. Trusted binding offers a way for a client computer to authenticate to an LDAP server and for the LDAP server to authenticate to the client.
- **Trusted directory binding.** Trusted directory binding, also called authenticated directory binding, provides an authenticated connection between a client computer and an LDAP directory on Mac OS X Server. Because the client computer authenticates the LDAP server before connecting to it, a malicious user can't control the client computer by interposing a counterfeit, unauthenticated LDAP server.
- **Importing accounts.** The performance of importing accounts into an LDAPv3 directory has been greatly improved. In addition, you can now import password policy settings, control whether presets are applied during import, and specify the amount of information logged.

Server Administration

Mac OS X Server management continues to become easier and more effective:

- **Open Directory schema replication.** You can now store LDAP schema in the directory, letting you add new schema without manually copying configuration files. Changes are automatically propagated from the Open Directory master to all its replicas.
- **Preference editor.** If you want fine-grain control of preference settings, you can work with preference manifests using Workgroup Manager's new preference editor. Preference manifests are files that describe the structure and values of an application's or utility's preferences. The preference editor lets you work with preference manifests for the predefined preferences or add new preference manifests for applications and utilities of interest.
- **Junk mail and virus filtering.** Mail service protects users from junk mail and other annoying or unauthorized messages. You can define filters that help minimize junk mail and viruses, filter out unsolicited commercial email, and detect messages that contain particular content. Junk mail filtering, based on the powerful SpamAssassin, includes an autolearning option.
- **Network gateway setup.** A new application, Gateway Setup Assistant, automates the configuration of a simple gateway between the local network and the Internet. A gateway lets you share the server's Internet connection among computers on the local area network (LAN). Gateway Setup Assistant configures Dynamic Host Configuration Protocol (DHCP), Network Address Translation (NAT), firewall, DNS, and VPN services automatically.
- **Secure Sockets Layer (SSL) certificate management.** Server Admin makes it easy to manage SSL certificates that can be used by mail, web, Open Directory, and other services that support them. You can create a self-signed certificate, and generate a Certificate Signing Request (CSR) to obtain an SSL certificate from an issuing authority and install the certificate.

Collaboration Services

Collaboration services promote interactions among users, facilitating teamwork and productivity. Mac OS X Server continues to provide such collaborative support as mailing list management, group account and folder management, and cross-platform file sharing. Two new collaborative services have been added for version 10.4:

- **Weblog service.** Mac OS X Server provides a multiuser weblog server that complies with the RSS and Atom XML standards. Weblog service supports Open Directory authentication. For additional safety, users can access Weblog service using a website that's SSL enabled.
- **iChat service.** Mac OS X Server provides instant messaging for Macintosh, Windows, and Linux users. User authentication is integrated into Open Directory, and setup and administration of iChat service is done using the graphical Server Admin application.

What's in This Guide

This guide is organized into two parts plus a glossary.

Part I: Introduction to Mac OS X Server

Read the chapters in this part to familiarize yourself with Mac OS X Server usage scenarios, services, and administration.

Part II: Installation and Initial Setup

The chapters in this part tell you how to install Mac OS X Server software and how to set up a server for the first time.

Part II includes two appendixes.

- Use Appendix A, *Mac OS X Server Worksheet*, to record information you'll need when you install and set up Mac OS X Server.
- Appendix B contains a setup example illustrating how you might install Mac OS X Server and perform initial server setup in a small business.

Glossary

Refer to the glossary when you want a brief definition of the terms used in this guide.

Note: Because Apple frequently releases new versions and updates to its software, images shown in this book may be different from what you see on your screen.

Using Onscreen Help

You can view instructions and other useful information from this and other documents in the server suite by using onscreen help.

On a computer running Mac OS X Server, you can access onscreen help after opening Workgroup Manager or Server Admin. From the Help menu, select one of the options:

- *Workgroup Manager Help* or *Server Admin Help* displays information about the application.
- *Mac OS X Server Help* displays the main server help page, from which you can search or browse for server information.
- *Documentation* takes you to www.apple.com/server/documentation, from which you can download server documentation.

You can also access onscreen help from the Finder or other applications on a server or on an administrator computer. (An administrator computer is a Mac OS X computer with server administration software installed on it.) Use the Help menu to open Help Viewer, then choose Library > Mac OS X Server Help.

To see the latest server help topics, make sure the server or administrator computer is connected to the Internet while you're using Help Viewer. Help Viewer automatically retrieves and caches the latest server help topics from the Internet. When not connected to the Internet, Help Viewer displays cached help topics.

The Mac OS X Server Suite

The Mac OS X Server documentation includes a suite of guides that explain the services and provide instructions for configuring, managing, and troubleshooting the services. All of the guides are available in PDF format from:

www.apple.com/server/documentation/

This guide ...	tells you how to:
<i>Mac OS X Server Getting Started for Version 10.4 or Later</i>	Install Mac OS X Server and set it up for the first time.
<i>Mac OS X Server Upgrading and Migrating to Version 10.4 or Later</i>	Use data and service settings that are currently being used on earlier versions of the server.
<i>Mac OS X Server User Management for Version 10.4 or Later</i>	Create and manage users, groups, and computer lists. Set up managed preferences for Mac OS X clients.
<i>Mac OS X Server File Services Administration for Version 10.4 or Later</i>	Share selected server volumes or folders among server clients using these protocols: AFP, NFS, FTP, and SMB/CIFS.
<i>Mac OS X Server Print Service Administration for Version 10.4 or Later</i>	Host shared printers and manage their associated queues and print jobs.
<i>Mac OS X Server System Image and Software Update Administration for Version 10.4 or Later</i>	Use NetBoot and Network Install to create disk images from which Macintosh computers can start up over the network. Set up a software update server for updating client computers over the network.
<i>Mac OS X Server Mail Service Administration for Version 10.4 or Later</i>	Set up, configure, and administer mail services on the server.
<i>Mac OS X Server Web Technologies Administration for Version 10.4 or Later</i>	Set up and manage a web server, including WebDAV, WebMail, and web modules.
<i>Mac OS X Server Network Services Administration for Version 10.4 or Later</i>	Set up, configure, and administer DHCP, DNS, VPN, NTP, IP firewall, and NAT services on the server.
<i>Mac OS X Server Open Directory Administration for Version 10.4 or Later</i>	Manage directory and authentication services.
<i>Mac OS X Server QuickTime Streaming Server Administration for Version 10.4 or Later</i>	Set up and manage QuickTime streaming services.
<i>Mac OS X Server Windows Services Administration for Version 10.4 or Later</i>	Set up and manage services including PDC, BDC, file, and print for Windows computer users.
<i>Mac OS X Server Migrating from Windows NT for Version 10.4 or Later</i>	Move accounts, shared folders, and services from Windows NT servers to Mac OS X Server.

This guide ...	tells you how to:
<i>Mac OS X Server Java Application Server Administration For Version 10.4 or Later</i>	Configure and administer a JBoss application server on Mac OS X Server.
<i>Mac OS X Server Command-Line Administration for Version 10.4 or Later</i>	Use commands and configuration files to perform server administration tasks in a UNIX command shell.
<i>Mac OS X Server Collaboration Services Administration for Version 10.4 or Later</i>	Set up and manage Weblog, iChat, and other services that facilitate interactions among users.
<i>Mac OS X Server High Availability Administration for Version 10.4 or Later</i>	Manage link aggregation, load balancing, and other hardware and software configurations to ensure high availability of Mac OS X Server services.
<i>Mac OS X Server Xgrid Administration for Version 10.4 or Later</i>	Manage computational Xserve clusters using the Xgrid application.
<i>Mac OS X Server Glossary: Includes Terminology for Mac OS X Server, Xserve, Xserve RAID, and Xsan</i>	Interpret terms used for server and storage products.

Getting Documentation Updates

Periodically, Apple posts new onscreen help topics, revised guides, and solution papers. The new help topics include updates to the latest guides.

- To view new onscreen help topics, make sure your server or administrator computer is connected to the Internet and click the Late-Breaking News link on the main Mac OS X Server help page.
- To download the latest guides and solution papers in PDF format, go to the Mac OS X Server documentation webpage: www.apple.com/server/documentation.

Getting Additional Information

For more information, consult these resources:

Read Me documents—important updates and special information. Look for them on the server discs.

Mac OS X Server website (www.apple.com/macosx/server/)—gateway to extensive product and technology information.

Apple Service & Support website (www.apple.com/support/)—access to hundreds of articles from Apple's support organization.

Apple customer training (train.apple.com/)—instructor-led and self-paced courses for honing your server administration skills.

Apple discussion groups (discussions.info.apple.com/)—a way to share questions, knowledge, and advice with other administrators.

Apple mailing list directory (www.lists.apple.com/)—subscribe to mailing lists so you can communicate with other administrators using email.

Part I: Introduction to Mac OS X Server

The chapters in this part of the guide introduce you to Mac OS X Server and the applications and tools available for administering its services.

- Chapter 1 Mac OS X Server in Action
- Chapter 2 Inside Mac OS X Server
- Chapter 3 Server Administration

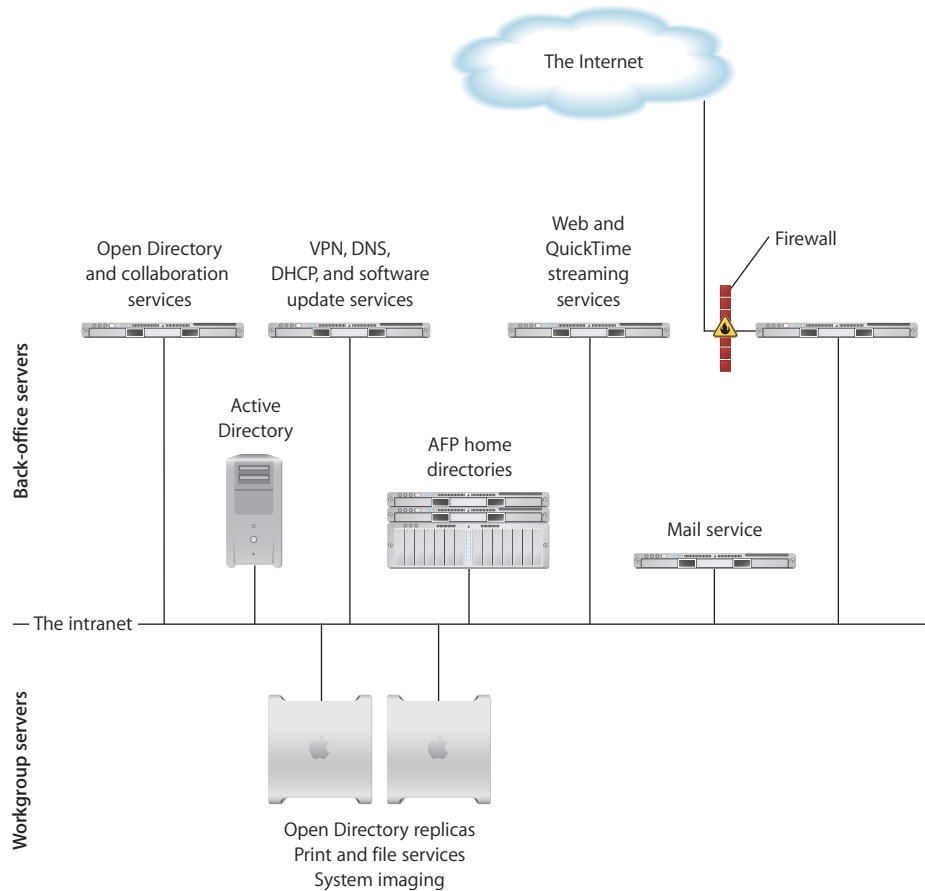
Mac OS X Server addresses the needs of many environments.

This chapter is a brief graphical tour that highlights services and configurations of special interest in some popular scenarios:

- Departments and workgroups
- Small and medium businesses
- Higher-education facilities
- K-12 labs and classrooms
- Computational clustering
- Data centers

Departments and Workgroups

In large organizations, Mac OS X Server helps you support the special needs of departments and workgroups, yet centralize corporate-level services.



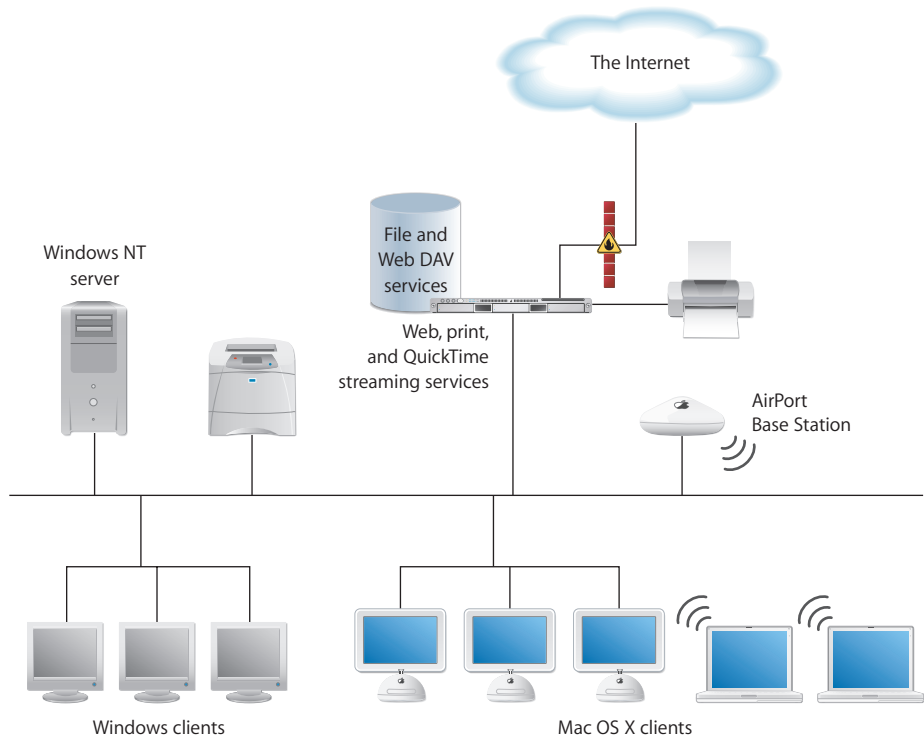
Back-office servers and services address business-wide needs:

- Open Directory lets you manage directory data centrally, but distribute it geographically using replication.
- Collaboration services help employees interact with each other while protecting the content they exchange. For example, the iChat server provides employees with instant messaging that's secure and encrypted.
- Software update service lets you control which updated Apple software to make available to particular employees.
- Other enterprise-level services might include DNS, Dynamic Host Configuration Protocol (DHCP), Virtual Private Network (VPN), mail, web, and streaming.
- The popular open-source Apache HTTP web server is built into Mac OS X Server.
- Mac OS X Server integrates well with existing corporate services, from directory systems such as Active Directory to Simple Network Management Protocol (SNMP) implementations.

Workgroup servers support the unique requirements of individual departments.

- Departmental servers frequently host replicated Open Directory information, file and print services that reflect the workgroup's needs, and system imaging services. System imaging lets you automate the setup of Mac OS X computers by using installation and boot images that reside on the server.
- For departments that use Windows computers, you can provide VPN support and file and printer sharing, Active Directory authentication integration, and Open Directory support for managing computer and group preferences. You can also use a Windows NT Server and Windows NT File Server for Windows home directories.

Here's an example of a departmental server for creative professionals who design and produce video and audio projects.

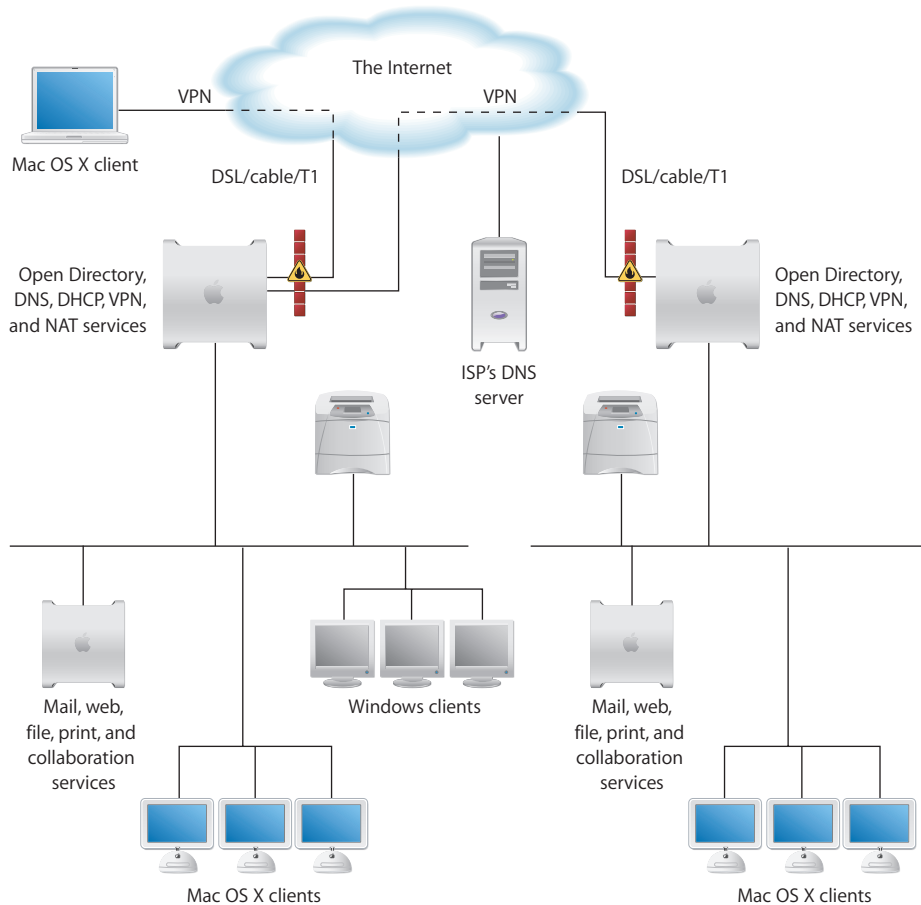


- Using Xserve as the departmental computer provides the bandwidth needed for large-file transfers. Xserve supports jumbo frame Ethernet packets and can utilize both built-in Ethernet interfaces.
- Web-based Distributed Authoring and Versioning (WebDAV) technology, integrated into Mac OS X Server's web service, lets you use a web server as an Internet file server. Users can author and access documents over the web from Mac OS X computers. You can use WebDAV for collaborative editing and file management even while a website is running.
- QuickTime streaming service lets you broadcast streaming video to client computers in real time using industry-standard streaming protocols.
- Mac OS X Server lets you set up mobile accounts for departmental employees who carry portable computers back and forth to client sites. Mobile accounts let users experience a similar work environment on and off the network.

Small and Medium Businesses

Small businesses (fewer than 100 employees) and medium businesses (about 100 to 500 employees) benefit from cross-platform file and printer sharing and numerous other services, including network, mail, web, and collaboration.

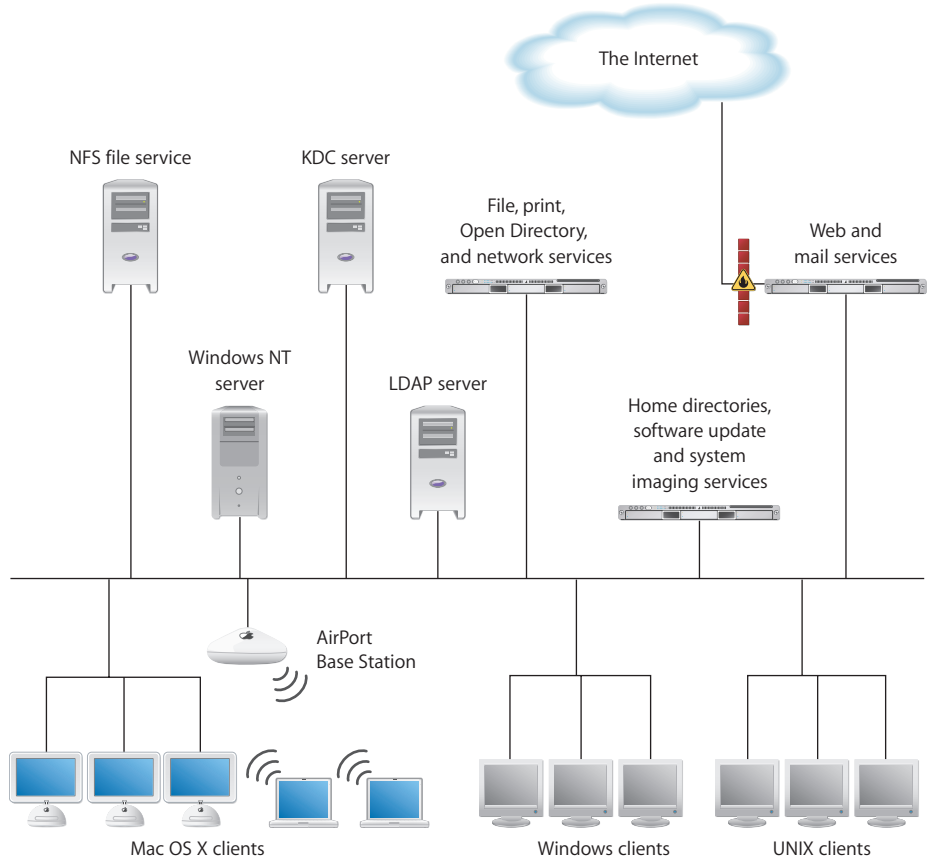
The following picture depicts a business with two small networks, joined by a VPN connection. Referred to as “site-to-site VPN,” this kind of secure connection is easy to establish when needed, as when a business needs to open another office. It offers the additional advantage of making both networks appear as one to employees working at either site. Using VPN service also lets employees access the company intranet to use mail, file and other services when away from the office.



- The directory and network services in each network reside on one Mac OS X Server, and a second server hosts mail, web, and other employee productivity services. In small businesses, all services might reside on a single server.
- Setting up basic network services, such as the Network Address translation (NAT), firewall (IP filter), DHCP, and DNS services in this scenario, are easy thanks to Gateway Setup Assistant. This tool configures a server as a gateway, linking a local area network (LAN) to the external Internet and letting you share a server's Internet connection among computers on the LAN.
- The firewall between Mac OS X Server and the Internet protects the company intranet from access by unauthorized users.
- An authoritative DNS server hosted by another company provides domain name (example.com) resolution. DNS services on Mac OS X Server provide names for the intranet devices (such as printers and client computers) that have static IP addresses and cache DNS lookups for faster name resolution.
- DHCP services provide dynamic IP addresses to some of the Macintosh and Windows clients.
- Like all the other services shown, VPN supports both Macintosh and Windows clients. If the organization uses a lot of Windows computers, you can set up Mac OS X Server as a Primary Domain Controller (PDC) so you can host Windows home directories.
- NAT service lets employees share a single Internet connection. NAT converts all client IP addresses to one IP address for Internet communications.
- Web service's proxy caching speeds up response times and reduces network traffic by storing recently accessed files in a cache on the web server so they can be retrieved quickly when requested again.
- You can customize what users see in the Finder when they select the Network icon in the sidebar of a Finder window by defining managed network views. Managed network views simplify finding files and folders that reside on network servers when they're used to list network resources in a fashion meaningful to users.

Higher-Education Facilities

Colleges and universities have heterogeneous computer environments, since the students and the computer systems they use are highly diverse. Mac OS X Server fits well into such an environment because of its capacity to integrate with a wide variety of existing services, protocols, and directory infrastructures.

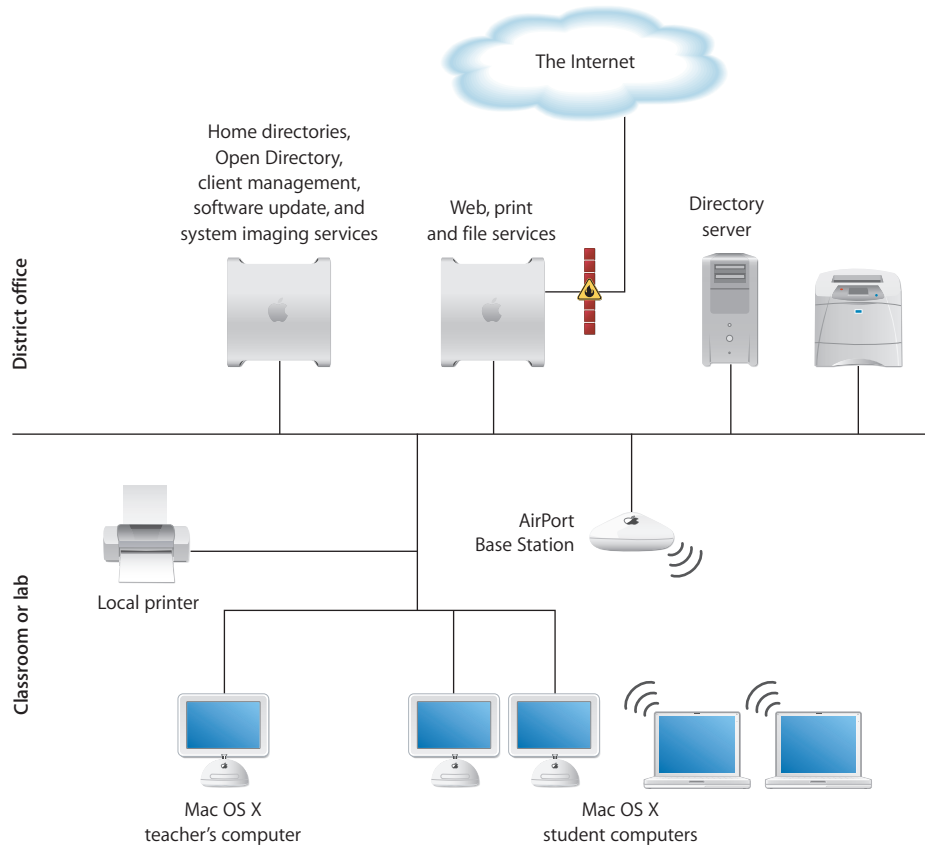


- The wide range of client computers (Macintosh, Windows, UNIX, Linux) demands flexible file access support. The highly scalable IP-based file services in Mac OS X Server support file access from anywhere on the network via AFP, NFS, FTP, and SMB/CIFS.
- Mac OS X Server can host home directories for users of all these client computers.
- User and network resource information can be retrieved by Mac OS X Server from existing directory systems, such as Lightweight Directory Access Protocol (LDAP), Active Directory, and Network Information Service (NIS) servers.
- Mac OS X Server can also use an existing directory system, such as LDAP or Kerberos Key Distribution Center (KDC), to authenticate users.
- Network Install makes it easy to change software configurations, over the network, on hundreds of Macintosh client computers, as often as necessary. It automates the setup of lab and faculty computers, facilitates software upgrades, and quickly refreshes computers to an original, preconfigured state.
- Mac OS X Server offers PostScript-compatible print spooling and job accounting for print jobs submitted using the Line Printer Remote (LPR) protocol, the industry-standard Transmission Control Protocol (TCP) protocol, the Windows SMB/CIFS protocol, and AppleTalk. The server supports both PostScript and non-PostScript print spooling using the Internet Printing Protocol (IPP).
- Because higher education networks are complex, network services are critically important. DNS and DHCP can be set up on Mac OS X Server to help client computers and services find resources on a network. IP filtering can be used to provide a security firewall around sensitive data.

K–12 Labs and Classrooms

In K–12 educational scenarios, students need access to their own files and must be able to turn in assignments electronically or in print. Students also need access to applications (such as iLife) that facilitate learning, but must also be prevented from using non-instructional applications (such as iChat).

Teachers need file services support so they can make lesson plans and teaching materials available to students online. Teachers also need a way to retrieve and update student records and other administrative information that's centralized on a remote server.



- Mac OS X Server's client management service provides a way to control student Macintosh computer work environments.

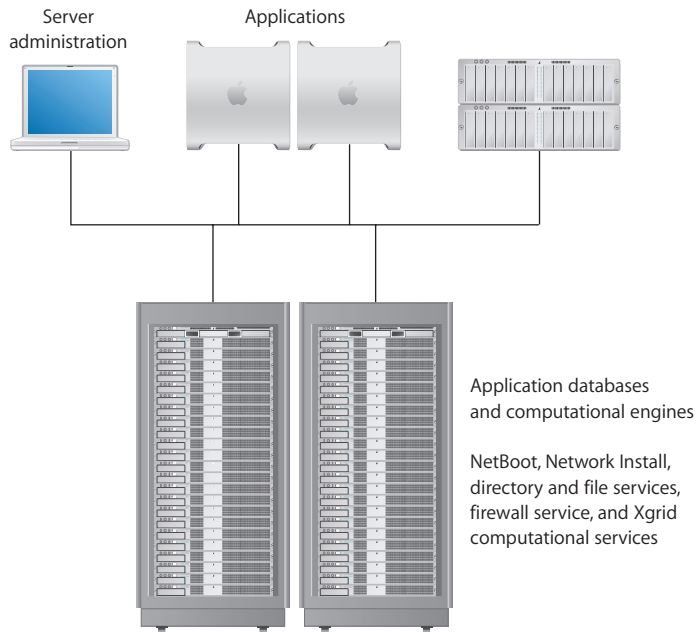
Many preferences, such as Dock and Finder preferences, are used to customize the appearance of student desktops. For example, you can set up Dock preferences and Finder preferences so that the work environment of lower-grade students is dramatically simplified.

Other preferences are used to manage what a student can access and control. For example, you can set up Media Access preferences to prevent students from burning CDs and DVDs or making changes to a computer's internal disk. Also, you can control which students can access the Internet.

- Many school districts have an LDAP or Active Directory server set up as a master directory server for all schools in the district. Mac OS X Server can use these existing centralized repositories for accessing student and teacher information, but host other services, such as file and printer sharing, on the server in a lab or classroom.
- Mobile accounts support students who use portable Macintosh computers such as the iBook. They let students work on assignments at home in an environment that mimics the classroom environment.
- Mac OS X Server's print service lets teachers manage student usage of classroom printers, including non-PostScript (inkjet) printers.
- NetBoot and Network Install images provide fast initial setup of student computers and rapid refresh of lab computers. To keep student operating systems and applications up to date you can use Network Install images or the server's software update service.
- The Gateway Setup Assistant quickly and easily configures basic network settings and lets you share a server's Internet connection among computers on a LAN.

Computational Clustering

Clusters of Xserve computers offer a high-performance, cost-effective approach to the computationally intensive processing needed for genetic research, video production, or other high-bandwidth computing.



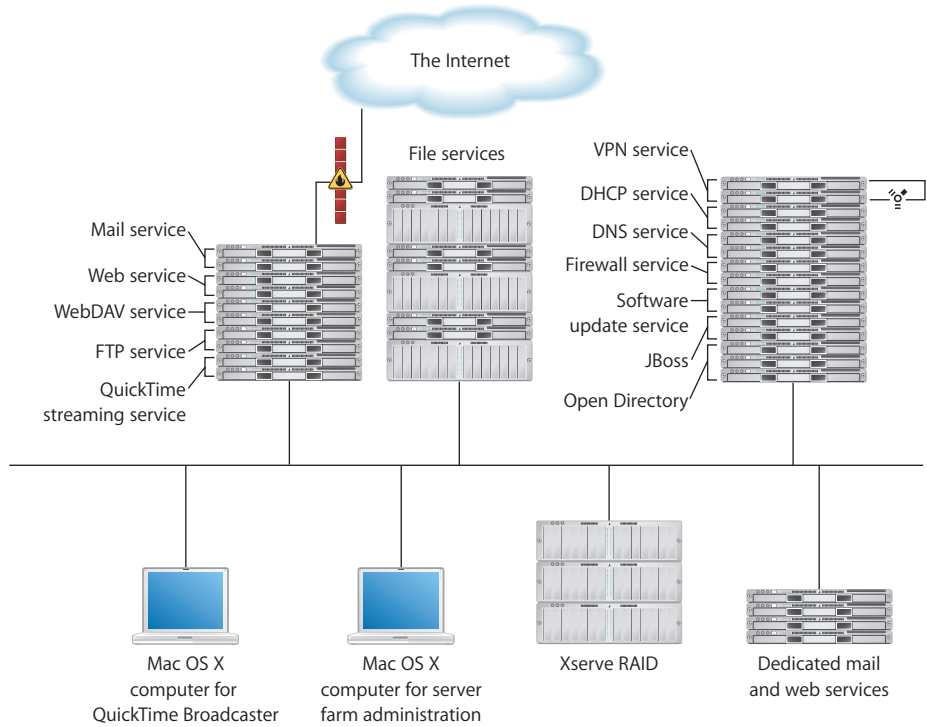
- One Xserve in a rack is usually set up as a master computer, called the *head node*. The head node runs NetBoot and Network Install and hosts directory services and other shared facilities for other computers in the rack, which are used for data processing and numerical computations.
- The head node is also likely to be set up as an AFP and NFS file server and implement an IP firewall that protects access to the cluster by unauthorized users.
- The head node can also be set up as an Xgrid cluster controller. Xgrid computational service lets you achieve supercomputer performance levels by distributing computations over collections of dedicated or shared computers. The Xgrid cluster controller provides centralized access to the distributed computing pool, referred to as a computational cluster.
- Scientists, videographers, and other application users work at Mac OS X computers to remotely configure and monitor applications and databases residing on the Xserve computers.
- Mac OS X Server offers scientists and researchers familiar UNIX utilities, shells, scripting languages, and compilers for building specialized software. A full suite of developer tools comes with Mac OS X Server, including the gcc command-line compiler and a development tool called Xcode 2.0.

You can write, compile, and debug using C, C++, Objective-C, or Java. Project Builder can be used to port command-line applications to Mac OS X and Mac OS X Server or to enhance them with a Mac OS X user interface.

- An administrator computer, such as an iBook running Mac OS X Server administrative applications, can be used to manage the entire network.

Data Centers

Mac OS X Server provides the full range of services you need if you host ecommerce websites or provide other Internet services that require high availability and scalability.



- High-availability support includes automatic restart after a service or power failure, software RAID, disk space monitoring, file system journaling, and Open Directory replication. In addition, IP failover can be configured using IP over FireWire, which lets you interconnect redundant servers without using up gigabit Ethernet ports.
- On some computers, you can improve physical connection availability by using link aggregation. Link aggregation configures several physical network links as a single logical link to improve the capacity and availability of network connections.
- You can host many websites on a single server. You can host each site with its own IP address (multihoming) or you can configure multiple sites with a single IP address (virtual hosting).
- Mac OS X Server's web service lets you set up Secure Sockets Layer (SSL) protection for secure Internet connections.
- Mac OS X Server has built-in support for Perl, Java Servlets, JavaServer Pages, and PHP Hypertext Preprocessor (PHP).
- You can deploy enterprise Java applications using the JBoss application server. JBoss, which runs on Java 1.4.2, implements the Enterprise Edition (J2EE) technologies. The Mac OS X Server implementation includes easy-to-use administration tools to help you configure and monitor the application servers. Because of its clustering capabilities, JBoss might be run on several Xserve computers.
- QuickTime Streaming Server lets you broadcast multimedia in real time, including live QuickTime Broadcaster streams.
- Xserve RAID provides extended storage.

Mac OS X Server blends a mature, stable UNIX foundation with open standards support and Macintosh ease of use.

This chapter introduces the services that Mac OS X Server offers and tells you where to find more information about them.

Core System Services

Mac OS X Server is built on top of Darwin, the core Mac OS X operating system. Darwin integrates Mach 3.0 operating-system services based on FreeBSD (Berkeley Software Distribution) 4.8 and the latest advances from FreeBSD 5.0. It includes high-performance networking facilities. It provides support for multiple integrated file systems, BSD symmetric multiprocessing with fine-grain locking, and 64-bit applications. Advanced networking capabilities include support for IPv6, IPSec, and link aggregation.

A key factor in the stability of the system is Darwin's advanced memory protection and management system. Darwin ensures reliability by providing applications and processes with their own unique address space. The Mach 3 microkernel supports multitasking and multiprocessing, memory management, real-time scheduling, unified buffer cache, hot-plug drivers, and power management.

Ease of use and simplicity are hallmarks of Mac OS X. It's visually powerful, using graphics technologies based on OpenGL, Quartz, and QuickTime. Mac OS X Server takes advantage of these capabilities by providing administrators with server management applications that are easy to use, but powerful and secure. Administrators who prefer to work in a command-line environment can do so. A complete shell environment, including popular UNIX utilities, offers a full palette of command-line administration techniques.

Read on to learn about the services that Mac OS X Server provides to extend its Mac OS X core in order to support Macintosh, Windows, UNIX, and Linux clients over a network. To learn more about server administration tools, see Chapter 3, "Server Administration," on page 57.

Open Directory

Open Directory is the Mac OS X directory services framework. It encompasses directory services, authentication, and service discovery for Mac OS X and Mac OS X Server.

Directory services are the means by which a server and its clients (users and services) locate and retrieve information needed for authentication, network resource discovery, and other crucial system activities. User and group information is needed to authenticate users when they log in and to authorize their access to services and files. Information about network resources is used to make printers, computers, and other devices visible for browsing.

Directory services retrieve this information from directories, repositories of information about users and computing resources. Open Directory lets your server retrieve information from:

- Directories on Mac OS X Server computers
- Directories on non-Apple servers
- Configuration files on Mac OS X Server or other servers

Open Directory also supports several protocols for discovering network resources:

- Multicast DNS
- Server Message Block/Common Internet File System (SMB/CIFS)
- AppleTalk
- Service Location Protocol (SLP)

The Open Directory administration guide provides complete details about how to set up and use Open Directory. Some highlights of the many features that Open Directory offers follow.

Using Mac OS X Server Directories

Mac OS X Server can host Lightweight Directory Access Protocol (LDAP) directories. These are LDAPv3 directories that store shared directory data you want to be used by other computers.

LDAP directories are easy to manage, can be replicated for performance and backup, support a very high volume of information, and give you read-write control over directory data.

Using Non-Apple Directories

Open Directory lets you take advantage of information you've already set up in non-Apple directories and in flat files:

- On other LDAPv3 servers
- On Active Directory servers
- In BSD configuration files
- In Sun Microsystems Network Information System (NIS) files

Mac OS X Server provides full read/write and Secure Sockets Layer (SSL) communications support for LDAPv3 directories.

Directory Management

Several Open Directory features help you effectively and efficiently manage your directory data:

- **Automatic LDAP schema replication.** You can store LDAP schema in the directory, letting you add new schema without manually copying configuration files. Changes are automatically propagated from the Open Directory master to all its replicas.
This feature lets you efficiently propagate administrative policy changes without manually updating servers on which directory replicas reside.
- **Directory access controls.** You can store data specifying user access to directory information in a directory.
- **Backing up directory services data.** You can back up Open Directory authentication and LDAP directory data with the click of a button in the Server Admin application.

Search Policies

Before a user can log in to or connect with a Mac OS X client or server, the user must enter a name and password associated with a user account that the computer can find. A Mac OS X computer can find user accounts that reside in a directory listed in the computer's search policy. A search policy is simply a list of directories the computer searches when it needs configuration data.

You can configure the search policy of Mac OS X computers on the computers themselves, using the Directory Access application:

- You can automate Mac OS X client directory setup by using Mac OS X Server's built-in Dynamic Host Configuration Protocol (DHCP) Option 95 support. With this approach, a DHCP server identifies the server from which a Mac OS X computer should obtain directory data at the same time the DHCP server provides an IP address to the client computer. This approach is intended for use by computers connected directly to a wired network.
- For mobile computers, frequently used in a wireless environment, trusted directory access binding is available. Trusted binding offers a way for a client computer to authenticate to an LDAP server and for the LDAP server to authenticate to the client. This mutual authentication offers the safest way to set up directory server connections in a wireless environment.

Authentication

You have several options for authenticating users:

- **Open Directory authentication.** Based on the standard Simple Authentication and Security Layer (SASL) protocol, Open Directory authentication supports many authentication methods, including CRAM-MD5, APOP, WebDAV, SHA-1, LAN Manager, NTLMv1, and NTLMv2. It's the preferred way to authenticate Windows users.

Authentication methods can be selectively disabled to make password storage on the server more secure. For example, if no clients will use Windows services, you can disable the NTLMv1 and LAN Manager authentication methods to prevent storing passwords on the server using these methods. Then someone who somehow gains access to your password database can't exploit weaknesses in these authentication methods to crack passwords.

Open Directory authentication lets you set up password policies for individual users or for all users whose records are stored in a particular directory, with exceptions if required. Open Directory authentication also lets you specify password policies for individual directory replicas.

For example, you can specify a minimum password length or require a user to change the password the next time he or she logs in. You can also disable login for inactive accounts or after a specified number of failed login attempts.

- **Kerberos v5 authentication.** Using Kerberos authentication allows integration into existing Kerberos environments. The Key Distribution Center (KDC) on Mac OS X Server offers full support for password policies you set up on the server. Using Kerberos also provides a feature known as *single sign-on*, described in the next section.

The following services on Mac OS X Server support Kerberos authentication: Apple Filing Protocol (AFP), mail, File Transfer Protocol (FTP), Secure Shell (SSH), login window, LDAPv3, Virtual Private Network (VPN), screen saver, and Apache (via the SPNEGO Simple and Protected GSS-API Negotiation Mechanism, protocol).

- **Storing passwords in user accounts.** This approach may be useful when migrating user accounts from earlier server versions. However, this approach may not support clients that require certain network-secure authentication protocols, such as APOP.
- **Non-Apple LDAPv3 authentication.** This approach is available for environments that already have an LDAPv3 server set up to authenticate users.

Single Sign-On

When a Mac OS X user is authenticated using Kerberos, the user doesn't have to enter a user name and password every time a Kerberized service is used.

The user enters the Kerberos name and password at login, but doesn't need to reenter it when using services that support Kerberos authentication.

Discovery of Network Services

Information about file servers and other services tends to change much more frequently than user information, so it isn't typically stored in directories. Instead, information about these services is discovered as the need arises.

Open Directory can discover network services that make their existence and whereabouts known. Services make themselves known by means of standard protocols. Open Directory supports the following service discovery protocols:

- Multicast DNS, for discovering file and print services on the local network
- SMB/CIFS, the protocol used by Microsoft Windows
- AppleTalk, the legacy Mac OS protocol for file services, also used for print services via Printer Access Protocol (PAP)
- SLP, an open standard for discovering file and print services

To make network browsing easy for users, you can use managed network views. See “Managed Network Views” on page 39 for more information.

User Management

Mac OS X Server helps you manage access to network resources, files, and services by Macintosh, Windows, UNIX, and Linux computer users.

The user management guide contains a full description of the server's user management capabilities. Some highlights follow.

User Accounts

User accounts contain the information needed to prove a user's identity: user name, password, and user ID. Other information in a user's account is needed by various services, to determine what the user is authorized to do and perhaps to personalize the user's environment.

Group Accounts

Group accounts offer a simple way to manage a collection of users with similar needs. A group account stores the identities of users who belong to the group as well as information that lets you customize the working environment for members of a group.

You can also use nested groups and group folders:

- A nested group is a group that's a member of another group. Nesting groups lets you manage groups of users at both a global level (when you want to influence all members of a group) and at a smaller, more focused level (when you want to influence only certain members of a group).

- A group folder is a place for group members to exchange ideas and receive information that's relevant to the group. By default, group folders contain three folders: Documents, Library, and Public, and there's a Drop Box folder in the Public folder. If needed, you can customize these folders and automatically mount them on the desktop of group members at login.

Computer Lists

Computer lists let you manage collections of computers.

For example, you can use a computer list to reserve high-capacity computers for film students. You'd set up a computer list consisting of the high-capacity computers, assign film students to a group, and give access to the computer list to only that group. A student who isn't a film student can't log in to one of those computers.

Home Directories

A home directory is a folder where a user's files and preferences are stored. Other users can see a user's home directory and read files in its Public folder, but they can't (by default) access anything else in that directory.

Mac OS X Server can host home directories for Macintosh, UNIX, and Windows users. With a home directory, these users can access their applications, documents, and individual settings regardless of the computer to which they log in.

You can impose disk quotas on home directories to regulate server disk usage for users with home directories.

Macintosh User Management

Mac OS X Server offers work environment personalization for Mac OS X computer users to:

- Manage preferences and set up mobile accounts and managed network views, features summarized next.
- Automate operating system images used by Macintosh client computers, as "System Image Services" on page 40 describes.

Preference Management

You can use Mac OS X Server to manage the work environments of Mac OS X users by defining preferences. Preferences are settings that customize and control a user's computer experience.

- Preferences can be used to change the appearance of a user's desktop. For example, you dramatically simplify the appearance of the Dock and the Finder for lower-grade students.
- Preferences can be used to manage what a user can access and control. For example, you can set up Media Access preferences to prevent students from burning CDs or DVDs or making changes to a computer's internal disk. You can also control which system preferences a user can change.

- Preferences can be used to configure a computer's network behavior. For example, you can enable or disable Internet sharing, or configure network proxy settings for a user's computer by defining a computer list and setting preferences for the list.
- Preferences can be used to automatically mount network home directories and group folders or to open applications at login. They can also be used to control the options visible in a computer's login window.

The Workgroup Manager application lets you define preferences that affect users, groups, and computers. A graphical interface offers a quick and easy way to work with preferences that are predefined.

If you want additional control of preference settings, you can work with preference manifests using Workgroup Manager's preference editor. Preference manifests are files that describe the structure and values of an application's or utility's preferences. The preference editor lets you work with preference manifests for the predefined preferences or add new preference manifests for applications and utilities of interest.

You can use DHCP Option 95 to identify a server from which a client computer retrieves directory information at login so that preference settings are automatically downloaded from the network without the need to configure the client computer directly.

Mobile Accounts

You can set up mobile accounts to support Mac OS X users who use their computers both on and off the network.

Mobile accounts let a user log in locally or use the network with the same network name and password. And they let the user experience similar work environments on and off the network.

While mobile accounts are especially useful for mobile computer users, they're advantageous for any user who needs to access network resources only occasionally. When most of the computer work can be done locally, using a mobile account reduces network traffic.

Managed Network Views

You can set up managed network views, which are custom views that users see when they select the Network icon in the sidebar of a Finder window.

A managed network view is one or more network neighborhoods, which appear in the Finder as folders. Each folder contains a list of resources an administrator has associated with the folder.

Managed network views offer a meaningful way to present network resources. You can create multiple views for different client computers. And because the views are stored using Open Directory, a computer's network neighborhood is automatically available when a user logs in.

Windows User Management

You can maximize the support you provide for Windows users by setting up a Windows primary domain controller (PDC) on Mac OS X Server and defining Windows settings for a user. When you do so, the server:

- Provides domain Open Directory authentication for Windows NT 4.x, Windows 2000, and Windows XP clients.
- Hosts home directories for Windows users in the domain.
- Supports roaming user profiles for home directories.

If you have more than one Mac OS X Server system, you can make one server a PDC and other servers BDCs (backup domain controllers). BDCs provide automatic failover and backup for the PDC. The PDC and BDCs have synchronized copies of directory and authentication data, and they share client requests for this data. If the PDC becomes unavailable, the BDCs automatically take over its load.

A user account can contain both Macintosh and Windows attributes, so users can log in from either type of computer. Windows users can use Mac OS X Server's VPN, file, and print services, as described later in this chapter.

The Windows services administration guide describes how to set up the many Windows-specific options that Mac OS X Server supports.

System Image Services

You can create disk images and then set up Mac OS X Server to host the images, letting Mac OS X computers start up from the images or install the images over the network. NetBoot images are used for remote startup, and Network Install images are used for remote installations.

The source of an image can be a CD, DVD, or DMG (disk image). You can also create an image that mimics an existing system already set up the way you want client computers to be set up. In this case, the source of the image is a volume or partition.

The system image administration guide provides complete information about NetBoot and Network Install.

NetBoot

NetBoot lets Macintosh clients, including Mac OS X clients without a local hard drive, start up from a system disk image located on Mac OS X Server instead of on the client computer's disk drive:

- NetBoot simplifies the administration of large-scale deployments of network-based Macintosh systems or racks of Xserve computers. It's ideal for an organization with computers that need to be identically configured; for example, NetBoot can offer a web service provider a way to configure multiple web servers.
- NetBoot also lets you set up multiple NetBoot disk images, so you can boot clients into Mac OS X or even customize the Macintosh environment for different groups of computers.
- NetBoot allows administrators to configure and update client computers instantly by updating a boot image stored on the server. Any changes made on the server are automatically reflected on the clients when they reboot. Systems that are compromised or otherwise altered can be instantly restored by rebooting.

Network Install

Network Install is a centrally managed installation service that lets administrators selectively install, restore, or upgrade Macintosh computers. You don't have to insert multiple discs to set up a system; all the installation data resides on the server.

Here are some of the advantages that Network Install offers:

- Network Install is one solution for operating system migrations and installing software updates.
- You can install site-licensed or custom applications, restore computer classrooms and labs, and reimagine desktop and portable computers.
- You can define custom installation images for various departments in an organization, such as marketing, engineering, and sales.
- You can define post-installation scripts that invoke actions after the installation of a software package or system image.
- You can set up an automated install image. This type of image includes answers to all of the usual installer questions so that, when the client boots from the image, installation occurs without user intervention.

Software Update Service

You can distribute Apple software updates to users by setting up a software update server on Mac OS X Server.

Using a software update server lets you conserve your Internet bandwidth. Instead of having all your users download new software from Apple, they can download it from a server on your own network.

Users select from the updates you choose to make available. You can prevent user downloads of particular updates until you've evaluated them or until your organization is ready for them.

See the system image and software update administration guide for details about software update service.

File Services

Mac OS X Server makes it easy to share files using the native protocols of different kinds of client computers. Mac OS X Server includes these file services:

- Apple file service, which uses the Apple Filing Protocol (AFP), lets you share resources among Macintosh clients.
- Windows services use the SMB/CIFS protocol to let you share resources with clients who use Windows, and to provide name resolution service for Windows clients. These services support users of Microsoft Windows 95, 98, ME, XP, NT 4.0, and 2000.
- File Transfer Protocol (FTP) service lets you share files with anyone using FTP.
- Network File System (NFS) service lets you share files and folders with users who have NFS client software (UNIX users).
- Web-based Distributed Authoring and Versioning (WebDAV) lets you use a web server as if it were a file server.

The file services administration guide describes how to set up and manage AFP, SMB/CIFS/ FTP, and NFS file services. The Windows services administration guide provides additional information on sharing files with Windows users. The web technologies administration guide covers WebDAV.

Sharing

You share files among users by designating share points. A share point is a folder, hard disk (or hard disk partition), or CD that you make accessible over the network. It's the point of access at the top level of a group of shared items.

You can use a share point over multiple protocols: AFP, SMB/CIFS, NFS, and FTP. On Mac OS X client computers, share points can be found in the /Network directory and by using the Finder's Connect To Server command. On Windows computers, users use Network Neighborhood.

Sharing offers several features that make your shared-file environment more secure and efficient:

- **Access Control Lists (ACLs).** ACLs give you a way to craft share point, folder, and file access permissions with a high degree of precision. A wide range of permissions, including the right to modify access permissions, the right to create and delete or change files, the right to read permissions, and others, can be assigned to individual users and to groups, which can be nested. In addition, you can use inheritance to propagate permissions through a file system hierarchy.
- **Unified file locking.** Mac OS X Server unifies file locking across AFP and SMB/CIFS protocols. This feature lets users working on multiple platforms simultaneously share files without worrying about file corruption.
- **Authentication options.** Mac OS X Server's Kerberos supports AFP and FTP authentication. For Windows users, the server supports Active Directory's Kerberos authentication.

Apple File Service

Apple Filing Protocol (AFP) allows Macintosh client users to connect to the server and access folders and files as if they were located on the user's own computer.

AFP offers:

- File sharing support for Macintosh clients over TCP/IP
- Autoreconnect support when a file server connection is interrupted
- Encrypted file sharing (AFP through SSH)
- Automatic creation of user home directories
- Kerberos v5 authentication for Mac OS X version 10.2 and later clients
- Fine-grain access controls for managing client connections and guest access
- Automatic disconnect of idle clients
- IPv6 support for AFP clients and server
- ACLs

AFP also lets you reshare NFS mounts using AFP. This feature provides a way for clients who aren't on the local network to access NFS volumes via a secure, authenticated AFP connection.

Windows Services

Windows file service in Mac OS X Server allows Windows clients to connect to Mac OS X Server using SMB/CIFS over TCP/IP.

When you enable Windows file service, you can also enable several additional native Windows services:

- Windows Internet Naming Service (WINS), which allows clients across multiple subnets to perform name/address resolution
- Browsing, which allows clients to browse for available servers across subnets

You can set up (and replicate) Primary Domain Controller (PDC) services, which:

- Provide Windows domain authentication from the Windows login window.
- Support Windows roaming profiles on Mac OS X Server.

Mac OS X Server provides unified file locking across AFP and SMB/CIFS protocols, letting Windows users share files with users on other computers without conflict or corruption. SMB/CIFS also supports ACLs.

Network File System (NFS) Service

NFS is the protocol used for file services on UNIX computers.

The NFS term for sharing is *export*. You can export a shared item to a set of client computers or to “World.” Exporting an NFS volume to World means that anyone who can access your server can also access that volume.

NFS doesn’t support name/password authentication. It relies on client IP addresses to authenticate users and on client enforcement of permissions, not a secure approach in most networks. Therefore, use NFS only if you’re on a local area network (LAN) with trusted client computers, or if you’re in an environment that can’t use Apple file sharing or Windows file sharing. If you have Internet access and plan to export to World, your server should be behind a firewall.

You can reshare NFS mounts using AFP, Windows, and FTP so that users can access NFS volumes in a more restricted fashion.

File Transfer Protocol (FTP)

FTP allows computers to transfer files over the Internet. Clients using any operating system that supports FTP can connect to your FTP file server and download files, depending on the permissions you set. Most Internet browsers and a number of freeware applications can be used to access your FTP server.

FTP service in Mac OS X Server supports Kerberos v5 authentication and, for most FTP clients, resumption of interrupted FTP file transfers. Mac OS X Server also supports dynamic file conversion, allowing users to request compressed or decompressed versions of information on the server.

Mac OS X Server supports anonymous FTP and by default prevents anonymous FTP users from deleting files, renaming files, overwriting files, and changing file permissions. Explicit action must be taken by an administrator to allow uploads from anonymous FTP users, and then only into a specific share point.

Web-based Distributed Authoring and Versioning (WebDAV)

Mac OS X Server supports WebDAV Internet file sharing as part of the built-in Apache web server and Mac OS X Server's web services.

Originally designed for collaborative web publishing, this enhancement to the HTTP protocol turns a website into a document database, enabling collaborative creation, editing, and searching from remote locations. With WebDAV enabled, any authorized WebDAV client, on any platform, can open files, make changes or additions, and save those revisions back to the web server. And because it uses HTTP (port 80), WebDAV can support file sharing through firewalls that don't allow FTP sharing.

Print Service

Print service in Mac OS X Server lets you share network and direct-connect printers among clients on your network. Print service also includes support for managing print queues, monitoring print jobs, extensive logging, and using print quotas.

Print service lets you:

- Share network PostScript printers with Mac OS 9 (PAP, LaserWriter 8), Mac OS X (IPP, IP/LPR), Windows (SMB/CIFS), and UNIX (IP/LPR) clients.
- Share PostScript and non-PostScript printers that are directly connected to Mac OS X Server with Mac OS X version 10.2 and later clients.
- Share directly connected non-PostScript printers as generic PostScript printers over LPR, SMB/CIFS, and AppleTalk.
- Connect to network printers using AppleTalk, LPR, and IPP, and connect to direct-connect printers using USB.
- Make printers easy for users to discover using Open Directory.
- Impose per-user print quotas to limit printer usage; in addition, you can impose a quota on individual printers.
- Set up printer pools for load balancing. A printer pool is a group of printers you designate to handle print jobs submitted to two or more print queues. A job is printed by the first available printer in the pool.
- Define cover pages for print jobs in a particular print queue.

The print service administration guide provides information about how to set up and administer print service.

Web Service

Web service in Mac OS X Server is based on Apache, an open-source HTTP web server. The server comes with both Apache 1.3 and Apache 2.0, but Apache 2.0 is included for evaluation only. Server Admin supports Apache 1.3.

Open-source software allows anyone to view and modify the source code to make changes and improvements. Those features have led to Apache's widespread use, making it the most popular web server on the Internet today.

Web service includes a high-performance, front-end cache that improves performance for websites that use static HTML pages. With this cache, data files don't need to be accessed by the server each time it's requested.

Web service also includes support for Web-based Distributed Authoring and Versioning (WebDAV). With WebDAV capability, your client users can check out web pages, make changes, then check the pages back in while the site is running. In addition, Mac OS X users can use a WebDAV-enabled web server as if it were a file server.

Web service's SSL support enables secure encryption and authentication for ecommerce websites and confidential materials. An easy-to-use digital certificate provides unforgeable proof of your website identity. Web service also supports Kerberos v5 authentication (via the SPNEGO protocol).

Mac OS X Server offers extensive support for dynamic websites:

- Web service supports Java Servlets, JavaServer Pages, MySQL, PHP, Perl, and CGI scripts or programs.
- Mac OS X Server includes a JBoss server and high-level administration tools for configuring and managing it. See "Application Server Support" on page 51 for more information about JBoss.

The web technologies administration guide provides information about configuring and managing web service.

Mail Service

Mac OS X Server provides an enterprise-capable mail server, which supports the SMTP, POP, and IMAP protocols, allowing you to select a local or server-based mail storage solution for server users.

Outgoing mail (SMTP) has these features:

- The SMTP mail transfer agent is based on Postfix. For complete information about this open-source agent, see www.postfix.org/.
- Authentication using the following methods is available: PLAIN, LOGIN, CRAM-MD5, and Kerberos v5.

Incoming mail (POP and IMAP) highlights include these:

- The mail access agent is a Cyrus POP and IMAP server. See asg.web.cmu.edu/cyrus/ for information about this agent.
- Authentication supported for IMAP is clear text, PLAIN, LOGIN, CRAM-MD5, and Kerberos v5. POP authentication options are clear text, APOP, and Kerberos v5.
- The mail database is extremely fast.
- Vacation rules and quotas for individual users are available.
- Mailman is used to create and maintain mailing lists.

Mail service protects your users from junk mail and other annoying or unauthorized messages. You can define filters that help you minimize junk mail and viruses, filter out unsolicited commercial email, and detect messages that contain particular content. Junk mail filtering, based on the powerful SpamAssassin, includes an autolearning option.

Flexible quotas let you set custom warning levels for user mail disk consumption and define customized warning messages. You can set up to three different warning levels based on percent of mail quota consumed. When a user has exceeded a certain quota level, the system sends an email warning with either a default message or a custom message. You can optionally enforce user quotas by denying new mail delivery for users who have exceeded their quota.

Virtual host support lets a single server host several different email domains. For example, your server can host email accounts for `postmaster@yourhost.com` and `postmaster@myhost.com`.

Mac OS X Server also includes SquirrelMail for web-based mail retrieval. For information about SquirrelMail, see www.squirrelmail.org.

The mail service administration guide tells you how to set up and manage mail service. The web technologies administration guide describes how to enable WebMail, the server's implementation of SquirrelMail.

Network Services

Mac OS X Server helps you manage network communications by providing:

- Dynamic Host Configuration Protocol (DHCP) service
- Domain Name System (DNS) service
- Firewall service
- Network Address Translation (NAT) service
- Virtual Private Network (VPN) service
- Network time service
- Gateway Setup Assistant
- IP failover

The network services administration guide provides information about network services.

DHCP

DHCP is especially useful when an organization has more clients than IP addresses. IP addresses are assigned on an as-needed basis, and when they're not needed they're available for use by other clients.

DHCP helps you administer and distribute IP addresses dynamically to client computers from your server. From a block of IP addresses that you define, your server locates an unused address and “leases” it to client computers as needed. The server's DHCP service also supports static IP address assignment to computers with a specific Ethernet (MAC) address.

As you learned in “Search Policies” on page 35, you can automate the directory services setup of Mac OS X clients using your DHCP server's Option 95 support. This option lets client computers learn about their directory settings from a DHCP server.

DNS

DNS service lets users connect to a network resource, such as a web or file server, by specifying a name (such as `server.example.com`) rather than an IP address (such as `192.168.11.12`). DNS is a distributed database that maps IP addresses to domain names.

A server that provides DNS service keeps a list of names and the IP addresses associated with the names. When a computer needs to find the IP address for a name, it sends a message to the DNS server (also known as a *name server*). The name server looks up the IP address and sends it back to the computer. If the name server doesn't have the IP address locally, it sends messages to other name servers on the Internet until the IP address is found.

If you don't have an Internet service provider (ISP) who handles DNS for your network, you can set up a DNS server on your Mac OS X Server. See individual service administration guides for information about DNS dependencies for each service.

Mac OS X Server provides administration tools for service configuration management, zone control, and monitoring, providing a graphical way to:

- Enable zone transfers and recursion
- Work with log files
- Manage zones and records for the machines in those zones

Firewall

Firewall service protects your server and its contents from intruders. It provides a software firewall, scanning incoming IP packets and accepting or rejecting them based on filters you define.

You can set up server-wide restrictions for packets from specific IP addresses. You can also restrict access to individual services, such as web, mail, and FTP, by defining filters for the ports used by the services. IP firewall can be used to block access to specific service ports or to allow access only to certain ports.

IP firewall also provides a sophisticated mechanism, stateful packet inspection, for determining whether an incoming packet is a legitimate response to an outgoing request or part of an ongoing session, allowing packets that would otherwise be denied.

NAT

NAT is a method of connecting multiple computers to the Internet (or any other IP network) using one IP address. NAT converts the IP addresses you assign to computers on your private, internal network into one legitimate IP address for Internet communications. For example, the AirPort Base Station uses NAT. By default, a base station assigns IP addresses using DHCP to computers on an Ethernet network, then uses NAT to convert those addresses when any of the computers needs to access the Internet.

NAT is becoming increasingly popular because it preserves IP addresses. It also increases the security of Internet access, because it supports only connections that originate on an internal network.

NAT is closely related to IP firewall. The firewall diverts network packets to the NAT process so they can be translated.

VPN

You can set up a VPN using Mac OS X Server.

VPN is a network transmission protocol that uses encryption and other technologies to provide secure communications over a public network. Typically the public network is the Internet, but VPNs are also used to support connections between multiple intranets within the same organization and to join networks between two organizations to form an extranet.

Site-to-site VPN connects two networks. It offers a secure connection that's easy to establish when the need arises to set up a network at another site, as when a business expands. Site-to-site VPN makes both networks appear as one to users working at either site.

VPNs transmit encrypted IP packets so that only legitimate targets can interpret them, protecting the contents of messages from network sniffing. Mac OS X Server lets you set up and manage VPN policies that support different authentication and authorization options and network connection attributes.

Mac OS X Server's VPN service serves Mac OS X, Windows, and UNIX clients, and supports strong authentication using MS-CHAP, IPSec, and Kerberos v5.

Gateway Setup Assistant

Gateway Setup Assistant automates the configuration of a simple gateway between the local network and the Internet. A gateway lets you share your server's Internet connection among computers on your local area network (LAN).

Gateway Setup Assistant automatically configures DHCP, NAT, firewall, DNS, and VPN as well as the server's network configuration. For example:

- Certain 192.168.x.x addresses are set aside for DHCP and VPN.
- A DHCP server is enabled and configured to provide addresses to computers on the LAN.
- NAT and firewall services are enabled so that all packets from the Internet except those required for connections with the server are blocked.
- A DNS server is configured as a caching server.
- A VPN server is optionally enabled for L2TP.

If you want to adjust the automatic settings after running Gateway Setup Assistant, you can do so using the Server Admin application.

"Setup Example" on page 149 describes how to use Gateway Setup Assistant in a small business.

IP Failover

You can configure IP failover to help maximize server availability.

IP failover is a way to set up a standby server that will take over if the primary server fails. The standby server takes over the IP address of the failed server, which takes the IP address back when it is online again. IP failover is useful for DNS servers, web servers hosting websites, media broadcast servers, and other servers that require minimal data replication.

Media Streaming and Broadcasting

QuickTime Streaming Server (QTSS) lets you stream multimedia in real time using the industry-standard RTSP/RTP protocols. QTSS supports MPEG-4, MP3, and QuickTime file formats.

You can deliver live and prerecorded media over the Internet to both Macintosh and Windows users, or relay streamed media to other streaming servers. You can provide unicast streaming, which sends one stream to each individual client, or multicast streaming, which sends the stream to a group of clients.

- For more information about QTSS, refer to the QuickTime website (www.apple.com/quicktime/products/qtss/).
- For information about managing streaming services on Mac OS X Server, see the QuickTime Streaming Server administration guide.

Two QuickTime applications that come with Mac OS X Server help you prepare content for streaming:

- QTSS Publisher lets you upload content to the streaming server and prepare it for delivery. It provides these key features: creation and management of playlists, generation of content directory websites, and editing of content annotations.

The QuickTime Streaming Server administration guide describes how to use QTSS Publisher.

- QuickTime Broadcaster lets you produce a live event. QuickTime Broadcaster allows you to stream live audio and video over the Internet. QuickTime Broadcaster provides preset broadcast settings and the ability to create custom settings. Built on top of the QuickTime architecture, QuickTime Broadcaster enables you to produce a live event using most codecs that QuickTime supports.

For information about QuickTime Broadcaster, go to www.apple.com/quicktime/ and navigate to the QuickTime Broadcaster page.

Application Server Support

An application server is software that runs and manages other applications, usually web applications, which are accessed using a web browser. The managed applications reside on the same computer where the application server runs.

One of the duties of the application server is to make sure the applications it manages are always available. For example, if an application fails or becomes unresponsive, the application server restarts it. Some application servers provide load balancing, which spreads application load among two or more computers.

This section highlights three integrated application server technologies that Mac OS X Server offers: Apache Tomcat, JBoss, and WebObjects. All of them are preinstalled with the server and can be used in conjunction with Apache Axis, which is also preinstalled. Axis is an open source Java framework for implementing web services over XML-based SOAP (Simple Object Access Protocol). For more information about SOAP, go to:

www.w3.org/TR/SOAP/

The web technologies administration guide provides more information about open-source applications and modules included with Mac OS X Server.

Apache Tomcat

Tomcat is an open-source JavaServer Pages (JSP)/servlet container used in the official Reference Implementation for the Java Servlet and JavaServer Pages technologies.

- The specification for Java Servlet is at java.sun.com/products/servlets/.
- The specification for JavaServer Pages is at java.sun.com/products/jsp/.

JBoss

JBoss is a widely used full-featured Java application server. It provides a full Java 2 Platform, Enterprise Edition (J2EE) technology stack with features such as:

- An Enterprise Java Bean (EJB) container
- Java Management Extensions (JMX)
- Java Connector Architecture (JCA)

Mac OS X Server provides easy-to-use graphical tools for configuring and monitoring JBoss and simplifying the deployment of JBoss applications. The JBoss administration guide describes how to manage Mac OS X Server's JBoss server. If you're interested in J2EE programming, see *Java Application Server Administration*, available from www.apple.com/server/documentation/.

- For more information about J2EE, see java.sun.com/j2ee/.
- For more information about JBoss, see www.jboss.org/.

By default, JBoss uses Tomcat as its web application container, but you can use other web application containers, such as Jetty.

WebObjects

WebObjects is the Apple solution for rapid development and deployment of ecommerce and other Internet applications. WebObjects applications can connect to multiple databases and dynamically generate HTML content. WebObjects offers a comprehensive suite of tools and run-time libraries that facilitate developing standards-based web services and Java server applications.

Mac OS X Server includes the WebObjects run-time libraries and an unlimited deployment license, making it the ideal platform for your J2EE-compatible WebObjects applications. Also provided are easy-to-use graphical tools for configuring and monitoring WebObjects from within the Server Admin application. You can optionally purchase the WebObjects development tools from the Apple Store (store.apple.com), Apple's retail stores, and authorized Apple resellers.

For more information and documentation on WebObjects, go to:

www.apple.com/webobjects/ or developer.apple.com/referencelibrary/WebObjects/

Collaboration Services

Collaboration services promote interactions among users, facilitating teamwork and productivity.

These are the collaboration services on Mac OS X Server:

- **Weblog service.** Mac OS X Server provides a multiuser Weblog server (based on Blojsom) that complies with the RSS and Atom XML standards. Weblog service supports Open Directory authentication. For additional safety, users can access Weblog service using a website that's SSL enabled.
- **iChat service.** Instant messaging for Macintosh, Linux, and Windows users is provided by a Jabber/XMPP (Extensible Messaging and Presence Protocol) server. User authentication is integrated into Open Directory. Setup and administration of iChat service is done using the graphical Server Admin application.
- **Mail service.** In addition to the features summarized in "Mail Service" on page 47, Mac OS X Server provides a graphical interface for Mailman, one of the most widely deployed mailing list managers. You can easily create and manage lists and take advantage of content filtering, digest delivery, and other options. See www.list.org for information about Mailman.
- **Group accounts, preferences, and folders.** See "Group Accounts" on page 37 for highlights.
- **File sharing.** See "File Services" on page 42 for a summary of file sharing options.

Integrating Into Existing Environments

Mac OS X Server offers many ways to interoperate with existing environments.

Open Directory offers several options for using existing directory information:

- You can use an existing Kerberos KDC or Active Directory (including Active Directory's Kerberos) to authenticate users.
- You can integrate AFP and SMB/CIFS file services with an Active Directory Kerberos environment.
- You can share information stored in an LDAPv3 directory system that's accessible from your server.
- You can retrieve configuration information from Berkeley Software Distribution (BSD) configuration files or Sun Microsystems Network Information System (NIS) files.

For Windows users, your server can:

- Provide VPN service
- Provide printer sharing
- Provide Open Directory authentication
- Act as a domain controller to provide Windows domain login and single sign-on
- Host home directories (if the home directory server is a PDC, a member of another Mac OS X Server's Windows domain, or a member of an Active Directory domain)
- Provide WINS naming service

You'll find instructions for setting up a server to work with other vendors' products in several guides:

- The Open Directory administration guide provides guidelines and instructions for integrating into existing directory systems.
- The Windows services administration guide describes how to set up print service and file services for Windows computer users, how to configure Windows options for individual users, and how to set up PDC support for Windows users.
- The Windows NT migration guide describes how to move accounts, user data, and service settings from Windows NT servers to Mac OS X Server.

High Availability

Mac OS X Server features that promote high availability include:

- Open Directory LDAP replication, including the authentication services of Open Directory Password Server and Kerberos KDC (see the Open Directory administration guide)
- Automatic restart after application, system, or power failures
- Disk space monitoring (see the command-line administration guide for information about log-rolling scripts and the `diskspacemonitor` tool)
- Software RAID, or mirroring (see Disk Utility online help)
- Journaled HFS disks (see the command-line administration guide for how to use disk journaling)

- Remote server monitoring (see Chapter 3, “Server Administration,” on page 57)
- Link aggregation (see the high availability administration guide). On some computers you can improve physical connection availability by using link aggregation. Link aggregation configures several physical network links as a single logical link to improve the capacity and availability of network connections.

High-Performance Computing

Mac OS X Server offers a high-performance, cost-effective approach to the computationally intensive processing needed for genetic research, video production, or other high-bandwidth computing.

For example, Xgrid computational service lets you achieve supercomputer performance levels by distributing computations over collections of dedicated or shared Mac OS X computers. The Xgrid cluster controller provides centralized access to the distributed computing pool, referred to as a computational cluster. The Xgrid administration guide describes how to set up and manage computational clustering.

“Computational Clustering” on page 29 provides other examples of Mac OS X Server’s support for high-performance computing.

Server Administration

Mac OS X Server provides an extensive range of tools and applications for managing your servers.

Administrators can use graphical applications or command-line tools for initial server setup, service configuration, day-to-day server management. Server administration can be conducted from a server or from a Mac OS X computer that has administration applications installed.

The next chapter, Chapter 3, “Server Administration,” tells you about the Mac OS X Server tools and applications.

Migrating and Upgrading

You can reuse data and settings you've been using on Macintosh servers earlier than version 10.4 or on Windows NT servers:

- If you're using the latest version of Mac OS X Server 10.3 or version 10.2.8 and you don't need to move to different computer hardware, you can perform an upgrade installation. Upgrading is simple because it preserves your existing settings and data.
- If you can't perform an upgrade installation, such as when you need to reformat the system disk or upgrade your server hardware, you can migrate data and settings to a computer onto which you've installed Mac OS X Server version 10.4. Migration from the latest version of 10.3; from versions 10.2.8, 10.1.4, 10.1.5, and 1.2; and from AppleShare IP version 6.3.3 are supported.
- If you want to replace a Windows NT computer with Mac OS X Server, you can migrate users, groups, files, and more.

The upgrading and migrating guide provides instructions for reusing Macintosh data and settings. The Windows NT migration guide provides instructions for migrating from a Windows NT server.

Manage Mac OS X Server using graphical applications or command-line tools.

These tools offer a diversity of approaches to server administration:

- You can administer servers locally (directly on the server you're using) or remotely, from another server, a Mac OS X computer, or a UNIX workstation.
- Graphical applications, such as Server Admin and Workgroup Manager, offer easy-to-use server administration and secure communications for remote server management. You can use these applications on Mac OS X Server (they're in `/Applications/Server/`) or on a Mac OS X computer onto which you've installed them as described in "Setting Up an Administrator Computer" on page 59.
- Command-line tools are available for administrators who prefer to use command-driven server administration. For remote server management, you can submit commands in a Secure Shell (SSH) session. You can type commands on Mac OS X Server computers and Mac OS X computers using the Terminal application, located in `/Applications/Utilities/`. You can also submit commands from a non-Macintosh computer that's been set up as described in "Using a Non-Mac OS X Computer for Administration" on page 59.

Using the Administration Tools

Information about individual administration tools can be found on the pages indicated in the following table.

Use this application or tool	To	For more information, see
Installer	Install server software or upgrade it from version 10.2 or 10.3	page 60
Server Assistant	Set up a version 10.4 server	page 60
Directory Access	Configure access to data in directories, define a search policy, and enable service discovery protocols	page 60

Use this application or tool	To	For more information, see
Workgroup Manager	Administer accounts and their managed preferences, configure share points, and set up managed network views.	page 61
Server Admin	Configure and monitor services Set up and manage QuickTime media streaming	page 67 page 74
Gateway Setup Assistant	Configure a simple gateway between two networks	page 72
System image tools	Manage NetBoot and Network Install disk images	page 73
Server Monitor	Monitor Xserve hardware	page 73
QTSS Publisher	Manage media and prepare it for streaming or progressive download	page 74
Apple Remote Desktop (optional)	Monitor and control other Macintosh computers	page 75
Command-line tools	Administer a server using a UNIX command shell	page 75
Xgrid Admin	Monitor local or remote Xgrid controllers, grids, and jobs	page 76

The next section describes how to set up a computer on which you can use these applications and tools.

Computers You Can Use to Administer a Server

When you want to administer a server locally using the graphical administration applications (they're in `/Applications/Server/`), log in to the server as a server administrator and open them.

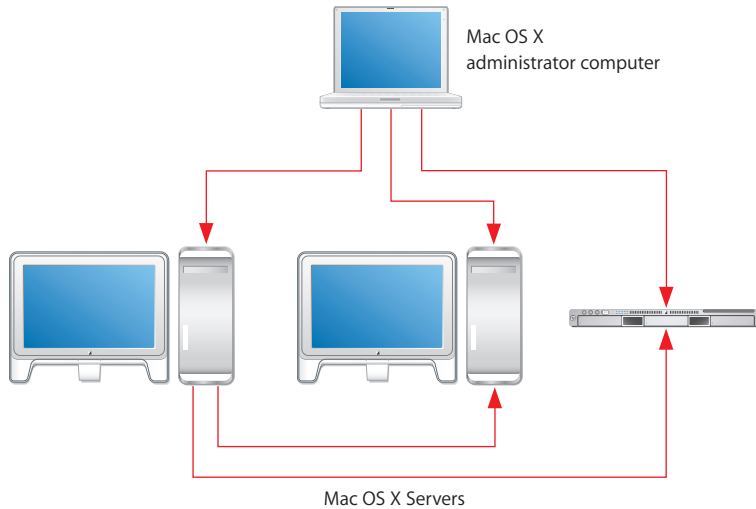
To administer a remote server, open the applications on an administrator computer. An administrator computer is any Mac OS X Server or Mac OS X version 10.4 or later computer onto which the administration tools have been installed from the *Mac OS X Server Administration Tools* CD. See "Setting Up an Administrator Computer" on page 59.

You can run command-line tools from the Terminal Application (in `/Applications/Utilities/`) on any Mac OS X Server or Mac OS X computer. You can also run command-line tools from a UNIX workstation.

Setting Up an Administrator Computer

An administrator computer is a computer with Mac OS X or Mac OS X Server version 10.4 or later that you use to manage remote servers.

In the picture below, the arrows originate from administrator computers and point to servers the administrator computers might be used to manage.



Once you've installed and set up a Mac OS X Server that has a display, keyboard, and optical drive, it's already an administrator computer. To make a computer with Mac OS X into an administrator computer, you need to install additional software.

To enable remote administration of Mac OS X Server from a Mac OS X computer:

- 1 Make sure the Mac OS X computer has Mac OS X version 10.4 or later installed.
In addition, make sure the computer has at least 128 MB of RAM and 1 GB of unused disk space.
- 2 Insert the *Mac OS X Server Administration Tools* CD.
- 3 Open the Installer folder.
- 4 Start the installer (`ServerAdmin.pkg`) and follow the onscreen instructions.

Using a Non-Mac OS X Computer for Administration

You can use a non-Mac OS X computer that offers SSH support, such as a UNIX workstation, to administer Mac OS X Server using command-line tools. See the command-line administration guide for more information.

Installer

Use the Installer to install server software on a local server from the Mac OS X Server install discs. The Installer lets you perform:

- A clean installation of Mac OS X Server, which installs version 10.4 after erasing and formatting a target disk.
- An upgrade installation, which upgrades version 10.2.8 or the latest version 10.3 servers to version 10.4 without erasing any data.
- A new installation of Mac OS X Server on a volume that has no Mac OS X system files on it.

See Chapter 6, “Installing Server Software,” for information about how to use the Installer.

Server Assistant

Server Assistant (located in `/Applications/Server/`) is used for:

- Remote server installations
- Initial setup of a local server
- Initial setup of one or more remote servers
- Preparing data for automated server setups

See Chapter 7, “Initial Server Setup,” for information about how to use Server Assistant. You can also click the Learn More button in Server Assistant for usage information.

Directory Access

Directory Access is the primary application for setting up a Mac OS X computer’s connections to Open Directory, Active Directory, and other directory domains as well as defining the computer’s search policy and service discovery protocols.

Directory Access is installed on both Mac OS X Server computers and Mac OS X computers in `/Applications/Utilities/`.

For information about how to use Directory Access, see the Open Directory administration guide or Directory Access help.

Workgroup Manager

You use Workgroup Manager to administer accounts: user accounts, group accounts, and computer lists. You also use it to set preferences for Mac OS X users, manage sharing, set up managed network views, and access the Inspector, an advanced feature that lets you do raw editing of Open Directory entries.

Information about using Workgroup Manager appears in several documents:

- The user management guide explains how to use Workgroup Manager for account and preference management. This guide also explains how to configure managed network views and how to import and export accounts.
- The file service administration guide explains how to use Sharing in Workgroup Manager to manage share points.
- The Open Directory administration guide describes how to use the Inspector.
- The Windows services administration guide describes how to use Workgroup Manager to manage users of Windows workstations.
- The print administration guide describes how to use Workgroup Manager to define print quotas for individual users.
- To retrieve online information, use the Help menu. It provides help for administration tasks you accomplish using Workgroup Manager as well as other Mac OS X Server topics.

Opening and Authenticating in Workgroup Manager

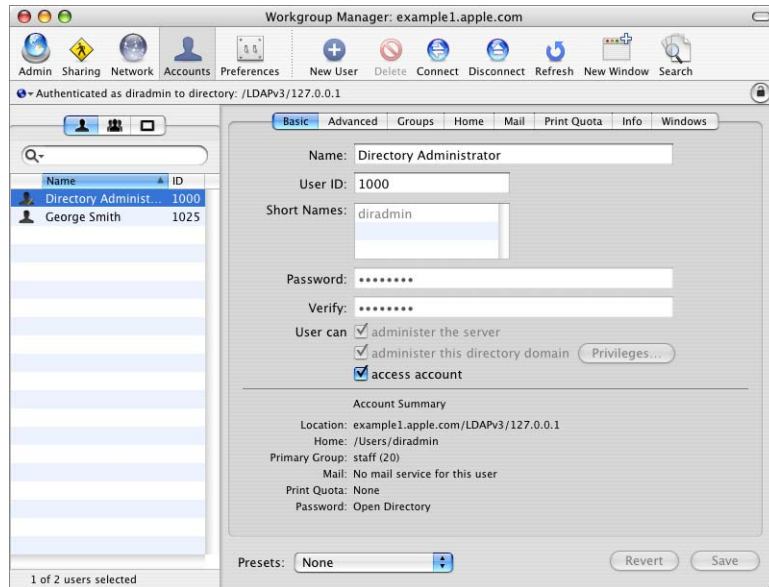
Workgroup Manager is installed in `/Applications/Server/`, from which you can open it in the Finder. Or you can open Workgroup Manager by clicking the Workgroup Manager icon in the Dock or in the toolbar of Server Admin:

- To open Workgroup Manager on the server you're using without authenticating, choose View Directories from the Server menu when you see the Workgroup Manager login dialog box. You have read-only access to information displayed in Workgroup Manager. To make changes, click the lock icon to authenticate as a server administrator. This approach is most useful when you're administering various servers and working with several directory domains.
- To authenticate as an administrator for a particular server, local or remote, enter the server's IP address or DNS name in the login dialog box, or click Browse to choose from a list of servers. Specify the user name and password for an administrator of the server, then click Connect. Use this approach when you'll be working most of the time with a particular server.

After opening Workgroup Manager, you can open a Workgroup Manager window for a different computer by clicking Connect in the toolbar or choosing Server > Connect.

Administering Accounts

After you log in to Workgroup Manager, the account window appears, showing a list of user accounts. Initially, accounts listed are those stored in the last directory node of the server's search path. When you use other Workgroup Manager windows, such as Preferences or Sharing, click Accounts in the toolbar to return to the account window.



To specify the directory or directories that store accounts you want to work with, click the small globe icon. To work with different accounts in different Workgroup Manager windows, click New Window in the toolbar.

To administer the accounts listed, click the Users, Groups, or Computer Lists button on the left side of the window. You can filter the accounts listed by using the pop-up search list above the accounts list. To refresh the accounts list, click the Refresh button in the toolbar.

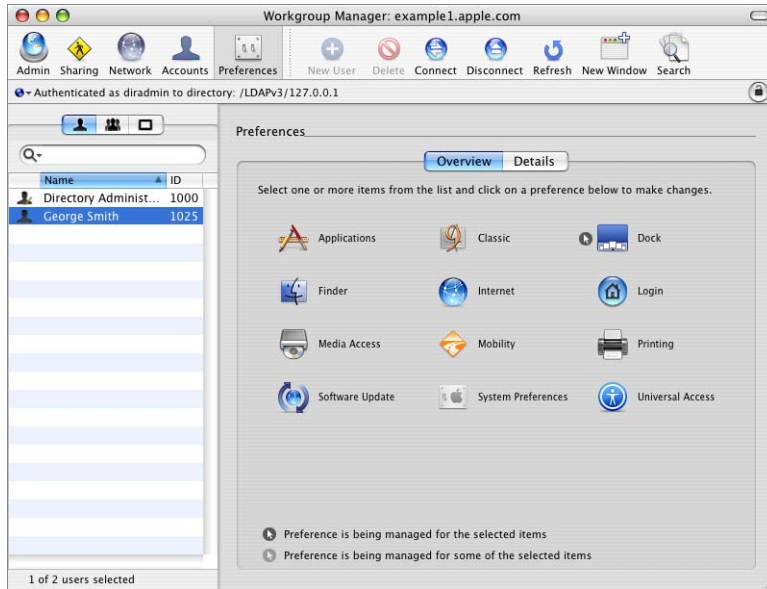
To simplify defining an account's initial attributes when you create the account, you can use presets. A preset is an account template. To create a preset, select an account, set up all the values the way you want them, then choose Save Preset from the Presets pop-up menu at the bottom of the window.

If you want to work with only accounts that satisfy very specific criteria, click Search in the toolbar. The Search features include the option for batch editing selected accounts.

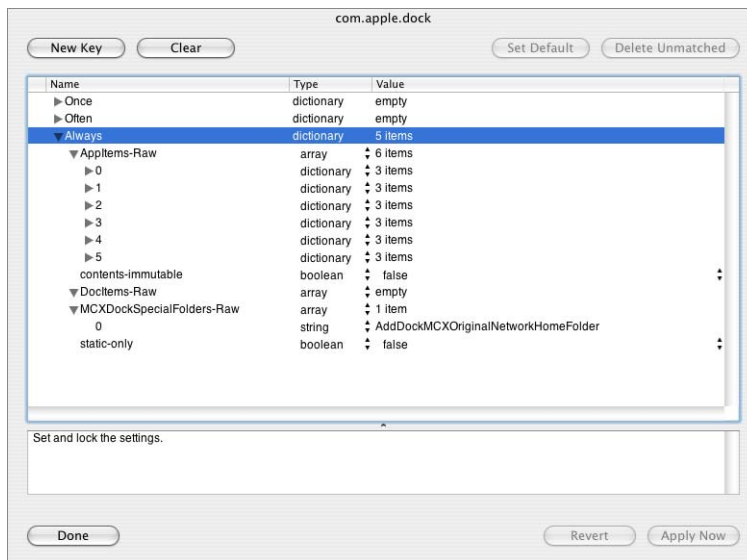
To import or export accounts, select the accounts of interest, then choose Server > Import or Server > Export, respectively.

Defining Managed Preferences

To work with managed preferences for user accounts, group accounts, or computer lists, click the Preferences icon in the Workgroup Manager toolbar.



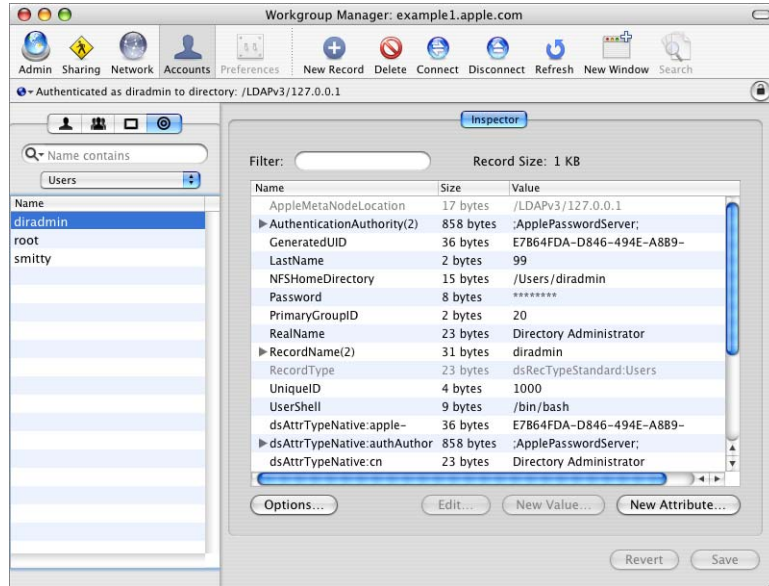
Click Details to use the preference editor to work with preference manifests.



Working With Directory Data

If you want to work with raw directory data, use Workgroup Manager's Inspector.

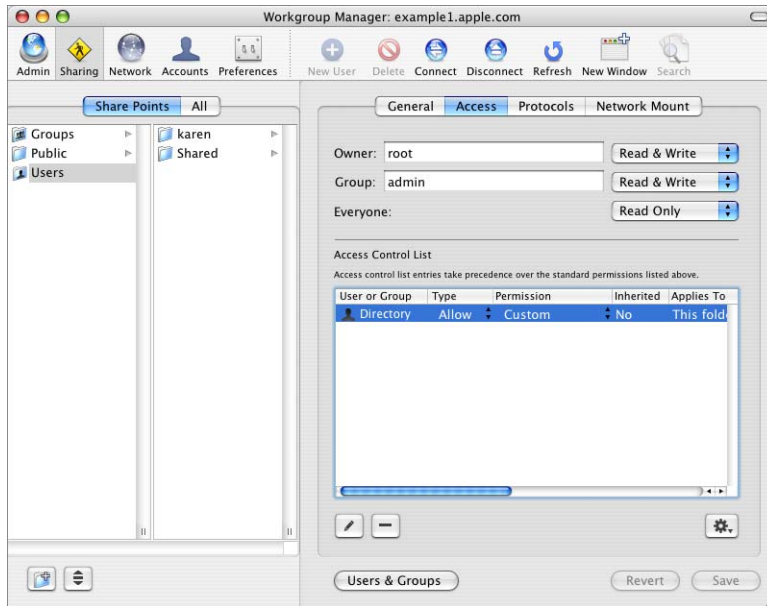
To display the Inspector, choose Workgroup Manager > Preferences. Enable "Show "All Records" tab and inspector" and click OK. Select the "All records" button (which looks like a bull's-eye) to access the Inspector.



Use the pop-up menu above the Name list to select the records of interest. For example, you can work with users, groups, computers, share points, and many other directory objects.

Managing Sharing

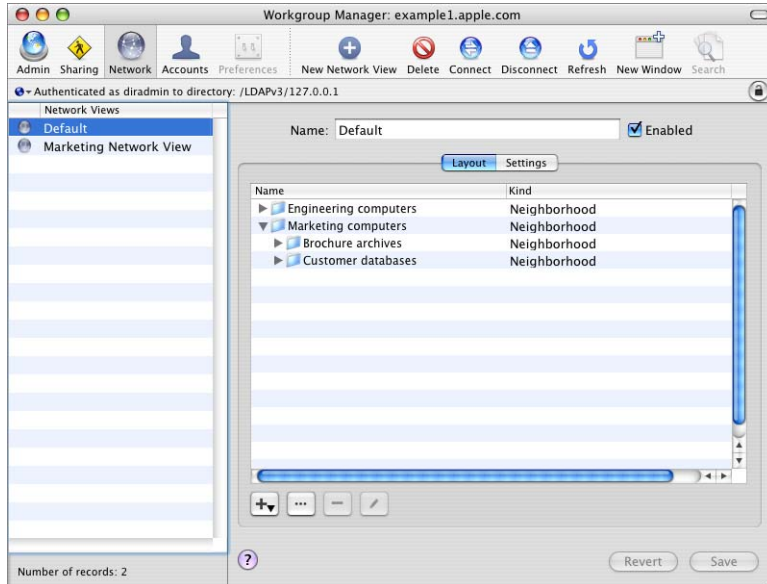
To work with share points and access control lists, click the Sharing icon in the Workgroup Manager toolbar.



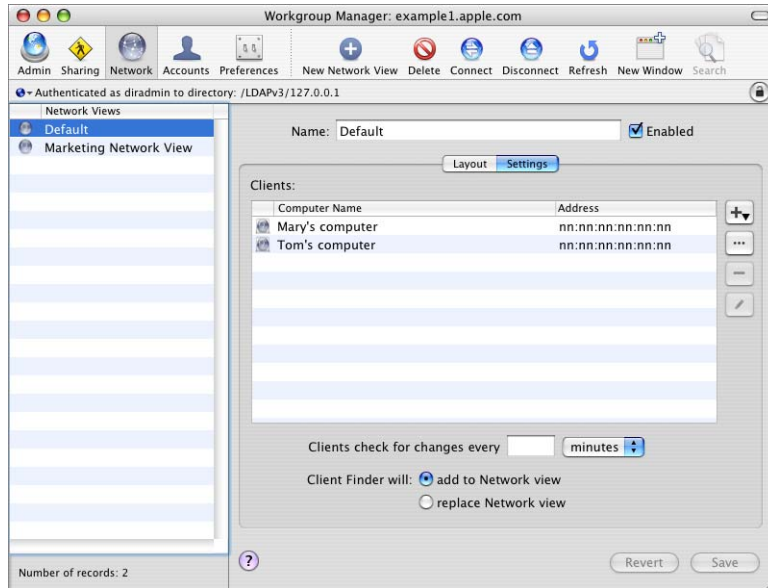
Configuring Managed Network Views

To configure how resources are listed when a user selects the Network icon in the sidebar of a Finder window, define a managed network view.

Click Network in the Workgroup Manager toolbar, then click Layout to specify the objects in the view hierarchy.



Click Settings to specify which computers should use a particular view.



Customizing the Workgroup Manager Environment

There are several ways to tailor the Workgroup Manager environment:

- You can control the way Workgroup Manager lists accounts, whether it should use SSL transactions for Sharing, and other behaviors by choosing Workgroup Manager > Preferences.
- To customize the toolbar, choose View > Customize Toolbar.
- To include predefined users and groups in the user and group lists, choose View > Show System Users and Groups.
- To open Server Admin so you can monitor and work with services on particular servers, click the Admin icon in the toolbar.

Server Admin

You use Server Admin to administer services on one or more Mac OS X Server computers. Server Admin also lets you specify settings that support multiple services, such as creating and managing SSL certificates and specifying which users and groups can access services.

Information about using Server Admin to manage services appears in the individual administration guides and in onscreen information accessible by using the Help menu in Server Admin.

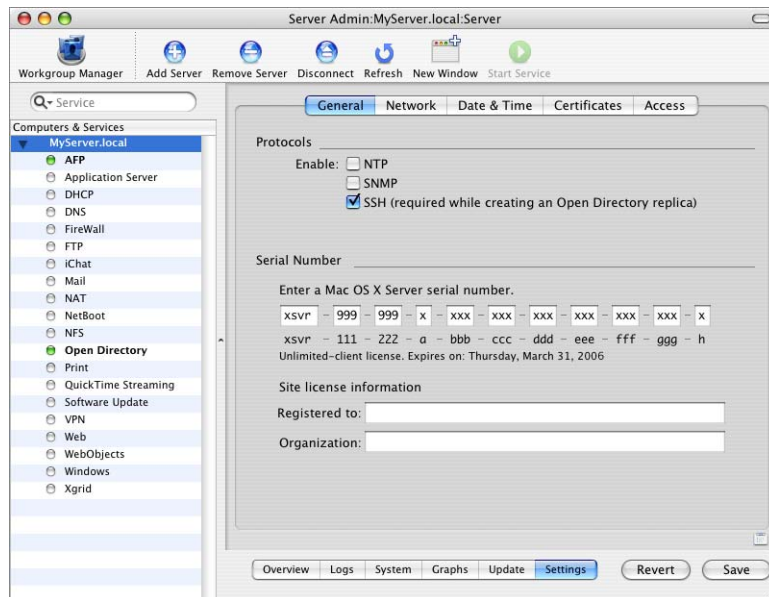
Opening and Authenticating in Server Admin

Server Admin is installed in `/Applications/Server/`, from which you can open it in the Finder. Or you can open Server Admin by clicking the Server Admin icon in the Dock or clicking the Admin button on the Workgroup Manager toolbar.

To select a server to work with, enter its IP address or DNS name in the login dialog box, or click Browse to choose from a list of servers. Specify the user name and password for an administrator, then click Connect.

Working With Specific Servers

The servers you can administer using Server Admin appear in the Computers & Services list on the left side of the application window.



To add a server to the Computers & Services list, click Add Server in the toolbar and log in to the server; the next time you open Server Admin, any server you've added is displayed in the list. To remove a server from the Computers & Services list, select the server, choose Server > Disconnect, and choose Server > Remove Server.

To limit the items that appear in the list, use the pop-up menu above the list to select the items you want listed. To change the order of servers in the list, drag a server to the new location in the list.

If a server in the Computers & Services list appears gray, double-click the server or click the Connect button in the toolbar to log in again. Check the "Add to Keychain" option while you log in to enable autoreconnect the next time you open Server Admin.

To work with general server settings, select a server in the Computers & Services list.

- Click Overview to view information about the server.
- Click Logs to view the system log and software update log.
- Click System to view information about ports and volumes the server uses.
- Click Graphs to view a pictorial history of server activity.
- Click Update to use Software Update to update the server's software.
- Click Settings to view or change the server's network settings, server software serial number, SSL certificates, service access controls, and other information.

When you click Settings, you have access to several panes:

- Click General to work with the server serial number or to enable SNMP, NTP, Macintosh Manager, or SSH.

SNMP is the abbreviation for Simple Network Management Protocol, a standard that facilitates computer monitoring and management. The server uses the open source net-snmp project for its SNMP implementation. While none of the server administration tools use or require SNMP, enabling it lets the server be monitored and managed from third-party software such as HP OpenView.

Use the NTP (Network Time Protocol) checkbox to enable NTP service. For information about NTP, see the network services administration guide.

Macintosh Manager is enabled only if an upgrade installation was used to upgrade a version 10.2 or 10.3 server to version 10.4. See "Upgrading and Migrating From an Earlier Version of Mac OS X Server" on page 94 for more information about upgrade installations.

SSH is the abbreviation for Secure Shell. The server uses the open source OpenSSH project for its SSH implementation. When you enable SSH, you can use command-line tools to remotely administer the server. SSH is also used for other remote server administration tasks, such as initial server setup, Sharing management, and displaying file system paths and the contents of folders in the server administration tools. SSH must be enabled while creating an Open Directory replica, but can be disabled afterwards.

- Click Network to view or change the server's computer name or local hostname.

The computer name is what a user sees when browsing the network (/Network). The local hostname name is usually derived from the computer name, but can be changed.

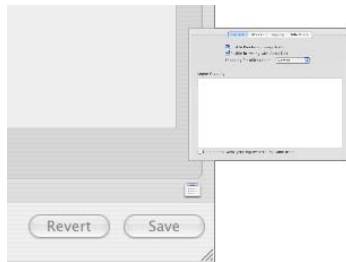
- Click Date & Time to set the server's date and time.
- Click Certificates to manage the server's SSL certificates. See "Using SSL for Remote Server Administration" on page 71 for more information.
- Click Access to control user access to some services. You can set up the same access to all services, or you can select a service and customize its access settings. Access controls are simple. Choose between letting all users and groups use services or letting only selected users and groups use services.

Administering Services

To work with a particular service on a server selected in the Computers & Services list of Server Admin, click the service in the list under the server. You can view information about a service (logs, graphs, and so forth) and manage its settings.

To start or stop a service, select it then click Start Service or Stop Service in the toolbar.

To copy service settings from one server to another or to save service settings in a property-list file for reuse later, use the drag-and-drop icon when it's visible in the lower right of the Server Admin window. Select the service whose settings you want to copy, and click Settings to display the settings. Then click the drag-and-drop icon; this action changes the icon to a miniature version of the Settings window.



To save the settings in a property-list file, drag the miniature window to your desktop or to a folder. To apply the settings on a different server, open another Server Admin window, then drag the miniature settings window to the service you want to inherit its values.

You can disable changes to service settings by unauthorized individuals by using Server Admin's view locking options.

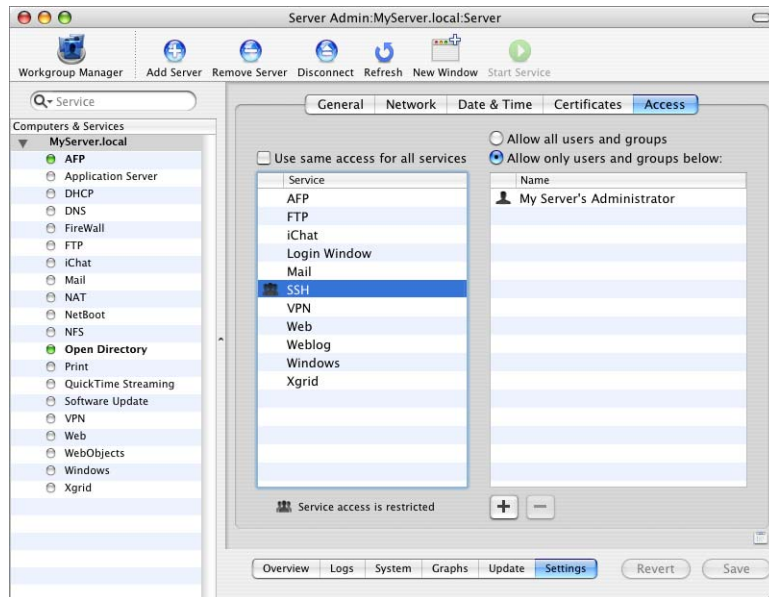
- To disable changes to service settings following a period of inactivity, choose Server Admin > Preferences. Select "Auto-lock view after" and specify the period, which is 60 minutes by default.
- To disable changes on demand, choose View > Lock View. To reenale changes, choose View > Unlock View and reauthenticate using the name and password used to log in to the system.

Important: To make sure that view locking persists after stopping then restarting Server Admin, don't store a password in the keychain. If you do, be sure to lock the keychain using the Keychain Access application.

Controlling Access to Services

You can use Server Admin to configure which users and groups can use services hosted by a server.

Select a server in the Computers & Services list, click Settings, then click Access.



You can separately specify access controls for individual services, or you can define one set of controls that applies for all services that the server hosts.

Using SSL for Remote Server Administration

You can control the level of security of communications between Server Admin and remote servers by choosing Server Admin > Preferences.

By default, "Use secure connections (SSL)" is enabled, and all communications with remote servers are encrypted using SSL. This option uses a self-signed 128-bit certificate installed in `/etc/servermgrd/ssl.crt/` when you install the server. Communications use the HTTPS protocol (port 311). If this option isn't enabled, the HTTP protocol (port 687) is used and clear text is sent between Server Admin and the remote server.

If you want a greater level of security, also select “Require valid digital signature”. This option uses an SSL certificate installed on a remote server to ensure that the remote server is a valid server. Before enabling this option, use the instructions in the mail administration guide for generating a Certificate Signing Request (CSR), obtaining an SSL certificate from an issuing authority, and installing the certificate on each remote server. Instead of placing files in `/etc/httpd/`, place them in `/etc/servermgrd/`. You can also generate a self-signed certificate and install it on the remote server.

You can use Server Admin to set up and manage self-signed or issued SSL certificates used by mail, web, Open Directory, and other services that support them. The mail service administration guide provides instructions for using Server Admin to create, organize, and use security certificates for SSL-enabled services. Individual service administration guides describe how to configure specific services to use SSL.

If you’re interested in higher levels of SSL authentication, see the information at www.modssl.org.

Customizing the Server Admin Environment

To control the Server Admin environment, you have several options.

- To control the appearance of the Server Admin lists, refresh rates, and other behaviors, choose Server Admin > Preferences.
- To customize the toolbar, choose View > Customize Toolbar.
- To add a button to the toolbar that’s a shortcut to a particular Server Admin view, go to the pane you want then choose View > Add Shortcut to View. The information displayed in the Server Admin window at the time you add the shortcut is displayed whenever you click the view in the toolbar.

Gateway Setup Assistant

Gateway Setup Assistant automates the configuration of a simple gateway between a local network and the Internet. A gateway lets you share a server’s Internet connection among computers on your local area network (LAN). Gateway Setup Assistant configures DHCP, NAT, firewall, DNS, and VPN automatically.

Run Gateway Setup Assistant from `/Applications/Server/`. Alternatively, run it from within Server Admin by choosing View > Gateway Setup Assistant.

See the network services administration guide for information about Gateway Setup Assistant.

System Image Management

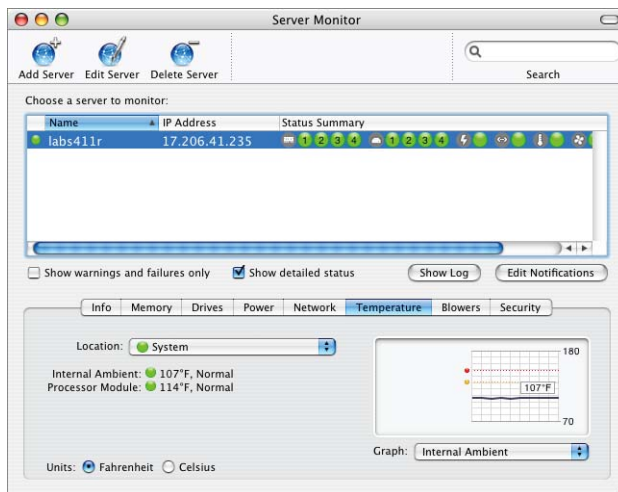
You can use the following Mac OS X Server applications to set up and manage NetBoot and Network Install images:

- System Image Utility creates Mac OS X disk images. It's installed with Mac OS X Server software in the /Applications/Server/ folder.
- Server Admin enables and configures NetBoot service and supporting services. It's installed with Mac OS X Server software in the /Applications/Server/ folder.
- PackageMaker creates package files that you use to add additional software to disk images. Access PackageMaker from Xcode 2.0. Xcode installation software is on the server install DVD in the Other Installs folder.
- Property List Editor edits property lists such as NBImageInfo.plist. Also access Property List Editor from Xcode 2.0.

The system imaging and software update administration guide provides instructions for using all these applications.

Server Monitor

You use Server Monitor to monitor local or remote Xserve hardware and trigger email notifications when circumstances warrant attention. Server Monitor shows you information about the installed operating system, drives, power supply, enclosure and processor temperature, cooling blowers, security, and network.



Server Monitor is installed in /Applications/Server/ when you install your server or set up an administrator computer. To open Server Monitor, click the Server Monitor icon in the Dock or double-click the Server Monitor icon in /Applications/Server/. From within Server Admin, choose View > Server Monitor.

To identify the Xserve server to monitor, click Add Server, identify the server of interest, and enter user name and password information for an administrator of the server.

Use the “Update every” pop-up menu in the Info pane to specify how often you want to refresh data.

Choose File > Export or File > Import to manage different lists of Xserve servers you want to monitor. Choose File > Merge to consolidate lists into one.

The system identifier lights on the front and back of an Xserve server light when service is required. Use Server Monitor to understand why the lights are on. You can also turn the lights on to identify a particular Xserve server in a rack of servers by selecting the server and clicking “System identifier light” in the Info pane.

Click Edit Notifications to set up Server Monitor to notify you by email when an Xserve server’s status changes. For each server, you set up the conditions for which you want notification. The email message can come from Server Monitor or from the server.

Server Monitor keeps logs of Server Monitor activity for each Xserve server. Click Show Log to view a log. The log shows, for example, Server Monitor attempts to contact the server and whether a connection was successful. The log also shows server status changes. (The logs don’t include system activity on the server.)

For additional information, see Server Monitor help.

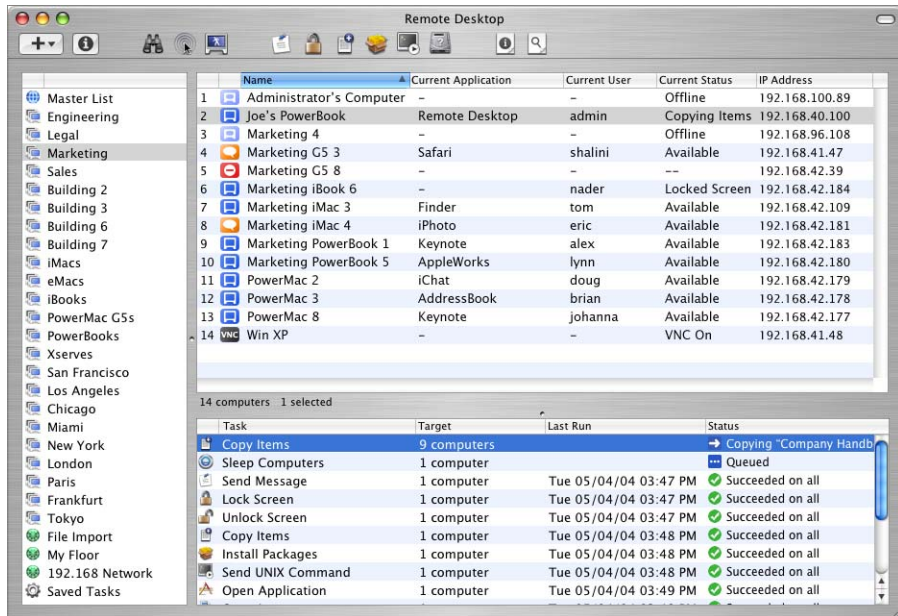
Media Streaming Management

The QTSS administration guide provides instructions for administering a QuickTime streaming server (QTSS) using Server Admin.

The QTSS administration guide also describes QTSS Publisher, an easy-to-use application for managing media and preparing it for streaming or progressive download. QTSS Publisher is installed with Mac OS X Server in /Applications/Server/. For more information, open QTSS Publisher and choose Help > QTSS Publisher Help.

Apple Remote Desktop

Apple Remote Desktop (ARD), which you can optionally purchase, is an easy-to-use network-computer management application. It simplifies the setup, monitoring, and maintenance of remote computers and lets you interact with users.



You can use ARD to control and observe computer screens. You can configure computers and install software. You can conduct one-on-one or one-to-many user interactions to provide help or tutoring. You can perform basic network troubleshooting. And you can generate reports that audit computer hardware characteristics and installed software.

For more information on Apple Remote Desktop, go to:

www.apple.com/remotedesktop/

Command-Line Tools

If you're an administrator who prefers to work in a command-line environment, you can do so with Mac OS X Server.

From the Terminal application in Mac OS X, you can use the built-in UNIX shells (sh, csh, tsh, zsh, bash) to use tools for installing and setting up server software and for configuring and monitoring services. You can also submit commands from a non-Mac OS X computer.

When managing remote servers, you conduct secure administration by working in a Secure Shell (SSH) session.

The command-line administration guide describes Terminal, SSH, server administration commands, and configuration files.

Xgrid Admin

You can use Xgrid Admin to monitor local or remote Xgrid controllers, grids, and jobs. You can add controllers and agents to monitor and specify agents that have not yet joined a grid. You also use Xgrid Admin to pause, stop, or restart jobs.

Xgrid Admin is installed in `/Applications/Server/` when you install your server or set up an administrator computer. To open Xgrid Admin, double-click the Xgrid Admin icon in `/Applications/Server/`.

For additional information, see Xgrid Admin help.

Working With Pre-Version 10.4 Computers From Version 10.4 Servers

Version 10.3 and 10.2 servers can be administered using version 10.4 server administration tools. Workgroup Manager on a version 10.4 server can be used to manage Mac OS X clients running Mac OS X version 10.2.4 or later.

Once you've edited a user record using Workgroup Manager on version 10.4, it can be accessed only by using Workgroup Manager on version 10.4.

Preferences of Mac OS 9 clients can be managed from a version 10.4 server using Macintosh Manager only when you perform an upgrade installation of version 10.4; you can use an upgrade installation to install version 10.4 on a version 10.2.8 server or the latest version 10.3 server.

Part II: Installation and Initial Setup



The chapters in this part of this guide tell you how to install server software and set up a server for the first time.

Chapter 4	Installation and Setup Overview
Chapter 5	Before You Begin
Chapter 6	Installing Server Software
Chapter 7	Initial Server Setup
Appendix A	Mac OS X Server Worksheet
Appendix B	Setup Example

Before installing and setting up Mac OS X Server, take the time to do a little planning and to become familiar with your options.

This chapter is a roadmap to details presented in later chapters. It surveys the stages of installation and initial server setup and the options available to you during each stage.



Planning

During the planning stage, you determine how you want to use Mac OS X Server and identify whether there's anything you need to accomplish before setting it up.

You may, for example, want to convert an existing server to version 10.4 and continue hosting directory, file, and mail services for clients on your network. Before you install server software, you may need to prepare data you want to migrate to your new server, and perhaps consider whether it's a good time to implement a different directory services solution.

Chapter 5, "Before You Begin," on page 91 will help you understand what you might want to do now and what you can postpone until later.

During the planning stage, you'll also decide which installation and server setup options best suit your needs. Appendix B, "Setup Example," on page 149 contains an example that illustrates server installation and initial setup in a small business scenario.

Installing Server Software

Some computers come with Mac OS X Server version 10.4 software already installed. Nonetheless, there are several times when you need to install server software, such as when you want to upgrade from a version 10.2 or 10.3 server, change a computer running Mac OS X version 10.4 into a server, or completely refresh your server environment.

You can install server software:

- From the server install discs
- From an installation image that you set up and store on disk, referred to as automated installation

Chapter 6, “Installing Server Software,” on page 99 provides detailed instructions for all the installation scenarios, which are summarized in the following sections.

Upgrading and Migrating

If you’re currently using a pre-10.4 version of the server and you want to reuse data and settings, you can upgrade or migrate to version 10.4.

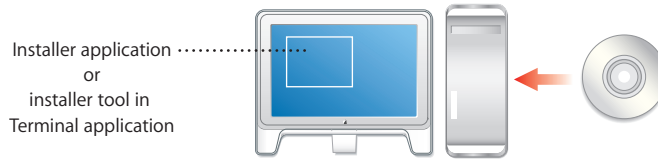
If you’re using Mac OS X Server version 10.2.8 or the latest 10.3 version and you don’t need to move to different computer hardware, you can perform an upgrade installation. Upgrading is simple because it preserves your existing settings and data. You can perform an upgrade installation using any of the installation scenarios described in the following sections.

If you can’t perform an upgrade installation, as when you need to reformat the system disk or upgrade your server hardware, you can migrate data and settings to a computer onto which you’ve installed Mac OS X Server version 10.4. Migration from the latest version 10.3 server; from versions 10.2.8, 10.1.4, 10.1.5, and 1.2; and from AppleShare IP version 6.3.3 are supported.

The upgrading and migrating guide provides complete instructions for reusing data and settings in both these scenarios.

Local Installation From the Server Install Discs

If the target server has a keyboard and display attached, and if it has an optical drive, you can start installing Mac OS X Server locally by booting the server from an install disc.



The Installer application, which automatically opens after startup, offers a graphical, guided way to install server software. See “Using Installer to Install Locally From the Install Discs” on page 103 for instructions.

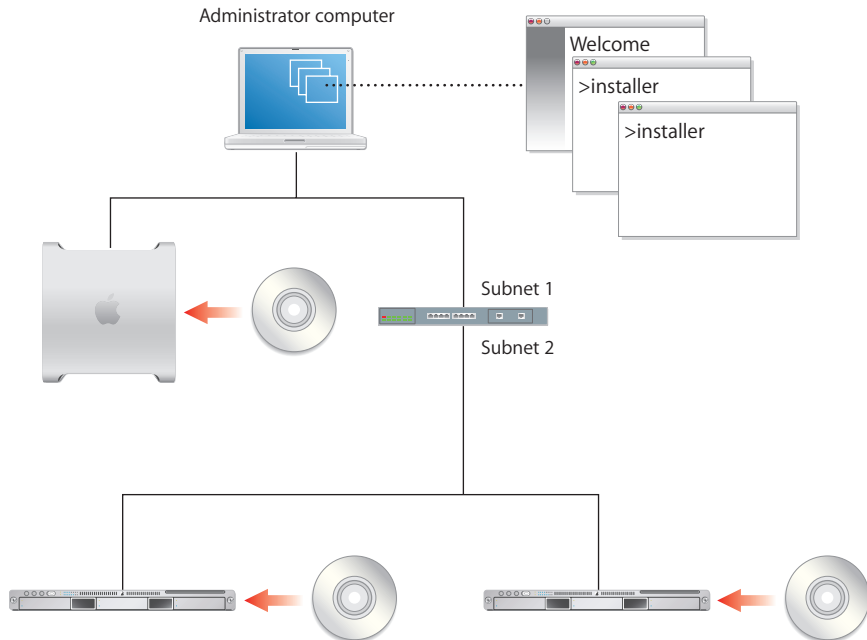
If you prefer using the command line, start the Terminal application from the Installer menu and follow the instructions in “Using the installer Command-Line Tool to Install Server Software” on page 107.

Remote Installation From the Server Install Discs

If the target server has no keyboard or display, or if it’s not the computer you’re using, you can use an administrator computer to install server software from the server install discs.

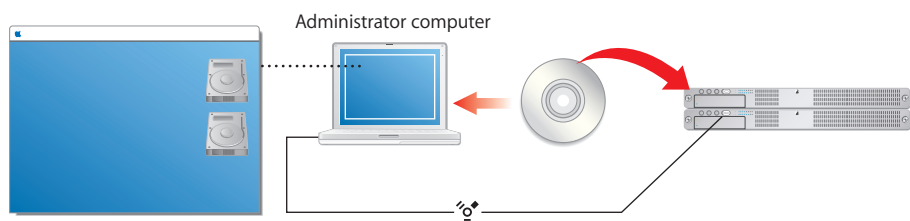
An administrator computer is a version 10.4 Mac OS X Server or version 10.4 Mac OS X computer onto which you’ve installed server management software. “Setting Up an Administrator Computer” on page 59 tells you how to set up a Mac OS X administrator computer. The target server can be on the same subnet as the administrator computer or on a different subnet.

If the target server has an optical drive, boot the server using a server install disc, then use Server Assistant from the administrator computer to initiate installation. If you have multiple servers onto which you want to install server software, you can boot each of them from an install disc, then open a Server Assistant window for each installation you want to perform. See “Using Server Assistant to Install Remotely From the Install Discs” on page 104 for instructions.



Alternatively, you can use the command line. After booting the target server, from an administrator computer, connect to the target server using SSH and follow the instructions in “Using the installer Command-Line Tool to Install Server Software” on page 107. If you have multiple servers onto which you want to install server software, boot them from an install disc, then open a Terminal window for each installation.

If the target server is an Xserve system with no built-in optical drive, you can use the optical drive on an administrator computer connected to the Xserve system using a FireWire cable.



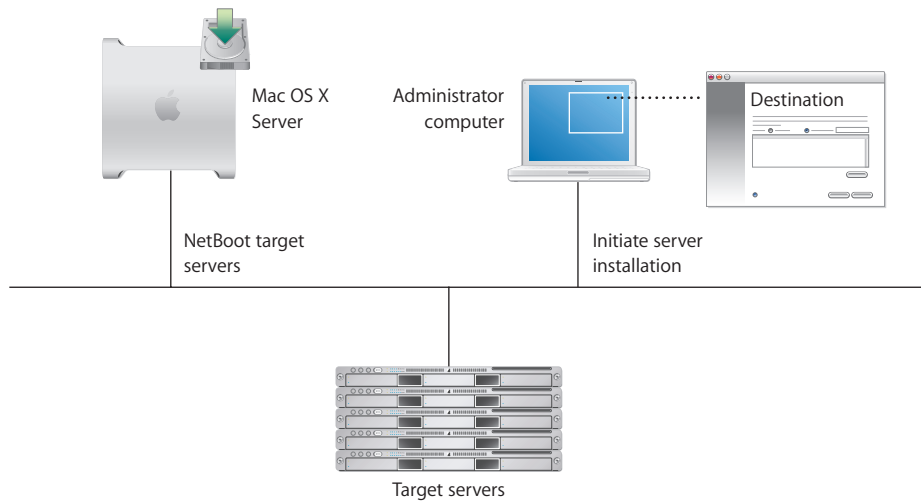
You start the Xserve in target disk mode, which is a technique that lets the target server appear as a FireWire hard disk on the administrator computer. (When you use this mode, you see a disk icon for each partition of the Xserve's hard disk on the desktop of the administrator computer.) On the administrator computer, you install from an install disc onto one of the mounted Xserve volumes. In this case, you need to complete one installation before starting another one.

There are other ways to work with an Xserve system that has no built-in optical drive. For example, you can boot the server from an external optical drive connected to the Xserve system using a FireWire cable. You can also boot the server using the optical drive from a second Xserve system. After startup in both these cases, you use an administrator computer to initiate server software installation.

Instructions for using target disk mode and external optical drives are in the *Quick Start* or *Xserve User's Guide* that comes with Xserve systems.

Automating Server Installation With a Disk Image

If you need to install server software on a large number of servers, or if you need to reinstall server software frequently, you can speed up installation by using an installation image that resides on disk rather than on the installation discs.



See the system imaging and software update administration guide for instructions on creating and deploying Network Install images created from a CD, a DVD, or an existing volume or partition. See "Automating Server Software Installation With a Disk Image" on page 106 for instructions on using these images to install the server.

Initial Server Setup

After installing server software, the next task is to set up the server.

There are several ways to set up a server:

- You can set up one or more servers interactively.
- You can automate the setup of servers by using setup data you've saved in a file or in a directory the servers are configured to access.

Chapter 7, "Initial Server Setup," on page 111 provides detailed instructions for all the server setup scenarios, summarized next following an explanation of what happens during initial server setup.

Settings Established During Initial Server Setup

During server setup, basic server settings are established:

- The language to use for server administration and the computer keyboard layout is defined.
- The server software serial number is set.
- A server administrator user is defined and the user's home directory is created. If you set the server up as an Open Directory master, a directory domain administrator for the LDAP directory is also defined.
- Default AFP and FTP share points, such as Shared Items, Users, and Groups, are defined.
- Basic Open Directory information is set up. At a minimum, a local NetInfo domain is created. You can also set up an LDAP directory for other computers to use or configure the server to obtain directory information from other servers.
- The server's host name, computer name, and local hostname are set. You can specify the computer name and local hostname, but Server Assistant automatically sets the host name to AUTOMATIC in `/etc/hostconfig`. This setting causes the server's host name to be the first name that's true in this list:

The name provided by the DHCP or BootP server for the primary IP address

The first name returned by a reverse DNS (address-to-name) query for the primary IP address

The local hostname

The name "localhost"

- Network interfaces (ports) are configured. TCP/IP and Ethernet settings are defined for each port you want to activate.
- Network time service can be set up.
- Services that require no additional configuration can be turned on. By default, to maximize security, the only server processes running after server setup are the essential ones needed for basic system function. Externally usable services, such as mail, web, and file services, are off by default and the corresponding ports are closed.

If you're upgrading, the current basic settings are displayed during the setup process, but you can change them. Other settings, such as share points you've defined and services you've configured, are preserved. See the upgrading and migrating guide for a complete description of what's upgraded and actions you may want to take following server setup.

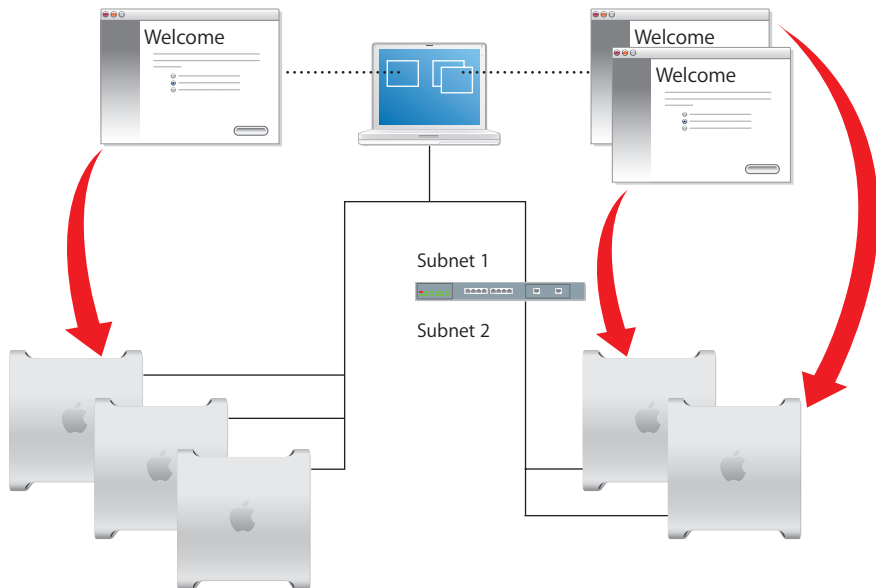
You can perform initial server setup only once without reinstalling a server. If you need to change any of the settings established during setup, you have alternative means to do so. For example, you can use Server Admin or Directory Access to manage Open Directory settings.

Setting Up Servers Interactively

The simplest way to set up a small number of servers is to use Server Assistant's guided interview process after establishing a connection with each server in turn. You provide server setup data interactively, then initiate setup immediately.

This is the technique you use to set up a local server, as "Setting Up a Local Server Interactively" on page 120 describes. You can also use this interactive approach to set up a remote server from an administrator computer. See "Setting Up a Remote Server Interactively" on page 120 for instructions.

When multiple remote servers can use the same setup data, you can supply the data, then initiate setup of all the servers at once, using a batch approach. This technique, shown on the left side of the following picture, requires that network identifiers for all the target servers be set using DHCP or BootP. See "Setting Up Multiple Remote Servers Interactively in a Batch" on page 121 for instructions.



When you want to customize the setup of individual servers, you can manage each setup individually from a different Server Assistant window. This approach is shown on the right side of the picture above. See “Setting Up Multiple Remote Servers Interactively One at a Time” on page 123 for instructions.

Although the previous picture shows target servers on the same subnet as the administrator computer in one scenario and target servers on a different subnet in the other scenario, both setup scenarios can be used to set up servers on the same and different subnets. If a target server is on a different subnet, you need to supply its IP address. Servers on the same subnet are listed by Server Assistant, so you just need to select one or more servers in the list.

Automating Server Setup

When you have more than just a few servers to set up, consider using automatic server setup. This approach also provides a way to preserve setup data so it can be reused should you need to reinstall server software.

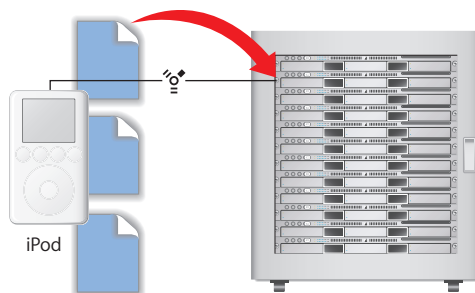
Use Server Assistant to specify setup data, then save the data in a file or in a directory. By default, saved setup data is encrypted for extra security.



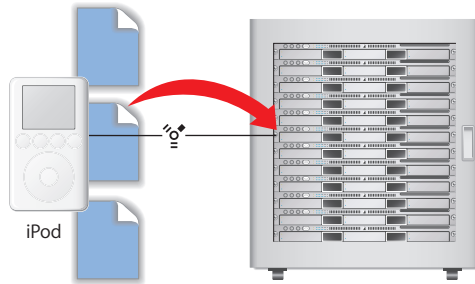
Using Setup Data Stored in a File

When you place a setup file on a volume (CD, DVD, iPod, USB solid-state drive, disk partition) mounted locally on a server you’ve installed but not set up, the server detects the file and automatically uses it to set itself up.

You could, for example, store multiple setup files on an iPod, then plug the iPod into the first server for which a setup file exists.



Then plug the iPod into the next server.



Each target server recognizes its own file, because it's been named using one of its identifiers and resides in a known location. For example, a server with WXYZ1234 as the first eight characters of its built-in serial number would use this setup file to set itself up: `/Volumes/MyIPod/Auto Server Setup/ WXYZ1234.plist`. Or a server's IP address can be used as an identifier. A server with the IP address 10.0.0.4 would use the following file: `/Volumes/MyIPod/Auto Server Setup/10.0.0.4.plist`.

You could also use a single file, which you'd name "generic.plist," to set up multiple servers if the setup data does *not* need to be unique and the servers' network identities are provided using DHCP.

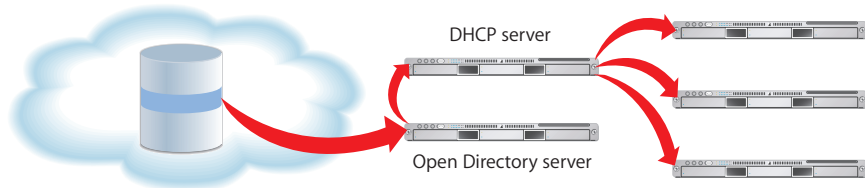
See "Setting Up Servers Automatically Using Data Saved in a File" on page 124 for instructions.

Using Setup Data Stored in a Directory

A target server can set itself up using setup data you've stored in a directory the server is configured to access.

Although storing setup data in a directory is the most automated way to set up multiple servers, this approach requires that you set up an infrastructure first so that target servers can locate the setup data stored in the directory.

The most critical components of the infrastructure are DHCP and Open Directory, as the following picture illustrates. The Open Directory server in this example hosts an LDAP directory in which setup data has been saved. The address of the Open Directory server is registered with DHCP service, running on another server in this example. The DHCP service provides the Open Directory server address to the target servers when it assigns IP addresses to those servers. The target servers automatically detect setup data that has been stored for them in the LDAP directory and use it to set themselves up.



You can save setup data in an Apple OpenLDAP directory or in another directory that supports Apple’s schema extensions for saved setup data, documented in the Open Directory administration guide.

See “Setting Up Servers Automatically Using Data Saved in a Directory” on page 127 for instructions.

Using Encryption

By default, saved setup data is encrypted for extra security. Before any server sets itself up using encrypted data, it must have access to the passphrase used when the data was encrypted.

The passphrase can be provided either interactively (using Server Assistant) or in a file on a local volume of the target server. For example, you can store the file with the passphrase on an iPod, then plug the iPod into each server that needs the passphrase. A server with the IP address 10.0.0.4 would use `/Volumes/MyiPod/Auto Server Setup/10.0.0.4.pass`.

Setting Up Services

After initial server setup is complete, you can:

- Migrate data and settings from a previous server. See the upgrading and migrating guide for instructions.
- Set up individual services you want to provide. Consult the administration guides for individual services for service-specific options. When you set up services, you’ll use the server administration tools described in Chapter 3, “Server Administration,” on page 57.

Keeping Current

After you've set up your server, you'll want to update it as Apple releases server software updates.

There are several ways to access update releases of Mac OS X Server:

- Use the Software Update pane of System Preferences.
- Use the `softwareupdate` command-line tool.
- In Server Admin, select a server in the Computers & Services list, then click the Update button.
- Use the server's software update service.
- Download a disk image of the software update from www.apple.com/support/downloads/.

Before installing and setting up Mac OS X Server, take the time to do a little planning.

The major goals of the planning phase are to make sure that:

- Server user and administrator needs are addressed by the servers you deploy
- Server and service prerequisites that affect installation and initial setup are identified

Installation planning is especially important if you're integrating Mac OS X Server into an existing network, migrating from earlier versions of Mac OS X Server, or preparing to set up multiple servers. But even single-server environments can benefit from a brief assessment of the needs you want a server to address.

Use this chapter to stimulate your thinking. It doesn't present a rigorous planning algorithm. Nor does it provide the details you'll need to determine whether to implement a particular service and assess its resource requirements. Instead, view this chapter as an opportunity to pause and think about how to maximize the benefits of Mac OS X Server in your environment.

Planning, like design, isn't necessarily a linear process. The sections in this chapter, for example, had to be in some particular order, but the order doesn't imply a mandatory sequence. Different sections in this chapter present suggestions that could be implemented simultaneously or iteratively.

Setting Up a Planning Team

Involve individuals in the installation planning process who can represent various points of view:

- What day-to-day user requirements need to be met by a server? For what activities will server users and workgroups depend on the server? If the server will be used in a classroom, make sure that the instructor who manages its services and administers it day to day provides input.

- What user management requirements need to be met? Will user computers need to be NetBooted? Will Macintosh client management and network home directories be required? Individuals with server administration experience should work with server users who may not have a technical background, so they'll appreciate how certain services might benefit them.
- What existing non-Apple services, such as Active Directory, will the server need to integrate with? If you've been planning to replace a Windows NT computer, consider using Mac OS X Server with its extensive built-in support for Windows clients. Make sure that administrators familiar with these other systems are part of the planning process.
- What are the characteristics of the network into which the server will be installed? Do you need to upgrade power supplies, switches, or other network components? Is it time to streamline the layout of facilities that house your servers? An individual with systems and networking knowledge can help with these details as well as completing the worksheet on page 137.

Identifying the Servers You'll Need to Set Up

Conduct a server inventory:

- How many servers do you currently have?
- How are they used?
- How can you streamline the use of servers you want to keep?
- Are there any existing servers that need to be retired? Which ones can Mac OS X Server replace?
- Which non-Apple servers will Mac OS X Server need to be integrated with? Why?
- Do you have any Mac OS X Server computers that need to be upgraded to version 10.4?
- How many new Mac OS X Server computers will you need to set up?

Determining Services to Host on Each Server

Identify which services you want to host on each Mac OS X Server and non-Apple server you decide to use.

How you distribute services among servers requires an understanding of both users and services. Here are a few examples of how service options and hardware and software requirements can influence what you put on individual servers:

- Directory services implementations can range from using directories and Kerberos authentication hosted by non-Apple servers to setting up Open Directory directories on servers distributed throughout the world. Directory services require thoughtful analysis and planning. The Open Directory administration guide can help you understand the options and opportunities.

- Home directories for network users can be consolidated onto one server or distributed among various servers. While you can move home directories if you need to, you may need to change a large number of user and share point records, so devise a strategy that will persist for a reasonable amount of time. See the user management guide for information about home directories.
- Some services offer ways to control the amount of disk space used by individual users. For example, you can set up both home directory and mail quotas for users. Consider whether using quotas will offer a way to maximize the disk usage on a server that stores home directories and mail databases. The user management guide and mail service administration guide describe home directory and mail quotas, respectively.
- Disk space requirements are also affected by the type of files a server hosts. Creative environments need high-capacity storage to accommodate large media files, whereas elementary school classrooms have much more modest file storage needs. The file services administration guide describes file sharing.
- If you'll be setting up a streaming media server, you'll need to allocate enough disk space to accommodate a certain number of hours of streamed video or audio. See the QuickTime Streaming Server administration guide for hardware and software requirements and for a setup example.
- The number of NetBoot client computers you can connect to a server depends on the server's Ethernet connections, the number of users, the amount of available RAM and disk space, and other factors. DHCP service needs to be available. See the system imaging and software update administration guide for NetBoot capacity planning guidelines.
- Mac OS X Server offers extensive support for Windows users. You can consolidate Windows user support on servers that provide PDC services, or you can distribute services for Windows users among different servers. The Windows services administration guide describes the options available to you.
- If you want to use software RAID to stripe or mirror disks, you'll need two or more drives (they can't be FireWire drives) on a server. See online help for Disk Utility for more information.

Before finalizing decisions about which servers will host particular services, familiarize yourself with information in the individual administration guides for services you want to deploy.

Define a Migration Strategy

If you're using a pre-version 10.4 Mac OS X Server or a Windows NT server, examine the opportunities for moving data and settings to a version 10.4 Mac OS X Server.

Upgrading and Migrating From an Earlier Version of Mac OS X Server

If you're using computers with Mac OS X Server versions earlier than 10.4, consider updating them to version 10.4.

If you're using the latest 10.3 version or version 10.2.8 and you don't need to move to different computer hardware, you can perform an upgrade installation. Upgrading is simple because it preserves your existing settings and data. If you've been using Macintosh Manager to manage Mac OS 9 client computers, you can continue to do so, an option not available when you migrate. See the documentation for your version 10.2 or 10.3 server for Macintosh Manager information.

When you can't use the upgrade approach, you can migrate data and settings. You'll need to migrate, not upgrade, when:

- A version 10.2.8 or 10.3 server's hard disk needs reformatting or doesn't meet the minimum version 10.4 system requirements. "Understanding System Requirements for Installing Mac OS X Server" on page 100 describes the minimum requirements.
- You want to move data and settings you've been using on a version 10.2.8 or 10.3 server to different server hardware.
- The server version you've been using is earlier than version 10.2.8.

Migration from the latest 10.3 version; from versions 10.2.8, 10.1.4, 10.1.5, and 1.2; and from AppleShare IP version 6.3.3 are supported. When you migrate, you install and set up a version 10.4 server, restore files onto it from the earlier server, and make some manual adjustments as required.

Read the upgrading and migrating guide for complete information.

Migrating From Windows NT

Mac OS X Server can provide a variety of services to users of Microsoft Windows 95, 98, ME, XP, NT 4, and 2000 computers. By providing these services, Mac OS X Server can replace Windows NT servers in small workgroups.

The Windows NT migration guide provides instructions for migrating users, groups, files, and more from a Windows NT server to Mac OS X Server.

Defining an Integration Strategy

Integrating Mac OS X Server into a heterogeneous environment has two aspects:

- Configuring Mac OS X Server to take advantage of existing services
- Configuring non-Apple computers to use Mac OS X Server

The first aspect primarily involves directory services integration. Identify which Mac OS X Server computers will use existing directories (such as Active Directory, LDAPv3, and NIS directories) and existing authentication setups (such as Kerberos). See the Open Directory administration guide for options and instructions. Integration may be as easy as enabling a Directory Access option, or it may involve adjusting existing services and Mac OS X Server settings.

The second aspect is largely a matter of determining the support you want Mac OS X Server to provide Windows computer users. The Windows services administration guide tells you what's available.

Defining Physical Infrastructure Requirements

Determine whether you need to make any site or network topology adjustments before installing and setting up servers.

- Who will administer the server, and what kind of server access will administrators need? Classroom servers may need to be conveniently accessible for instructors, while servers that host network-wide directory information should be secured with restricted access in a district office building or centralized computer facility.

Because Mac OS X Server administration tools offer complete remote server administration support, there are few times when an administrator should need physical access to a server.

- Are there air conditioning or power requirements that need to be met? See the documentation that comes with server hardware for this kind of information.
- Have you been thinking about upgrading elements such as cables, switches, and power supplies? Now may be a good time to do it.
- Are your TCP/IP network and subnets configured to support the services and servers you want to deploy?

Defining Server Setup Infrastructure Requirements

The server setup infrastructure consists of the services and servers that need to be set up early because other services or servers depend on them.

For example, if you'll use Mac OS X Server to provide DHCP, network time, or BootP services to other servers you'll be setting up, the server or servers that provide these services should be set up and the services running before you set up servers that depend on those services. Or if you want to automate server setup by using setup data stored in a directory, both DHCP and directory servers must be set up first.

The amount of setup infrastructure you require depends on the complexity of your site and what you want to accomplish. In general, DHCP, DNS, and directory services are desirable or required for medium-sized and larger server networks:

- The most fundamental infrastructure layer comprises network services like DHCP and DNS.

All services run better if DNS is on the network, and many services require DNS to work properly. If you're not hosting DNS, work with the administrator responsible for the DNS server you'll use when you set up your own servers. DNS requirements for individual services are published in the service-specific administration guides.

Setting up DHCP will reflect the physical network topology you'll be using.

- Another crucial infrastructure component is directory services, required for sharing data among services, servers, and user computers. The most common data you need to share is for users and groups, but configuration information such as mount records and other directory data is also shared. A directory services infrastructure is necessary when you want to host cross-platform authentication and when you want different services to share the same names and passwords.

Here's an example of the sequence in which you might set up a server infrastructure that includes DNS, DHCP, and directory services; the services can be set up on the same server or on different servers:

- 1 Set up the DNS server.
- 2 Set up DHCP.
- 3 Configure DHCP to specify the DNS server address so it can be served to DHCP clients.
- 4 Set up a directory server, including Windows PDC service if required.
- 5 Populate the directory with data, such as users, groups, and home directory data. This process involves, for example, importing users and groups, setting up share points, setting up managed preferences, and so forth.
- 6 Configure DHCP to specify the address of the directory server so it can be served to DHCP clients.

Your particular needs may affect this sequence. For example, if you want to use VPN, NAT, or IP firewall services, you would factor their setup into the DNS and DHCP setups. Appendix B, “Setup Example,” on page 149 illustrates the steps you might take to set up the directory and network infrastructure of Mac OS X Server in a small business scenario.

Making Sure Required Server Hardware Is Available

You may want to postpone setting up a server until all its hardware is in place.

For example, you might not want to set up a server whose data you want to mirror until all the disk drives on which you need to set up mirroring are available. You might also want to wait until a RAID subsystem is set up before setting up a home directory server or other server that will use it.

Minimizing the Need to Relocate Servers After Setup

Try to place a server in its final network location (subnet) before setting it up for the first time. If you’re concerned about preventing unauthorized or premature access during setup, you can set up a firewall to protect the server while finalizing its configuration.

If you can’t avoid moving a server after initial setup, you must change settings that are sensitive to network location before it can be used. For example, the server’s IP address and host name, stored in both directories and configuration files on the server, must be updated.

When you move a server, take these guidelines into account:

- Minimize the time the server is in its temporary location so the amount of information you need to change is limited.
- Postpone configuring services that depend on network settings until the server is in its final location. Such services include Open Directory replication, Apache settings (such as virtual hosts), DHCP, and other network infrastructure settings that other computers depend on.
- Wait to import final user accounts. Limit accounts to test accounts so you minimize the user-specific network information (such as home directory location) that will need to change after the move.
- After you move the server, use the `changeip` tool to change IP addresses, host names, and other data stored in Open Directory NetInfo and LDAP directories on the server. You may need to manually adjust some network configurations, such as the local DNS database, after using the tool. Because `changeip` doesn’t actually change the server’s IP address, use the `networksetup` command (or Network preferences) to change the server’s IP address in its network settings. See the command-line administration guide or the man page for `changeip` for details.

- Reconfigure the search policy of computers (such as user computers and DHCP servers) that have been configured to use the server in its original location.

Changing the Server's Host Name After Setup

When you perform initial server setup for new installations, Server Assistant sets the host name value by assigning AUTOMATIC to the hostname parameter in `/etc/hostname`. This setting causes the server's host name to be the first name that's true in this list:

- The name provided by the DHCP or BootP server for the primary IP address
- The first name returned by a reverse DNS (address-to-name) query for the primary IP address
- The local hostname
- The name "localhost"

After initial setup, if you want to change the host name, don't use the System Preferences Sharing pane to modify the server's computer name; use the `changeip` command-line tool.

See the command-line administration guide or the man page for `changeip` for details.

Changing the Server's IP Address After Setup

To change a server's IP address after initial setup, use the `changeip` tool.

Because `changeip` doesn't actually change the server's IP address, use the `networksetup` command (or Network preferences) to change the server's IP address in its network settings. See the command-line administration guide or the man page for `changeip` for details.

Determining the Installation and Setup Strategy to Use

Review the installation and server setup options in Chapter 4, "Installation and Setup Overview," on page 79.

Select the options you want to use, then address the prerequisites for installation on page 100 and for initial server setup on page 112.

Collecting and Organizing Information

For each server you set up, fill out the Mac OS X Server worksheet. It lets you record all the data you'll need to quickly move through any of the installation and setup options you decide to use.

The worksheet is located on page 137.

You can upgrade to Mac OS X Server version 10.4 from version 10.3 or 10.2 or you can install a fresh copy of Mac OS X Server version 10.4.

Review the system requirements below and record information for each server you want to install using Appendix A, “Mac OS X Server Worksheet,” on page 137. Then use the detailed installation instructions, which you’ll find as indicated in the following table.

Instructions for	Are on
“Using the Server Installation Discs”	page 100
“Upgrading and Migrating”	page 100
“Preparing Disks for Installing Mac OS X Server”	page 101
“Hardware-Specific Instructions for Installing Mac OS X Server”	page 102
“Identifying Remote Servers When Installing Mac OS X Server”	page 102
“Connecting to the Network During Installation”	page 103
“Using Installer to Install Locally From the Install Discs”	page 103
“Using Server Assistant to Install Remotely From the Install Discs”	page 104
“Installing Server Software on a Computer With Mac OS X Version 10.4 Preinstalled”	page 106
“Automating Server Software Installation With a Disk Image”	page 106
“Using the installer Command-Line Tool to Install Server Software”	page 107
“Installing Multiple Servers”	page 109

Understanding System Requirements for Installing Mac OS X Server

The computer onto which you install Mac OS X Server must have:

- A PowerPC G3, G4, or G5 processor
- Built-in FireWire
- At least 128 megabytes (MB) of random access memory (RAM). At least 256 MB of RAM is required for high-demand servers running multiple services.
- At least 4 gigabytes (GB) of disk space available

A display and keyboard are optional. You can install server software on a computer that has no display and keyboard by using an administrator computer. “Setting Up an Administrator Computer” on page 59 describes how to set one up.

Information You Need

Use Appendix A, “Mac OS X Server Worksheet,” on page 137 to record information for each server you want to install. The information below provides supplemental explanations for items on the worksheet.

Using the Server Installation Discs

You can install the server using either an install DVD or a set of install CDs.

If you install the server using CDs, only two are required. Use the third CD if you want to install optional printer drivers.

The install DVD contains everything you need to install the server, plus Xcode 2.0 installation software (in the Other Installs folder).

Both the first install CD and the install DVD also contains utilities such as Disk First Aid, Firmware Updates, and Startup Disk.

Regardless of the disc(s) you use to install server software, you’ll need the fourth CD, the *Mac OS X Server Administration Tools* CD, when you want to set up an administrator computer.

Upgrading and Migrating

If you’re using computers with Mac OS X Server versions earlier than 10.4, consider updating them to version 10.4.

If you’re using the latest 10.3 version or version 10.2.8 and you don’t need to move to different computer hardware, you can perform an upgrade installation. Upgrading is simple because it preserves your existing settings and data. If you’ve been using Macintosh Manager to manage Mac OS 9 client computers, you can continue to do so, an option not available when you migrate. See the documentation for your version 10.2 or 10.3 server for Macintosh Manager information.

When you can't use the upgrade approach, you can migrate data and settings. You'll need to migrate, not upgrade, when:

- A version 10.2.8 or 10.3 server's hard disk needs reformatting or doesn't meet the minimum version 10.4 hardware requirements. See "Understanding System Requirements for Installing Mac OS X Server" on page 100.
- You want to move data and settings you've been using on a version 10.2.8 or 10.3 server to different server hardware.
- The server version you've been using is earlier than version 10.2.8.

Migration from the latest version 10.3 server; from versions 10.2.8, 10.1.4, 10.1.5, and 1.2; and from AppleShare IP version 6.3.3 are supported. When you migrate, you install and set up a version 10.4 server, restore files onto it from the earlier server, and make some manual adjustments as required.

Read the upgrading and migrating guide for more information.

Preparing Disks for Installing Mac OS X Server

When you perform a clean installation, the target disk or partition is erased. Before erasing the target disk or partition:

- Preserve any user data you want to save by copying it to another disk or partition.
- Optionally, partition the target disk so you can install the server software on one of the partitions. The minimum recommended size for an installation partition is 4 GB.

Important: Don't store additional software or user data on the hard disk or partition where the operating system is installed. With this approach, you won't risk losing those files if you need to reinstall or upgrade system software. If you must store additional software or data on the system partition, consider mirroring the drive.

- If the target server has a second physical drive, you can configure the target disk for RAID mirroring. RAID mirroring sets up two disks so that the second disk is used automatically if the primary disk isn't available. Both disks must have a single partition. To use all your disk capacity, both disks should be the same size.

If the target disk has a single partition and the second physical drive has a single partition and no data, you can set up RAID mirroring after installation. To prevent data loss, however, it's best to set up RAID mirroring as soon as possible.

In most cases, format the target disk using Mac OS Extended (Journaled) format. You can also use Mac OS Extended or case-sensitive HFS+ format, which supports case-sensitive filenames (useful for legacy UNIX applications, for example). Disks formatted as case-sensitive HFS+ are also journaled.

You can format a disk or partition as Mac OS Extended (Journaled) from the Installer application. Use the Disk Utility application to apply the Mac OS Extended format. To format a disk or a partition as case-sensitive HFS+, use the Terminal application. For example:

- 1 Choose a Mac OS Extended volume (for example, /Volumes/MyHFSPlus) to convert to case-sensitive HFS.
- 2 Open the Terminal application.
- 3 Erase and reformat the volume as bootable; in this example MyCaseSensitive is the new volume name:

```
sudo diskutil eraseVolume "Case-sensitive HFS+" MyCaseSensitive  
bootable /Volumes/MyHFSPlus
```

See the man page for `diskutil` and the command-line administration guide for additional information on creating a case-sensitive HFS+ volume.

Instructions provided later in this chapter describe when to perform disk preparation tasks.

Hardware-Specific Instructions for Installing Mac OS X Server

When you install server software on Xserve systems, the procedure you use when starting the computer for installation is specific to the kind of Xserve hardware you have. You may need to refer to the *Xserve User's Guide* or *Quick Start* that came with your Xserve, where these procedures are documented.

Identifying Remote Servers When Installing Mac OS X Server

For remote server installations, you need to know this information about the target server:

- The identity of the target server.

When using Server Assistant, you need to be able to recognize the target server in a list of servers on your local subnet or enter the IP address of the server (in IPv4 format: 000.000.000.000) if it resides on a different subnet.

Information provided for servers in the list include IP address, host name, and Mac (Media Access Control) address (also called hardware or Ethernet address). The IP address is assigned by a DHCP server on the network; if no DHCP server exists, the target server uses a 169.xxx.xxx.xxx address unique among servers on the local subnet. Later, when you set up the server, you can change the IP address.

- The preset password for the target server.

The password consists of the first 8 digits of the server's built-in hardware serial number. To find a server's serial number, look for a label on the server. Older computers have no built-in hardware serial numbers; for these systems, use 12345678.

Connecting to the Network During Installation

If you want to use a server as an Open Directory master, make sure it has an active Ethernet connection before installation and initial setup.

Installing Server Software Interactively From the Install Discs

You can use the install discs to install server software interactively on a local server on a remote server, or on a computer with Mac OS X preinstalled.

Using Installer to Install Locally From the Install Discs

You can install Mac OS X Server directly onto a computer with a display, a keyboard, and an optical drive attached.

To install server software locally:

- 1 If you'll be performing a clean installation rather than upgrading, preserve any user data that resides on the disk or partition onto which you'll install the server software.
 - 2 Turn on the computer and insert the first Mac OS X Server install disc into the optical drive.
 - 3 Restart the computer while holding down the C key on the keyboard. The computer boots from the install disc. You can release the C key when you see the Apple logo.
 - 4 After the computer restarts, choose the language you want the server to use and click Continue.
 - 5 When Installer opens, if you want to perform a clean installation, optionally use the Utilities menu to open Disk Utility or Terminal to prepare the target disk before proceeding. Use Disk Utility to format the disk as Mac OS Extended. Use the `diskutil` command in Terminal to format it as case-sensitive HFS+.
- Important:** Don't store additional software or user data on the hard disk or partition where the operating system is installed. With this approach, won't risk losing those files if you need to reinstall or upgrade system software. If you must store additional software or data on the system partition, consider mirroring the drive.
- 6 Proceed through the Installer's panes by following the onscreen instructions.
 - 7 When the Select a Destination pane appears, select a target disk or volume (partition) and make sure it's in the expected state.

If you're doing a clean installation, you can choose Utilities > Open Disk Utility or Utilities > Open Terminal to work with disk preparation one final time before selecting the target volume and clicking Continue. Or you can click Options to format the destination disk or volume in Mac OS Extended (Journaled) format; select Erase to format the disk in Mac OS Extended (Journaled) format; then click OK.

If the volume you selected contains the latest 10.3 server version or version 10.2.8 and you want to upgrade, click Options and select “Don’t erase.” Click OK.

Important: When you perform an upgrade installation, make sure that saved setup data won’t be inadvertently detected and used by the server. If saved setup data is used, existing server settings will be overwritten by the saved settings. See “How a Server Searches for Saved Setup Data” on page 112 for more information.

- 8 During installation, progress information is displayed. Insert the next installation disc if prompted.

After installation is complete, the server restarts automatically and you can perform initial server setup. Chapter 7, “Initial Server Setup,” on page 111 describes how.

Using Server Assistant to Install Remotely From the Install Discs

To install Mac OS X Server on a remote server from the server install discs, you need access to the target computer and an administrator computer from which to manage the installation.

To install to a remote server using the install discs:

- 1 If you’ll be performing a clean installation rather than upgrading, preserve any user data that resides on the disk or partition onto which you’ll install the server software. Then optionally use Disk Utility or Terminal locally (in /Applications/Utilities/) to prepare the target disk. Use Disk Utility to format the disk as Mac OS Extended. Use the `diskutil` command in Terminal to format it as case-sensitive HFS+.

Important: Don’t store additional software or user data on the hard disk or partition where the operating system is installed. With this approach, you won’t risk losing those files if you need to reinstall or upgrade system software. If you must store additional software or data on the system partition, consider mirroring the drive.

- 2 Start the target computer from the first install disc. The procedure you use depends on the target server hardware.

If the target server has a keyboard and an optical drive, insert the first install disc into the optical drive. Then hold down the C key on the keyboard while restarting the computer.

If the target server is an Xserve with a built-in optical drive, start the server using the first install disc by following the instructions in the *Xserve User’s Guide* for starting from a system disc.

If the target server is an Xserve with no built-in optical drive, you can start it in target disk mode and insert the install disc into the optical drive on your administrator computer. You can also use an external FireWire optical drive or an optical drive from another Xserve system to start the server from the install disc. Instructions for using target disk mode and external optical drives are in the *Quick Start* guide or *Xserve User’s Guide* that came with your Xserve system.

3 On an administrator computer, navigate to /Applications/Server/ and open Server Assistant (you don't have to be an administrator on the local computer to use Server Assistant). Select "Install software on a remote server."

4 Identify the target server.

If it's on the local subnet, select it in the list.

Otherwise, click "Server at IP Address" and enter an IP address in IPv4 format (000.000.000.000).

5 When prompted for a password, type the first 8 digits of the server's built-in hardware serial number. To find a server's serial number, look for a label on the server.

If you're installing on an older computer that has no built-in hardware serial number, use 12345678 for the password.

6 Proceed by following the onscreen instructions.

7 When the Volumes pane appears, select a target disk or volume (partition) and make sure it's in the expected state. Then select it and click Continue.

If the volume you selected contains the latest 10.3 server version or version 10.2.8 and you want to upgrade, select "Don't erase." Otherwise, you can select Erase to format the disk in Mac OS Extended (Journaled) format. Click OK.

Important: When you perform an upgrade installation, make sure that saved setup data won't be inadvertently detected and used by the server. If saved setup data is used, existing server settings will be overwritten by the saved settings. See "How a Server Searches for Saved Setup Data" on page 112 for more information.

During installation, progress information is displayed. Insert the next installation disc if prompted.

While installation proceeds, you can open another Server Assistant window to install server software on another computer; choose File > New Window to do so.

After installation is complete, the target server restarts automatically and you can perform initial server setup. Chapter 7, "Initial Server Setup," on page 111 describes how.

Installing Server Software on a Computer With Mac OS X Version 10.4 Preinstalled

Follow these instructions to install server software on a computer that came with Mac OS X version 10.4 installed.

To install server software on your computer:

- 1 Start up the computer from the hard disk, as you would for normal use. Do not use an install disc.
- 2 If the server install discs are CDs, insert the second install disc and double-click MacOSXServerInstall.mpkg to run the Installer.
If the server install disc is a DVD, insert the DVD, open the Other Installs folder, and double-click MacOSXServerInstall.mpkg to run the Installer.
- 3 When the Installer finishes, your computer restarts automatically and Server Assistant opens to let you set up the server.
- 4 After the server restarts, use the Software Update System preference to install any available server software updates.

Automating Server Software Installation With a Disk Image

If you need to install server software on a large number of servers or if you need to reinstall server software frequently, you can automate installation by using an installation image that resides on disk rather than on the installation discs.

To install server software using a disk image:

- 1 On a version 10.4 Mac OS X Server, open System Image Utility.
- 2 Create a Network Install image from the server installation CDs or DVD or from a “model” version 10.4 server you’ve already set up.
- 3 Use Server Admin to start NetBoot service and enable the disk image.
- 4 NetBoot each target computer so it starts up using the disk image.
- 5 Open Server Assistant and choose “Install software on a remote server,” then identify the NetBooted computers when you get to the Destination pane.
- 6 Proceed as you would to install server software on any remote computer.

The system imaging and software update administration guide describes how to create and deploy disk images.

Using the installer Command-Line Tool to Install Server Software

You use the `installer` tool to install server software on a local or remote computer from the command line. For detailed information about `installer`:

- See the command-line administration guide.
- Open the Terminal application and type `installer`, `installer -help`, or `man installer`.

To use `installer` to install server software:

- 1 Start the target computer from the first install CD or the install DVD. The procedure you use depends on the target server hardware.

If the target server has a keyboard and an optical drive, insert the first install disc into the optical drive. Then hold down the C key on the keyboard while restarting the computer.

If the target server is an Xserve with a built-in optical drive, start the server using the first install disc by following the instructions in the *Xserve User's Guide* for starting from a system disc.

If the target server is an Xserve with no built-in optical drive, you can start it in target disk mode and insert the install disc into the optical drive on your administrator computer. You can also use an external FireWire optical drive or an optical drive from another Xserve system to start the server from the install disc. Instructions for using target disk mode and external optical drives are in the *Quick Start* guide or *Xserve User's Guide* that came with your Xserve system.

- 2 If you're installing a local server, when Installer opens choose Utilities > Open Terminal to open the Terminal application.

If you're installing a remote server, from Terminal on an administrator computer or from a UNIX workstation, establish an SSH session as the root user with the target server, substituting the target server's actual IP address for `<ip address>`:

```
ssh root<ip address>
```

If you don't know the IP address and the remote server is on the local subnet, you can use the `sa_srchr` command to identify computers on the local subnet on which you can install server software:

```
/System/Library/Serversetup/sa_srchr 224.0.0.1  
mycomputer.example.com#PowerMac4,4#<ip address>#<mac address>#Mac OS  
X Server 10.4#RDY4PkgInstall#2.0#512
```

You can also use Server Assistant to generate information for computers on the local subnet. Open Server Assistant, select "Install software on a remote computer," and click Continue to access the Destination pane and generate a list of servers awaiting installation.

- 3 When prompted for a password, type the first 8 digits of the server's built-in hardware serial number. To find a server's serial number, look for a label on the server. If the target computer had been set up as a server, you'll also find the hardware serial number in `/System/Library/ServerSetup/SerialNumber`.

If you're installing on an older computer that has no built-in hardware serial number, use 12345678 for the password.

- 4 Identify the target-server volume onto which you want to install the server software. To list the volumes available for server software installation from the install discs, type this command:

```
/usr/sbin/installer -volinfo -pkg /System/Installation/Packages/  
OSInstall.mpkg
```

You can also identify a Network Install image you've created and mounted:

```
/usr/sbin/installer -volinfo -pkg /Volumes/ServerNetworkImage10.4/  
System/Installation/Packages/OSInstall.mpkg
```

The list displayed reflects your particular environment, but here's an example showing three available volumes:

```
/Volumes/Mount 01  
/Volumes/Mount1  
/Volumes/Mount02
```

- 5 If the target volume has the latest 10.3 server version or version 10.2.8 installed, when you run `installer` it will upgrade the server to version 10.4 and preserve user files. If you're not upgrading but performing a clean installation, back up the user files you want to preserve, then use `diskutil` to erase the volume and format it and to enable journaling:

```
/usr/sbin/diskutil eraseVolume HFS+ "Mount 01" "/Volumes/Mount 01"  
/usr/sbin/diskutil enableJournal "/Volumes/Mount 01"
```

You can also use `diskutil` to partition the volume and to set up mirroring. See the `diskutil` man page for more information about the command.

Important: Don't store data on the hard disk or hard disk partition where the operating system is installed. With this approach, you won't risk losing data should you need to reinstall or upgrade system software. If you must store additional software or data on the system partition, consider mirroring the drive.

- 6 Install the operating system on a volume from the list generated in step 4. For example, to use Mount 01 in the example in step 4 to install from a server install disc, type:

```
/usr/sbin/installer -verboseR -lang en -pkg /System/Installation/  
Packages/OSInstall.mpkg -target "/Volumes/Mount 01"
```

If you're using a Network Install image, the command identifies them as step 4 shows.

When you type the `-lang` parameter, use one of the following values: `en` (for English), `de` (for German), `fr` (for French), or `ja` (for Japanese).

- 7 During installation, progress information is displayed. While installation proceeds, you can open another Terminal window to install server software on another computer.
- 8 When installation from the disc is complete, restart the server. Type:

```
/sbin/reboot
```

or

```
/sbin/shutdown -r
```

If you're using CDs to install the server, use the next two steps to install the remaining software from the remaining install CDs.

Server Assistant opens automatically when installation is complete.

- 9 To use the next install disc, type the `sa_srchr` command to locate the server that's waiting. For `<ip address>`, specify the address you used in step 2:

```
/System/Library/Serverssetup/sa_srchr <ip address>
```

- 10 When the `sa_srchr` response includes the string `"#InstallInProgress"`, insert the next installation disc:

```
mycomputer.example.com#PowerMac4,4#<ip address>#<mac address> #Mac OS  
X Server 10.4#InstallInProgress#2.0#2080
```

Installing Multiple Servers

After using Server Assistant to initiate server software installation on one remote computer, choose `File > New Window` to install the software on another computer.

Alternatively, open the Terminal application and use the `installer` tool to initiate another server software installation.

Basic characteristics of your Mac OS X Server are established during initial server setup.

Here's a quick reference to the topics in this chapter.

To read about	See	On
Options and prerequisites	"Saving Setup Data"	page 112
	"Specifying Initial Open Directory Usage"	page 116
	"Connecting to the Network During Initial Server Setup"	page 119
	"Configuring Servers With Multiple Ethernet Ports"	page 119
Collecting information	The Mac OS X Server Worksheet	page 137
Setting up servers interactively	"Using Interactive Server Setup"	page 119
	"Setting Up a Local Server Interactively"	page 120
	"Postponing Local Server Setups Following Installation"	page 120
	"Setting Up a Remote Server Interactively"	page 120
	"Setting Up Multiple Remote Servers Interactively in a Batch"	page 121
	"Setting Up Multiple Remote Servers Interactively One at a Time"	page 123
Setting up servers automatically	"Using Automatic Server Setup"	page 124
	"Setting Up Servers Automatically Using Data Saved in a File"	page 124
	"Setting Up Servers Automatically Using Data Saved in a Directory"	page 127
Monitoring and troubleshooting	"Determining the Status of Setups"	page 130
What to do after initial setup	"Setting Up Services"	page 131

Information You Need

See Appendix A, “Mac OS X Server Worksheet,” on page 137 to understand and record information for each server you want to set up. The information below provides supplemental explanations for some of the items on the worksheet.

When you’re upgrading from Mac OS X Server version 10.2.8 or the latest 10.3 version, Server Assistant displays the existing server settings, but you can change them. Use the worksheet to record settings you want the version 10.4 server to use.

Saving Setup Data

When you want to work with saved setup data, determine a strategy for naming, encrypting, and storing the data.

How a Server Searches for Saved Setup Data

A freshly installed server sets itself up using saved setup data it finds while using the following search sequence. When the server finds any saved setup data that matches the criteria described, it stops searching and uses the data to set itself up.

- 1 The server first searches through locally mounted volumes for setup files in `/Volumes/*/Auto Server Setup/`, where `*` is a file system (device) name. It searches through volumes alphabetically by device name, looking for a file with the extension `.plist` that’s named using its MAC address, its IP address, its partial DNS name, its built-in hardware serial number, its fully qualified DNS name, its partial IP address, or `generic.plist`, in that order.
- 2 Next, the server looks in a directory it’s configured to use for a setup record in a path named `“AutoServerSetup”`. It searches for records named using its MAC address, its IP address, its partial DNS name (`myserver`), its built-in hardware serial number, its fully qualified DNS name (`myserver.example.com`), its partial IP address, or `“generic,”` in that order.

If the setup data is encrypted, the server needs the correct passphrase before setting itself up. You can use Server Assistant to supply the passphrase interactively, or you can supply the passphrase in a text file in `/Volumes/*/Auto Server Setup/<pass-phrase-file>`. The target server searches through volumes alphabetically by file system name, looking for a file with the extension `.pass` that’s named using its MAC address, its IP address, its partial DNS name, its built-in hardware serial number, its fully qualified DNS name, its partial IP address, or `generic`, in that order.

Important: When you perform an upgrade installation, make sure that saved setup data won’t be inadvertently detected and used by the server you’re upgrading. If saved setup data is used, existing server settings will be overwritten by the saved settings.

The next two sections provide more details about how to use saved setup data.

Using Setup Data Saved in a File

When you save setup data in a file, a target server automatically detects and uses the file if:

- Setup data the target server recognizes isn't found in a directory the server is configured to use. See "Using Setup Data Saved in a Directory" on page 114 for information on how a server detects and uses directory data to set itself up.
- The setup file is on a volume mounted locally in `/Volumes/*/Auto Server Setup/`, where `*` is any device mounted under `/Volumes`. A target server searches through volumes alphabetically by device name.

The device that is mounted as a file system can be the server's hard drive or an iPod, DVD, CD, FireWire drive, USB drive, or other device plugged in to the server. For example, `/Volumes/AdminiPod/Auto Server Setup/myserver.example.com.plist`.

- The setup file name is one of these; when searching for setup files, target servers search for names in the order listed:

`<MAC-address-of-server>.plist` (include any leading zeros but omit colons). For example, `0030654dbcef.plist`.

`<IP-address-of-server>.plist`. For example, `10.0.0.4.plist`.

`<partial-DNS-name-of-server>.plist`. For example, `myserver.plist`.

`<built-in-hardware-serial-number-of-server>.plist` (first 8 characters only). For example, `ABCD1234.plist`.

`<fully-qualified-DNS-name-of-server>.plist`. For example, `myserver.example.com.plist`.

`<partial-IP-address-of-server>.plist`. For example, `10.0.plist` (matches `10.0.0.4` and `10.0.1.2`).

`generic.plist` (a file that any server will recognize, used to set up servers that need the same setup values). If the serial number specified in the file isn't site licensed, after setup you need to manually set it. Use Server Admin or the following command in the Terminal application: `serversetup -setServerSerialNumber`.

- The correct passphrase is provided to the server if the setup data is encrypted.

You can use Server Assistant to supply a passphrase interactively, or you can supply the passphrase in a text file. Place the passphrase file on a volume mounted locally on the target server in `/Volumes/*/Auto Server Setup/<pass-phrase-file>`.

The passphrase file can have one of these names; target servers search for names in the order listed:

`<MAC-address-of-server>.pass` (include any leading zeros but omit colons). For example, `0030654dbcef.pass`.

`<IP-address-of-server>.pass`. For example, `10.0.0.4.pass`.

`<partial-DNS-name-of-server>.pass`. For example, `myserver.pass`.

<built-in-hardware-serial-number-of-server>.pass (first 8 characters only). For example, ABCD1234.pass.

<fully-qualified-DNS-name-of-server>.pass. For example, myserver.example.com.pass.

<partial-IP-address-of-server>.pass. For example, 10.0.pass (matches 10.0.0.4 and 10.0.1.2).

generic.pass (a file that any server will recognize). If the server software serial number isn't site licensed, after setup you need to manually set it. Use Server Admin or the following command in Terminal: `serversetup -setServerSerialNumber`.

If you want to reuse saved setup data after reinstalling a server, you can store the server's setup file(s) in a small local partition that isn't erased when you reinstall the server. The setup files are automatically detected and reused after each reinstallation.

Using Setup Data Saved in a Directory

Using this approach offers the most unattended way to set up multiple servers, but it requires that you have a DHCP and directory infrastructure in place.

Using Server Assistant, you save setup data to an existing directory the computer you're using is configured to access and from which you want newly installed servers to retrieve setup data. The schema of the directory must support stored setup data. Open Directory has built-in support for stored setup data. If you want to store setup data in a non-Apple directory, you first need to extend its schema as the Open Directory administration guide describes.

When you save setup data in a directory, a target server automatically detects and uses the setup data if:

- The target server receives its network names (host name, computer name, and local hostname) and its port configuration from a DHCP server.
- The DHCP server is configured to identify the IP address of the directory server where the setup data resides. See the network services administration guide for DHCP server configuration instructions.
- The directory and DHCP servers are running.
- The setup data is stored in the directory in a path named `/AutoServerSetup/` and a record having one of these names; target servers search for names in the order listed:

<MAC-address-of-server> (include any leading zeros but omit colons). For example, 0030654dbcef.

<IP-address-of-server>. For example, 10.0.0.4.

<partial-DNS-name-of-server>. For example, myserver.

<built-in-hardware-serial-number-of-server> (first 8 characters only). For example, ABCD1234.

<fully-qualified-DNS-name-of-server>. For example, myserver.example.com.

<partial-IP-address-of-server>. For example, 10.0 (matches 10.0.0.4 and 10.0.1.2).

generic (a record that any server will recognize, used to set up servers that need the same setup values). If the serial number specified in the file isn't site licensed, after setup you need to manually set it. Use Server Admin or the following command in the Terminal application: `serversetup -setServerSerialNumber`.

- The correct passphrase is provided to the server (setup data stored in a directory should always be encrypted).

You can use Server Assistant to supply a passphrase interactively, or you can supply the passphrase in a text file. Place the passphrase file on a volume mounted locally on the target server in `/Volumes/*/Auto Server Setup/<pass-phrase-file>`, where `*` is any device mounted under `/Volumes`. A target server searches through volumes alphabetically by device name.

The passphrase file can have one of these names; target servers search for names in the order listed:

<MAC-address-of-server>.pass (include any leading zeros but omit colons). For example, 0030654dbcef.pass.

<IP-address-of-server>.pass. For example, 10.0.0.4.pass.

<partial-DNS-name-of-server>.pass. For example, myserver.pass.

<built-in-hardware-serial-number-of-server>.pass (first 8 characters only). For example, ABCD1234.pass.

<fully-qualified-DNS-name-of-server>.pass. For example, myserver.example.com.pass.

<partial-IP-address-of-server>.pass. For example, 10.0.pass (matches 10.0.0.4 and 10.0.1.2).

generic.pass (a file that any server will recognize). If the server software serial number isn't site licensed, after setup you need to manually set it. Use Server Admin or the following command in Terminal: `serversetup -setServerSerialNumber`.

Keeping Backup Copies of Saved Setup Data

Saved setup data isn't only useful for automating the setup of multiple servers. It also provides a way to set up servers again if you ever need to reinstall server software on them.

You can keep backup copies of setup data files on a network file server. Alternatively, you can store setup data files in a local partition that won't be erased when you reinstall server software.

Specifying Initial Open Directory Usage

When you set up a server initially, you specify its directory services configuration.

Choices are:

- **No change**, available only when upgrading from Mac OS X Server version 10.2.8 or the latest 10.3 version.
- **Standalone Server**, used to set up only a local NetInfo directory domain on the server.
- **Open Directory Master**, used to set up an LDAP directory on the server for other computers to share.
- **Connected to a Directory System**, used to set up the server to obtain directory information from a shared directory domain that's already been set up on another server.

In all these cases, Open Directory authentication is set up on the server and used by default for any new users added to domains that reside on the server.

If you're setting up multiple servers and one or more of them will host a shared directory, set up those servers before setting up servers that will use those shared directories.

Note: If you connect Mac OS X Server version 10.4 to a directory domain of Mac OS X Server version 10.2 or earlier, be aware that users defined in the older directory domain cannot be authenticated with the MS-CHAPv2 method. This method may be required to securely authenticate users for the VPN service of Mac OS X Server version 10.4. Open Directory in Mac OS X Server version 10.4 supports MSCHAPv2 authentication, but Password Server in Mac OS X Server version 10.2 doesn't support MS-CHAPv2.

After setup, use the Directory Access or Server Admin applications to refine the server's directory configuration, if necessary. Directory Access lets you set up connections to multiple directories, including Active Directory and other non-Apple directory systems, and specify a search policy (the order in which the server should search through the domains). Server Admin lets you set up replicas of an Open Directory master and manage other aspects of a server's directory service configuration.

The Open Directory administration guide can help you decide which of the directory usage setup options is right for you. If you're upgrading, the best choice is usually "No change," and if you're setting up a new server, the simplest choice is "Standalone Server." After initial server setup, you can use Directory Access or Server Admin to adjust and finalize the directory setup.

Not Changing Directory Usage When Upgrading

When setting up a server that you're upgrading to version 10.4 from the latest 10.3 version or from version 10.2.8, and you want the server to use the same directory setup it's been using, choose "No change" in the Directory Usage pane in Server Assistant.

Even when you want to change the server's directory setup, selecting "No change" is the safest option, especially if you're considering changing a server's shared directory configuration. Changing from hosting a directory to using another server's shared directory or vice versa, or migrating a shared NetInfo domain to LDAP are examples of directory usage changes you should make *after* server setup in order to preserve access to directory information on your network.

See the Open Directory administration guide for information about all the directory usage options available to you and how to use Directory Access and Server Admin to make directory changes. See the upgrading and migrating guide for information on how to continue using existing directory data when you change directory service settings.

If you choose the "No change" option and the server wasn't using a Password Server, Open Directory authentication will be set up. When you add users to any Apple directory domain residing on the server, their passwords are validated by default using Open Directory authentication.

Setting Up a Server as a Standalone Server

When you don't want the server you're setting up to host or use shared directory information, choose the directory usage option called Standalone Server in Server Assistant. This option sets up only a local NetInfo domain on the server. Because it's a local domain, the data stored in it is accessible only to the server you're setting up.

Open Directory authentication is also set up on the server. By default, Open Directory authentication is used when a user is added to the local domain.

When a user attempts to log in to the server or use one of its services that require authentication, the server authenticates the user by consulting the local database. If the user has an account on the system and supplies the appropriate password, authentication succeeds.

Setting Up a Server as an Open Directory Master

When you want a server you're setting up to host an LDAP directory for use by itself and other computers, make sure the server is connected to the network when you set it up and choose the directory usage option called Open Directory Master in Server Assistant. This option:

- Sets up an LDAP directory on the server.
- Creates a directory domain administrator for the directory. This is the administrator who has the privileges required to change information stored in the directory, such as accounts and managed network views.
- Turns on Open Directory authentication for validating all users defined in the local NetInfo domain and the LDAP directory.

- Sets up a Kerberos KDC on the server. Before an Open Directory master can provide Kerberos and single sign-on authentication, DNS must be properly configured. DNS must resolve the fully qualified DNS names of all servers, including the Open Directory master itself, to their IP addresses and provide the corresponding reverse lookups.
- Optionally enables a Windows Primary Domain Controller on the server, letting your server authenticate and provide home directories for users of computers with Windows NT4.x, Windows 9x, and Windows XP.

To set up another server as an Open Directory replica and optional backup domain controller (BDC) for a PDC, use Server Admin after setup is complete. To configure additional directory connectivity, use Directory Access. See the Open Directory administration guide for more information about directory configuration.

Open Directory authentication is set up on the server and used by default for any users added to domains that reside on the server.

Setting Up a Server to Connect to a Directory System

When you want a server you're setting up to use a shared directory on another computer, choose the directory usage option called Connected to a Directory System in Server Assistant. Then choose one of the following options:

- **As Specified by DHCP Server**, which sets up a server to use a DHCP server to obtain information for connecting to a directory system. The DHCP server must be set up to provide the address and search base of an LDAP server (DHCP option 95) or the address and tag of a legacy NetInfo server. The directory service and DHCP service are independent; they don't have to be provided by the same server.
- **Open Directory Server**, which lets you indicate that the address of the Mac OS X Server hosting the LDAP directory should be obtained using DHCP or specify the IP address or DNS name of the server.
- **NetInfo Server**, which lets you indicate how the server being set up should locate the server hosting a shared domain. Choose one or more of these: Broadcast, DHCP, and Static IP Address, the last of which requires that you supply the NetInfo server's IP address and the NetInfo tag of the directory domain, usually "network."
- **Other Directory Server**, which is the selection to make when you want to configure access to non-Apple directories such as Active Directory, Novell eDirectory, or an NIS domain. After server setup, use Directory Access to specify the server's directory configuration. See the Open Directory administration guide for more information.

You can set up a server to connect to a shared NetInfo directory on Mac OS X Server version 10.0 and later or an LDAP directory on version 10.2 or version 10.3. However, you may not be able to take advantage of some features:

- VPN service on version 10.3 or later requires MS-CHAP2 authentication, which isn't available with version 10.2 and earlier.
- Replication isn't supported by version 10.2 or earlier.

- Kerberos configuration is much more complex on version 10.2. In addition, automatic synchronization of Kerberos and Password Server requires version 10.3 or later.
- On version 10.3 and earlier, trusted directory binding, support for LDAP subdomains, and directory access controls aren't available.

Connecting to the Network During Initial Server Setup

Try to place a server in its final network location (subnet) before setting it up for the first time. If you're concerned about preventing unauthorized or premature access during setup, you can set up a firewall to protect the server while you're finalizing its configuration.

If you can't avoid moving a server after initial setup, you must change settings that are sensitive to network location before it can be used. For example, the server's IP address and host name, stored in both directories and configuration files on the server, must be updated. See "Changing the Server's Host Name After Setup" on page 98 for more information.

Configuring Servers With Multiple Ethernet Ports

Your server has a built-in Ethernet port and may have additional Ethernet ports built in or added on.

When you're using Server Assistant to interactively set up one or more servers, all of a server's available Ethernet ports are listed and you select one or more to activate and configure. When you work in Server Assistant's offline mode, you click an Add button to manually create a list of ports to configure.

If you enable more than one port, you specify the order in which the ports should be used by the server when routing traffic to the network. While the server receives network traffic on any active port, network traffic initiated by the server is routed through the first active port.

See Appendix A, "Mac OS X Server Worksheet," on page 137 for a description of port configuration attributes.

Using Interactive Server Setup

When you have only a few servers to set up, the interactive approach is useful.

To use this approach, open Server Assistant, connect to one or more target servers, supply setup data, then initiate the setup immediately.

You can use the interactive approach to set up a local server, a remote server, or several remote servers.

Setting Up a Local Server Interactively

After server software has been installed on a server, you can use the interactive approach to set it up locally if you have physical access to the computer.

To set up a local server interactively:

- 1 Fill out the Mac OS X Server worksheet. The worksheet is on page 137. Supplemental information appears in “Information You Need” on page 112.
- 2 When the server is restarted, Server Assistant opens automatically.
- 3 Enter the setup data you’ve recorded on the worksheet as you move through the Assistant’s panes, following the onscreen instructions. Make sure that any DHCP or DNS servers you specify for the server you’re setting up to use are running.
- 4 After all setup data has been entered, Server Assistant displays a summary of the data.
- 5 Review the setup data you entered. Optionally click Go Back to change it.
- 6 To save the setup data as a text file or in a form you can use for automatic server setup (a saved setup file or saved directory record), click Save As.
To encrypt the file or record, select “Save in Encrypted Format” then enter and verify a passphrase. You must supply the passphrase before an encrypted setup file can be used by a target server.
- 7 To initiate setup of the local server, click Apply.

When server setup is complete, click Restart Now. Now you can log in as the server administrator user created during setup to configure services.

Postponing Local Server Setups Following Installation

After installation of server software on a local computer is complete, the computer restarts and Server Assistant opens automatically.

If you want to postpone server setup until a later time, press Command-Q. The computer shuts down. When it’s restarted, Server Assistant opens automatically.

Setting Up a Remote Server Interactively

After server software has been installed on a server, you can use the interactive approach to set it up remotely from an administrator computer that can connect to the target server.

To set up a remote server interactively:

- 1 Fill out the Mac OS X Server worksheet. The worksheet is on page 137. Supplemental information appears in “Information You Need” on page 112.
- 2 Make sure the target server is running.
- 3 On an administrator computer, open Server Assistant. It’s in /Applications/Server/. You don’t have to be an administrator on the administrator computer to use Server Assistant.

- 4 In the Welcome pane, select “Set up a remote server” and click Continue.
- 5 In the Destination pane, put a check in the Apply column for the remote server you want to set up, then type its preset password in the Password field and click Continue to connect to the server.

If you don't see the target server on the list, click Add to add it or Refresh to determine whether it's available.
- 6 In the Language pane, specify the language you want to use to administer the target server.
- 7 Use step 8 if you want to use saved setup data. Otherwise, use step 9.
- 8 In the Language pane, choose File > Open Configuration File or File > Open Directory Record to load the saved setup data you want to use. If the saved setup data is encrypted, type the passphrase when prompted.

Optionally choose View > Jump to Review to review the setup data, then use Go Back as necessary to change it.
- 9 Click Continue and enter the setup data as you move through the Assistant's panes, following the onscreen instructions. Make sure that any DHCP or DNS servers you specify for the server you're setting up to use are running.
- 10 After all setup data has been specified, review the summary displayed by Server Assistant and optionally click Go Back to change data.
- 11 To save the setup data as a text file or in a form you can use for automatic server setup (a saved setup file or saved directory record), click Save As.

To encrypt the file or record, select “Save in Encrypted Format” then enter and verify a passphrase. You must supply the passphrase before an encrypted setup file can be used by a target server.
- 12 To initiate setup of the remote target server, click Apply.

When server setup is complete, click Continue Now. The target server restarts automatically and you can log in as the server administrator user created during setup to configure services.

Setting Up Multiple Remote Servers Interactively in a Batch

You can use the interactive approach to set up multiple servers as a batch if:

- All the servers are accessible from an administrator computer
- All the servers use the same setup data except for server software serial numbers and network identities (host name, computer name, and local hostname)
- Network identities are provided by a DHCP or BootP server

To set up multiple remote servers interactively in a batch:

- 1 Fill out the Mac OS X Server worksheet with settings you want to use for all servers you want to set up. The worksheet is on page 137. Supplemental information appears in “Information You Need” on page 112.
- 2 Make sure the target servers and any DHCP or DNS servers you want them to use are running.
- 3 On an administrator computer that can connect to all the target servers, open Server Assistant. It’s located in /Applications/Server/. You don’t have to be an administrator on the administrator computer to use Server Assistant.
- 4 In the Welcome pane, select “Set up a remote server” and click Continue.
- 5 In the Destination pane, put a check in the Apply column for each remote server you want to set up. Then type the preset password in the Password field for each server and click Continue to connect to the servers.

If you don’t see a target server you want to set up on the list, click Add to add it.

- 6 In the Language pane, specify the language you want to use to administer the target servers.
- 7 Use step 8 if you want to use saved setup data. Otherwise, use step 9.
- 8 In the Language pane, choose File > Open Configuration File or File > Open Directory Record to load the saved setup data you want to use. If the saved setup data is encrypted, type the passphrase when prompted.
Optionally choose View > Jump to Review to review the setup data, then use Go Back as necessary to change it.
- 9 Click Continue and enter the setup data as you move through the Assistant’s panes, following the onscreen instructions. When prompted, enter the server software serial number for each target server.
- 10 After all setup data has been specified, review the summary displayed by Server Assistant and optionally click Go Back to change data.
- 11 To save the setup data as a text file or in a form you can use for automatic server setup (a saved setup file or saved directory record), click Save As.

To encrypt the file or record, select “Save in Encrypted Format” then enter and verify a passphrase. You must supply the passphrase before an encrypted setup file can be used by a target server.

- 12 To initiate server setup, click Apply.

When server setup is complete, click Continue Now. The target servers restart automatically and you can log in as the server administrator user created during setup to configure their services.

Setting Up Multiple Remote Servers Interactively One at a Time

You can use the interactive approach to set up multiple servers by using multiple Server Assistant windows on an administrator computer.

To set up multiple remote servers interactively one at a time:

- 1 Fill out the Mac OS X Server worksheet for each server you want to set up. The worksheet is on page 137. Supplemental information appears in “Information You Need” on page 112.
- 2 Make sure the target servers and any DHCP or DNS servers you want them to use are running.
- 3 On an administrator computer that can connect to all the target servers, open Server Assistant. It's located in /Applications/Server/. You don't have to be an administrator on the administrator computer to use Server Assistant.
- 4 In the Welcome pane, select “Set up a remote server” and click Continue.
- 5 In the Destination pane, check one of the remote servers you want to set up. Then type the preset password in the Password field for the server and click Continue to connect to the server.

If you don't see the server you want to set up on the list, click Add to add it.

- 6 In the Language pane, specify the language you want to use to administer the target server.
- 7 Use step 8 if you want to use saved setup data. Otherwise, use step 9.
- 8 In the Language pane, choose File > Open Configuration File or File > Open Directory Record to load the saved setup data you want to use. If the saved setup data is encrypted, type the passphrase when prompted.
Optionally choose View > Jump to Review to review the setup data, then use Go Back as necessary to change it.
- 9 Click Continue and enter the setup data as you move through the Assistant's panes, following the onscreen instructions.
- 10 After all setup data has been specified, review the summary displayed by Server Assistant and optionally click Go Back to change data.
- 11 To save the setup data as a text file or in a form you can use for automatic server setup (a saved setup file or saved directory record), click Save As.

To encrypt the file or record, select “Save in Encrypted Format” then enter and verify a passphrase. You must supply the passphrase before an encrypted setup file can be used by a target server.

- 12 To initiate server setup, click Apply.

- 13 To work with another server's setup before the setup you started is complete, choose File > New Window and repeat steps 4 through 12.

When its setup is complete, the target server restarts automatically and you can log in as the server administrator user created during setup to configure its services.

Using Automatic Server Setup

The automatic approach is useful when you:

- Have more than just a few servers to set up.
- Want to prepare for setting up servers that aren't yet available.
- Want to save setup data for backup purposes.
- Need to reinstall servers frequently.

One way to use this approach is to use Server Assistant's offline mode, which lets you work with setup data without connecting to specific servers. You specify setup data, then save it in a file or in a directory accessible from target servers, as the next two sections describe. Target servers on which Mac OS X Server version 10.4 software has been installed automatically detect the presence of the saved setup information and use it to set themselves up.

You can define generic setup data. Generic setup data can be used to set up *any* server. For example, you might want to define generic setup data for a server that's on order, or to configure 50 Xserve computers you want to be identically configured. Alternatively, you can save setup data that's specifically tailored for a particular server.

Important: When you perform an upgrade installation, make sure that saved setup data won't be inadvertently detected and used by the server. If saved setup data is used, existing server settings will be overwritten by the saved settings. See "How a Server Searches for Saved Setup Data" on page 112. for more information.

Setting Up Servers Automatically Using Data Saved in a File

After server software has been installed on a server, you can set it up automatically using data saved in a file.

To save and apply setup data in a file:

- 1 Fill out the Mac OS X Server worksheet for each server you want to set up. The worksheet is on page 137. Supplemental information appears in "Information You Need" on page 112.
- 2 On an administrator computer, open Server Assistant. It's in /Applications/Server/. You don't need to be an administrator on the administrator computer to use Server Assistant.
- 3 In the Welcome pane, select "Save setup information in a file or directory record" to work in offline mode, which doesn't require a server connection.

- 4 In the Language pane, specify the language you want to use to administer the target server or servers.
- 5 If you want to create a new setup file, use step 6. If you want to work with a setup file that already exists, use step 7.

If you intend to create a generic setup file because you want to use the file to set up more than one server, don't specify network names (computer name and local hostname) and make sure that each network interface (port) is set to be configured "Using DHCP" or "Using BootP."

- 6 Click Continue and enter the setup data as you move through the Assistant's panes, following the onscreen instructions.
- 7 In the Language pane, choose File > Open Configuration File or File > Open Directory Record to load the saved setup data you want to work with. If the saved setup data is encrypted, type the passphrase when prompted.

Optionally choose View > Jump to Review to review the setup data, then use Go Back as necessary to change it.

- 8 In the Network Interfaces pane, click Add to specify network interfaces.
- 9 After all the setup data has been specified, review the summary displayed by Server Assistant and optionally click Go Back to change data.

- 10 Click Save As, then select "Configuration File."

- 11 To encrypt the file, select "Save in Encrypted Format" then enter and verify a passphrase.

You must supply the passphrase before an encrypted setup file can be used by a target server.

- 12 Click OK, navigate to the location where you want to save the file, name the file using one of the following options, and click Save; when searching for setup files, target servers search for names in the order listed:

<MAC-address-of-server>.plist (include any leading zeros but omit colons). For example, 0030654dbcef.plist.

<IP-address-of-server>.plist. For example, 10.0.0.4.plist.

<partial-DNS-name-of-server>.plist. For example, myserver.plist.

<built-in-hardware-serial-number-of-server>.plist (first 8 characters only). For example, ABCD1234.plist.

<fully-qualified-DNS-name-of-server>.plist. For example, myserver.example.com.plist.

<partial-IP-address-of-server>.plist. For example, 10.0.plist (matches 10.0.0.4 and 10.0.1.2).

generic.plist (a file that any server will recognize, used to set up servers that need the same setup values).

- 13 Place the file in a location where the target server or servers can detect it.

A server can detect a setup file if it resides on a volume mounted locally in `/Volumes/*/Auto Server Setup/`, where `*` is any device mounted under `/Volumes`. The device can be the server's hard drive or an iPod, DVD, CD, FireWire drive, USB drive, or other device plugged into the server.

For example, if you have an iPod named AdminiPod, the path used would be `/Volumes/AdminiPod/Auto Server Setup/<setup-file-name>`.

- 14 If the setup data is encrypted, make the passphrase available to the target server or servers. You can supply the passphrase interactively, using Server Assistant, or you provide it in a text file.

To provide the passphrase in a file, use step 15. To provide it interactively, use step 16.

- 15 To provide a passphrase in a file, create a new text file and type the passphrase for the saved setup file on the first line. Save the file using one of the following names; target servers search for names in the order listed:

`<MAC-address-of-server>.pass` (include any leading zeros but omit colons). For example, `0030654dbcef.pass`.

`<IP-address-of-server>.pass`. For example, `10.0.0.4.pass`.

`<partial-DNS-name-of-server>.pass`. For example, `myserver.pass`.

`<built-in-hardware-serial-number-of-server>.pass` (first 8 characters only). For example, `ABCD1234.pass`.

`<fully-qualified-DNS-name-of-server>.pass`. For example, `myserver.example.com.pass`.

`<partial-IP-address-of-server>.pass`. For example, `10.0.pass` (matches `10.0.0.4` and `10.0.1.2`).

`generic.pass` (a file that any server will recognize).

Put the passphrase file on a volume mounted locally on the target server in `/Volumes/*/Auto Server Setup/<pass-phrase-file>`, where `*` is any device mounted under `/Volumes`.

- 16 To provide a passphrase interactively, use Server Assistant on an administrator computer that can connect with the target server.

In the Welcome or Destination pane, choose `File > Supply Passphrase`. In the dialog box, enter the target server's IP address, password, and the passphrase.

Click `Send`.

- 17 If you're using a generic setup file, and the serial number isn't site licensed, after setup you must specify the server's serial number by using Server Admin or the command line. In Server Admin, select the server, click Settings, and click General. Alternatively, in the Terminal application, use ssh to connect with the server and type the `serversetup -setServerSerialNumber` command.

See the command-line administration guide for a description of the layout of a saved setup file and more information about the `serversetup` command.

Setting Up Servers Automatically Using Data Saved in a Directory

After server software has been installed on a server, you can set it up automatically using data saved in a directory. This method requires a pre-existing directory and DHCP infrastructure, as the procedure below describes.

To save and apply setup data in a directory record:

- 1 Make sure that the directory in which you want to save setup data exists, that its schema supports stored setup data, and that it's accessible from the administrator computer you're using. The Open Directory administration guide describes how to set up and access directories. It also describes the schema for stored setup data. Stored setup data support is built into Apple OpenLDAP directories, but the schema of other directories needs to be extended to support stored setup data.
- 2 Fill out the Mac OS X Server worksheet for each server you want to set up. The worksheet is on page 137. Supplemental information appears in "Information You Need" on page 112.
- 3 On an administrator computer, open Server Assistant. It's in `/Applications/Server/`. You don't have to be an administrator on the administrator computer to use Server Assistant.
- 4 In the Welcome pane, select "Save setup information in a file or directory record" to work in offline mode, which doesn't require a server connection.
- 5 In the Language pane, specify the language you want to use to administer the target server or servers.
- 6 If you want to create a new setup, use step 7. If you want to work with a setup that already exists, use step 8.

If you're creating generic setup data, don't specify network names (computer name and local hostname) and make sure that each network interface (port) is set to be configured "Using DHCP" or "Using BootP".

- 7 Click Continue and enter the setup data as you move through the Assistant's panes, following the onscreen instructions.

- 8 In the Language pane, choose File > Open Configuration File or File > Open Directory Record to load the saved setup data you want to work with. If the saved setup data is encrypted, type the passphrase when prompted.

Optionally choose View > Jump to Review to review the setup data, then use Go Back as necessary to change it.

- 9 In the Network Interfaces pane, click Add to specify network interfaces.
- 10 After all the setup data has been specified, review the summary displayed by Server Assistant and optionally click Go Back to change data.

- 11 Click Save As, then select "Directory Record."

- 12 To encrypt the file, select "Save in Encrypted Format" then enter and verify a passphrase.

You must supply the passphrase before an encrypted directory record can be used by a target server.

- 13 Specify the directory where you want to save the setup, name the setup record, and click OK. When prompted, enter information required to authenticate yourself as a directory domain administrator. Settings are saved in the directory in AutoServerSetup.

Target servers search for record names in the following order:

<MAC-address-of-server> (include any leading zeros but omit colons). For example, 0030654dbcef.

<IP-address-of-server>. For example, 10.0.0.4.

<partial-DNS-name-of-server>. For example, myserver.

<built-in-hardware-serial-number-of-server> (first 8 characters only). For example, ABCD1234.

<fully-qualified-DNS-name-of-server>. For example, myserver.example.com.

<partial-IP-address-of-server>. For example, 10.0 (matches 10.0.0.4 and 10.0.1.2).

generic (a record that any server will recognize, used to set up servers that need the same setup values).

- 14 Make sure the proper infrastructure is in place so that servers you want to use the stored setup record can find it.

The directory server storing the setup record needs to be running. DHCP needs to be configured to identify the directory server to the target servers using Option 95. In addition, you may need to have DNS configured if your directory data includes DNS names.

See "Defining Server Setup Infrastructure Requirements" on page 96 for some additional infrastructure information. The Open Directory and network services administration guides provide instructions for setting up directories and DHCP.

- 15 If the setup data is encrypted, make the passphrase available to the target server or servers. You can supply the passphrase interactively, using Server Assistant, or you provide it in a text file.

To provide the passphrase in a file, use step 16. To provide it interactively, use step 17.

- 16 To provide a passphrase in a file, create a new text file and type the passphrase for the saved setup file on the first line. Save the file using one of the following names; target servers search for names in the order listed:

<MAC-address-of-server>.pass (include any leading zeros but omit colons). For example, 0030654dbcef.pass.

<IP-address-of-server>.pass. For example, 10.0.0.4.pass.

<partial-DNS-name-of-server>.pass. For example, myserver.pass.

<built-in-hardware-serial-number-of-server>.pass (first 8 characters only). For example, ABCD1234.pass.

<fully-qualified-DNS-name-of-server>.pass. For example, myserver.example.com.pass.

<partial-IP-address-of-server>.pass. For example, 10.0.pass (matches 10.0.0.4 and 10.0.1.2).

generic.pass (a file that any server will recognize).

Put the passphrase file on a volume mounted locally on the target server in `/Volumes/* /Auto Server Setup/<pass-phrase-file>`, where `*` is any device that is mounted under the directory `/Volumes`.

- 17 To provide a passphrase interactively, use Server Assistant on an administrator computer that can connect with the target server.

In the Welcome or Destination pane, choose `File > Supply Passphrase`. In the dialog box, enter the target server's IP address, password, and the passphrase.

Click `Send`.

- 18 If you're using a generic setup record and the server serial number isn't site licensed, you must specify the server's serial number by using Server Admin or the command line after setup. In Server Admin, select the server, click `Settings`, and click `General`. To use the command line, in the Terminal application use `ssh` to connect with the server and type the `serversetup -setServerSerialNumber` command.

See the Open Directory administration guide for a description of the schema of setup data saved in a directory. See the command-line administration guide for information about `serversetup`.

Determining the Status of Setups

If setup isn't successful, there are several methods by which you're notified.

Using the Destination Pane for Setup Status Information

Server Assistant displays error information in its Destination pane. To access this pane, on the Welcome pane select "Set up a remote server" and click Continue.

If the server of interest isn't listed, click Add to list it. Select the server and review the information displayed.

You can save a list of servers you're interested in monitoring in the Destination pane using File > Save Server List. When you want to monitor the status of those servers, choose File > Load Server List.

Handling Setup Failures

When a server's setup fails, an error log is created as /System/Library/ServerSetup/Configured/POR.err on the target server. The contents of this log can be displayed and the log file deleted on a remote administrator computer. Double-click the error icon for a server on Server Assistant's Destination pane. If prompted, supply the preset password and click Send. The log contents are displayed, and you can click Delete to delete the log file. Setup can't be reinitiated until this file has been deleted.

If setup fails because a passphrase file can't be found when using setup data saved in a file or directory record, you can:

- Use Server Assistant to supply a passphrase interactively. On the Destination pane, choose File > Supply Passphrase.
- Supply the passphrase in a text file. Place the passphrase file on a volume mounted locally on the target server in /Volumes/*/Auto Server Setup/<pass-phrase-file>, where * is any device mounted under /Volumes/. A target server searches through volumes alphabetically by device name.

If a remote server setup fails for any other reason, you should re-install the server software and repeat initial setup.

If a local server setup fails, you can restart the computer, re-run Server Assistant, and re-initiate setup, or you can re-install the server software.

Handling Setup Warnings

When setup completes but a condition that warrants your attention exists, a warning log is created as `/Library/Logs/ServerAssistant.POR.status` on the target server. Click the target server's desktop link named `ServerAssistant.status` to open this file.

Here are some messages you may encounter in the log:

- The server software serial number is invalid. Open Server Admin, select the server in the Computers & Services list, click Settings, and click General. Enter the correct serial number, and click Save.
- Because this server was set up using a generic file or directory record and the serial number isn't site licensed, you must enter the server software serial number using Server Admin. Open Server Admin, select the server in the Computers & Services list, click Settings, and click General. Enter the correct serial number, and click Save.
- The server administrator user defined in the setup data already exists on the server you've upgraded.

Getting Upgrade Installation Status Information

When you perform an upgrade installation, log files may be placed on the target server. See the information on upgrading in the upgrading and migrating guide for information about upgrade logs.

Setting Up Services

The following sections survey initial setup of individual services and tell you where to find complete instructions for tailoring services to support your needs.

Setting Up Open Directory

Unless your server needs to be integrated with another vendor's directory system or the directory architecture of a server you're upgrading needs changing immediately, you can start using the directories you configured during server setup right away.

The Open Directory administration guide provides instructions for all aspects of Open Directory domain and authentication setup, including:

- Setting up client computer access to shared directory data
- Replicating LDAP directories and authentication information of Open Directory masters
- Integrating with Active Directory and other non-Apple directories
- Configuring single sign-on
- Using Kerberos and other authentication techniques

Setting Up User Management

Unless you're using a server exclusively to host Internet content (such as webpages) or perform computational clustering, you probably want to set up user accounts in addition to the administrator account(s) created during server setup.

To set up a user account:

- 1 Open Workgroup Manager.
- 2 Click the small globe near the top of the application window to select the directory you want to add users to.
- 3 Click the New User button.
- 4 Specify user settings in the panes that appear.

You can set up user accounts by using Workgroup Manager to import settings from a file.

The user management guide tells you how to define user settings, set up group accounts and computer lists, define managed preferences, and import accounts.

Setting Up File Services

When you turn on file sharing services, users can share items in selected folders.

If you turned on Apple file service during server setup, users who have existing accounts can already share items by putting them in the Public folders in their home directories or by copying the items into the Drop Box folder inside another user's Public folder.

If you didn't turn on Apple file service or other available file services already, you can turn them on now.

To set up file sharing:

- 1 Open Server Admin.
- 2 In the list beneath the server of interest, click each file service you want to turn on, then click the Start Service button in the toolbar.

To share with Macintosh computers, turn on Apple file service (AFP service).

To share with Windows computers, turn on Windows service.

To provide File Transfer Protocol (FTP) access, turn on FTP service.

To share with UNIX computers, turn on NFS service.

- 3 Open Workgroup Manager and click Sharing to set up a share point.
- 4 Select a volume or folder you want to share from the All list.
- 5 Click General, then select "Share this item and its contents."
- 6 Click the other tabs to specify attributes for the share point.

The file services administration guide provides instructions for managing share points and for configuring file sharing using all the protocols.

Setting Up Print Service

When you turn on print service, server users can share network PostScript printers or Postscript and non-Postscript printers connected directly to the server.

A queue is set up automatically for any USB printer connected to the server. No printer queues are set up automatically for network printers, but they're easy to add.

To set up a shared printer queue:

- 1 Open Server Admin.
- 2 In the list beneath the server of interest, click the button for print service.
- 3 Click the Settings button at the bottom of the application window, then click Queues.
- 4 Click the Add (+) button.
- 5 Choose a connection protocol, identify a printer, then click OK.
- 6 If it isn't running, click the Start Service button in the toolbar.

Users of Mac OS X computers can now add the printer using Printer Setup Utility.

For more information about setting up print services, see the print service administration guide.

Setting Up Web Service

You can use the Apache HTTP Server that comes with Mac OS X Server to host server and individual user websites.

If you turned on web service in Server Assistant, your server is ready to serve HTML pages from the general server and individual user sites folders.

- To view the main server site, open a web browser on any computer with access to the server and type the server's IP address or domain name.
- To view a user site, add a slash (/), a tilde (~), and the user's short name after the server address. For example, type

```
http://192.268.2.1/~someuser
```

To turn on web service if it's not running:

- 1 If you already have the HTML files for your main site, copy them into the Documents folder in the /Library/WebServer/ directory. If the files that make up your site are organized in folders, copy the entire folder structure to the Documents folder.

For a user site, the files go into the Sites folder in the user's home directory.

Make sure the files and folders you want web service to present are readable by user www. If you plan to enable WebDAV, make sure the appropriate files and folders are writable by user www.

If you don't have your own HTML files yet, you can still turn on web service to see how it works using the default start pages provided with Mac OS X Server.

- 2 Open Server Admin.
- 3 In the list beneath the server of interest, click the button for web service.
- 4 If it isn't running, click the Start Service button in the toolbar.

The web technologies administration guide describes the many features of web service, including how to set up SSL for a site, enable WebMail, and use WebDAV for file sharing.

Setting Up Mail Service

If you didn't turn on email service in Server Assistant, you can start it by using Server Admin, in the same fashion described above for other services.

Providing full mail service for your users requires additional configuration. The mail service administration guide provides detailed instructions for setting up and managing a mail server.

Setting Up Network Services

If you want a server to host any of the following network services, refer to the network services administration guide for setup instructions:

- DHCP service
- DNS
- Firewall service
- NAT (Network Address Translation)
- VPN
- Network time service

Setting Up System Image and Software Update Services

For details on using NetBoot and Network Install to simplify the management and installation of client operating systems and other software, see the system imaging and software update administration guide. It tells you how to create disk images and set up Mac OS X Server so other Macintosh computers can start up from, or install, those images over the network.

The same guide describes how to set up software update service, which lets you customize updates of Apple software on client computers.

Setting Up Media Streaming and Broadcasting

For information about how to manage a streaming server that delivers media streams live or on demand to client computers, see the QuickTime Streaming Server administration guide.

Setting Up an Application Server

If you want to set up a Java application server, see the JBoss administration guide. It tells you how to develop and deploy servlets, enterprise beans, and enterprise applications and how to configure and administer a Java application server.

Use Server Admin to administer JBoss and Tomcat.

To turn on JBoss if it's not running:

- 1 Open Server Admin.
- 2 In the list beneath the server of interest, click Application Server.
- 3 Click Start Service.

Setting Up a WebObjects Server

If you want to develop WebObjects applications, see the WebObjects Reference Library, available at developer.apple.com/referencelibrary/WebObjects/. If you want to set up a WebObjects application server, see the Deployment section of the WebObjects Reference Library.

To turn on WebObjects if it's not running:

- 1 Open Server Admin.
- 2 In the list beneath the server of interest, click WebObjects.
- 3 Click Start Service.

Setting Up Collaboration Service

In addition to services already discussed that help users stay in touch (for example, mail and file services and group accounts and preferences), you can set up an iChat server and a Weblog server.

How you use Server Admin to set up iChat and Weblog services is described in the collaboration services administration guide.

Settings for the following server appear in the tables below:

Server:

Item	Description	Your information
Identity of remote server for installation and setup	<p>For interactive installation and setup of a remote server on the local subnet, one of these values for the server:</p> <ul style="list-style-type: none">- IP address in IPv4 format (000.000.000.000)- host name (someserver.example.com)- MAC address (00:03:93:71:26:52). <p>For command-line or remote-subnet installations and setups, the target server's IP address, in IPv4 format.</p>	
Preset password (for remote installation and setup)	<p>The first 8 digits of the target server's built-in hardware serial number, printed on a label on the computer.</p> <p>For older computers with no such number, use 12345678 for the password.</p>	
Type of installation	<p>Upgrade from the latest 10.3 version or from version 10.2.8, complete installation without disk formatting, or clean installation.</p> <p>The target volume (partition) is erased when you do a clean installation.</p>	
Target disk or partition	<p>Name of the target disk or partition (volume).</p>	
Disk format (when erasing the disk is OK)	<p>A format for the target disk.</p> <p>In most cases, use Mac OS Extended (Journaled). You can also use Mac OS Extended or case-sensitive HFS+.</p>	
Disk partitioning (when erasing the disk is OK)	<p>Indicate whether you want to partition the target disk.</p> <p>The minimum recommended size of a target disk partition is 4 GB.</p>	

Item	Description	Your information
RAID mirroring (when erasing the disk is OK and you have a second physical drive on the target server)	<p>Indicate whether you want to set up RAID mirroring. The second disk is used automatically if the primary disk isn't available.</p> <p>If the target disk has a single partition and the second physical drive has a single partition and no data, you can set up RAID mirroring after installation. However, to prevent data loss, set up RAID mirroring as soon as possible.</p>	
Using saved setup data	<p>If you want to use saved setup data to set up this server, identify the file or directory storing the data you want to use. If the data is encrypted, also identify the passphrase.</p> <p>If you want to save settings in a file or directory, use one of the next two rows.</p>	
Saving setup data in a file	<p>Name the file using one of these options:</p> <ul style="list-style-type: none"> - <MAC-address-of-server>.plist (include any leading zeros but omit colons). For example, 0030654dbcef.plist. - <IP-address-of-server>.plist. For example, 10.0.0.4.plist. - <partial-DNS-name-of-server>.plist. For example, myserver.plist. - <built-in-hardware-serial-number-of-server>.plist (first 8 characters only). For example, ABCD1234.plist. - <fully-qualified-DNS-name-of-server>.plist. For example, myserver.example.com.plist. - <partial-IP-address-of-server>.plist. For example, 10.0.plist (matches 10.0.0.4 and 10.0.1.2). - generic.plist (a file that any server will recognize, used to set up servers that need the same setup values). <p>If you choose to encrypt the file, you can save the passphrase in a file named using the above conventions, except use the extension .pass, not .plist.</p> <p>Place the file(s) in a location where the target server or servers can detect it. A server can detect files that reside on a volume mounted locally in /Volumes/*/Auto Server Setup/, where * is any device mounted under /Volumes.</p>	

Item	Description	Your information
Saving setup data in a directory	<p>Navigate to the directory where you want to save the setup, and name the setup record using one of these options:</p> <ul style="list-style-type: none"> - <MAC-address-of-server> (include any leading zeros but omit colons). For example, 0030654dbcef. - <IP-address-of-server>. For example, 10.0.0.4. - <partial-DNS-name-of-server>. For example, myserver. - <built-in-hardware-serial-number-of-server> (first 8 characters only). For example, ABCD1234. - <fully-qualified-DNS-name-of-server>. For example, myserver.example.com. - <partial-IP-address-of-server>. For example, 10.0 (matches 10.0.0.4 and 10.0.1.2). - generic (a file that any server will recognize, used to set up servers that need the same setup values). <p>If you choose to encrypt the file, you can save the passphrase in a file named using the above conventions, except add the extension .pass. Place the passphrase file in a location where the target server or servers can detect it. A server can detect the file if it resides on a volume mounted locally in /Volumes/*/Auto Server Setup/, where * is any device mounted under /Volumes.</p>	
Language	<p>The language to use for server administration (English, Japanese, French, or German). The language affects the server's time and date formats, displayed text, and the default encoding used by the AFP server.</p>	
Keyboard layout	<p>The keyboard for server administration.</p>	

Item	Description	Your information
Serial number	<p>The serial number for your copy of Mac OS X Server. The format of the server serial number is xsvr-999-999-x-xxx-xxx-xxx-xxx-xxx-xxx-x, where x is a letter and 9 is a digit. The first element (xsvr) and the fourth one (x) must be lower case.</p> <p>Unless you have a site license, you need a unique serial number for each server. You'll find the server software serial number printed on the materials provided with the server software package.</p> <p>If you have a site license, a registered owner name and organization must be entered exactly as specified by your Apple representative.</p> <p>If you set up a server using a generic setup file or directory record and the serial number isn't site licensed, you must enter the server's serial number using Server Admin.</p>	
Administrator's long name (sometimes called full name or real name)	<p>A long name can contain no more than 255 bytes. The number of characters ranges from 255 Roman characters to as few as 85 3-byte characters. It can include spaces. It can't be the same as any predefined user name, such as System Administrator. This name is case sensitive in the login window, but not when accessing file servers.</p>	
Administrator's short name	<p>A short name can contain as many as 255 Roman characters, typically eight or fewer. Use only a through z, A through Z, 0 through 9, _ (underscore), or - (hyphen). Avoid short names that Apple assigns to predefined users, such as "root."</p>	
Administrator's password	<p>This value is case sensitive and must contain at least 4 characters. It is also the password for the root user.</p> <p>If you record this value, be sure to keep this worksheet in a safe place.</p> <p>After setup, use Workgroup Manager to change the password for this account.</p>	

Item	Description	Your information
Host name	<p>You can't specify this name during server setup. Server Assistant sets the host name to AUTOMATIC in /etc/hostconfig. This setting causes the server's host name to be the first name that's true in this list:</p> <ul style="list-style-type: none"> - The name provided by the DHCP or BootP server for the primary IP address - The first name returned by a reverse DNS (address-to-name) query for the primary IP address - The local hostname - The name "localhost" 	
Computer name	<p>The AppleTalk name and the default name used for SLP/DA. Specify a name 63 characters or fewer but avoid using =, :, or @.</p> <p>The Network browser in the Finder uses SMB/CIFS to find computers that provide Windows file sharing. Spaces are removed from a computer name for use with SMB/CIFS, and the name can contain no more than 15 characters, no special characters, and no punctuation.</p>	
Local hostname	<p>The name that designates a computer on a local subnet. It can contain lower-case letters, numbers, and/or hyphens (but not at the ends). The name ends with ".local" and must be unique on a local subnet.</p>	
Network interface data	<p>Your server has a built-in Ethernet port and may have an additional Ethernet port built in or added on. Record information for each port you want to activate.</p>	<p>Use the table provided later in this worksheet to record data for each port.</p>
Directory usage	<p>Select one:</p> <ul style="list-style-type: none"> - Standalone Server (use only the local directory). - Connected to a Directory System (get information from another server's shared directory). If you choose this option, use one of the next four rows in this table to indicate how the server will connect with the directory. - Open Directory Master (provide directory information to other computers). If you choose this option, use the row for "Using Open Directory Master." - No change (for upgrades only). 	
Using "As Specified by DHCP Server"	<p>The directory to use will be identified by a DHCP server set up to provide the address and search base of an LDAP server (DHCP option 95) or the address and tag of a legacy NetInfo server.</p>	

Item	Description	Your information
Using “Open Directory Server”	The directory to use will be an LDAP directory identified by a DHCP server or identified by specifying an IP address or domain name for the LDAP server.	
Using “NetInfo Server”	The directory to use will be a NetInfo parent directory on an existing Apple server. Choose one or more ways to locate that directory: <ul style="list-style-type: none"> - Broadcast - DHCP - Static IP Address (specify IP address and NetInfo tag) 	
Using “Other Directory Server”	The directory or directories to use will be configured using the Directory Access application after you’re finished setting up the server.	
Using “Open Directory Master”	Optionally indicate you want to enable a Windows Primary Domain Controller on the server. Provide a Windows computer name and domain for the server. The computer name and domain can contain a-z, A-Z, 0-9, -, but no . or space and can’t contain only numbers. Finish setting up the directory you want to host by using Server Admin after completing server setup.	
Automating service startup	Indicate whether you want any of the following to start automatically every time the server starts; these items need no additional configuration to be useful: <ul style="list-style-type: none"> Apple file service Apple Remote Desktop FTP service iChat service Mail service NetBoot service Network time service QuickTime Streaming service Software update service Web service WebDAV service Weblog service Windows file service Xgrid Agent service Xgrid Controller service 	
Time zone	Choose the time zone you want the server to use.	
Network time	Optionally indicate a Network Time Server for the server. Apple recommends that you keep your server’s clock accurate by synchronizing it with a network time server.	

Configuration settings for the following port appear in the table below:

Port Name: Built-in Ethernet

Item	Description	Your information
Device name	A UNIX name for the port in the format <code>enx</code> , where <code>x</code> starts with 0. See your hardware manual for the value of <code>x</code> for the port you're describing. The value <code>en0</code> always designates a built-in Ethernet port.	<code>en0</code>
Ethernet address	The Media Access Control (MAC) address of the port (00:00:00:00:00:00). This value is usually on a sticker on the server hardware, but you can run Apple System Profiler or a command-line tool such as <code>networksetup</code> to discover the value.	
TCP/IP and AppleTalk	Indicate whether you want to enable the port for TCP/IP and/or AppleTalk. You can connect a port to the Internet by enabling TCP/IP and use the same or a different port for AppleTalk. Enable no more than one port for AppleTalk.	
Order of ports	If you enable more than one port, indicate the order in which the ports should be accessed when trying to connect to a network. All non-local network traffic uses the first active port.	
TCP/IP settings	Use one of the next four rows in this table.	
"Manually"	Specify these settings if you want to manually specify TCP/IP settings: <ul style="list-style-type: none">- IP address (000.000.000.000). A unique static address.- Subnet mask (000.000.000.000). Used to locate the subnet on the local area network where the server resides. This mask is used to derive the network part of the server's address; what remains identifies the server computer on that network.- Router (000.000.000.000) that supports the subnet the server's on. The router is the machine on the local subnet to which messages are sent if the target IP address isn't on the local subnet.- DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port.- Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify <code>campus.univ.edu</code> as a search domain, you can type <code>server1</code> in the Finder's Connect To Server dialog box to connect to <code>server1.campus.univ.edu</code>.	

Item	Description	Your information
<p>“Using DHCP with Manual IP address”</p>	<p>Specify these settings if you want to use a DHCP server to assign a static IP address and optionally other settings for the port. Make sure the DHCP server is already set up and DHCP service running when you initiate server setup:</p> <ul style="list-style-type: none"> - IP address (000.000.000.000). A unique static address. - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu. 	
<p>“Using DHCP”</p>	<p>Specify these settings if you want to use a DHCP server to assign a dynamic IP address and optionally other settings for the port. Make sure the DHCP server is already set up and DHCP service running when you initiate server setup:</p> <ul style="list-style-type: none"> - DHCP client ID (optional). A string that's useful for recognizing a port when its IP address changes. Don't specify a DHCP client ID when using Server Assistant to set up the server remotely. Instead, after setup, use the server's Network preferences to define a DHCP client ID. - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu. 	
<p>“Using BootP”</p>	<p>Specify these settings if you want to use a Bootstrap Protocol server to assign an IP address for the identified port. With BootP, the same IP address is always assigned to a particular network interface. It's used primarily for computers that start up from a NetBoot image:</p> <ul style="list-style-type: none"> - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified domain names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu. 	

Item	Description	Your information
IPv6	<p>To configure IPv6 addressing for the port, select Automatically or Manually.</p> <p>Choose Automatically if you want the server to automatically generate an IPv6 address for the port.</p> <p>Choose Manually to specify IPv6 settings:</p> <ul style="list-style-type: none"> - IPv6 address. Generally written in the form 0000:0000:0000:0000:0000:0000:0000. - Router. The IPv6 address of the router on the local subnet. - Prefix length. The number of significant bits in the subnet mask that are used to identify the network. 	
Ethernet settings	<p>To automatically configure Ethernet settings for the port, choose Automatically.</p> <p>You may want to choose Manually (Advanced) to specify settings if you have specific requirements for the network the server's connected to. Note that incorrect Ethernet settings can affect network performance or render a port unusable:</p> <ul style="list-style-type: none"> - Speed. The maximum Ethernet speed, in number of bits per second, that can be transmitted using the port. Select one of these options: autoselect, 10baseT/UTP, 100baseTX, and 1000baseTX. - Duplex. Determine whether input and output packets are transmitted at the same time (full-duplex) or alternately (half-duplex). - Maximum Packet Size (MTU). The largest packet the port will send or receive. MTU stands for maximum transfer unit, expressed in bytes. Increasing the packet size improves throughput, but the devices that receive the packet (switches, routers, and so forth) must support the packet size. Select one of these options: Standard (1500), Jumbo (9000), or Custom (enter a value from 72 to 1500). 	

Configuration settings for the following port appear in the table below:

Port Name:

Item	Description	Your information
Device name	A UNIX name for the port in the format <code>enx</code> , where <code>x</code> starts with 0. See your hardware manual for the value of <code>x</code> for the port you're describing. The value <code>en0</code> always designates a built-in Ethernet port.	
Ethernet address	The Media Access Control (MAC) address of the port (00:00:00:00:00:00). This value is usually on a sticker on the server hardware, but you can run Apple System Profiler or a command-line tool such as <code>networksetup</code> to discover the value.	
TCP/IP and AppleTalk	Indicate whether you want to enable the port for TCP/IP and/or AppleTalk. You can connect a port to the Internet by enabling TCP/IP and use the same or a different port for AppleTalk. Enable no more than one port for AppleTalk.	
Order of ports	If you enable more than one port, indicate the order in which the ports should be accessed when trying to connect to a network. All non-local network traffic uses the first active port.	
TCP/IP settings	Use one of the next four rows in this table.	
"Manually"	Specify these settings if you want to manually specify TCP/IP settings: <ul style="list-style-type: none">- IP address (000.000.000.000). A unique static address.- Subnet mask (000.000.000.000). Used to locate the subnet on the local area network where the server resides. This mask is used to derive the network part of the server's address; what remains identifies the server computer on that network.- Router (000.000.000.000) that supports the subnet the server's on. The router is the machine on the local subnet to which messages are sent if the target IP address isn't on the local subnet.- DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port.- Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify <code>campus.univ.edu</code> as a search domain, you can type <code>server1</code> in the Finder's Connect To Server dialog box to connect to <code>server1.campus.univ.edu</code>.	

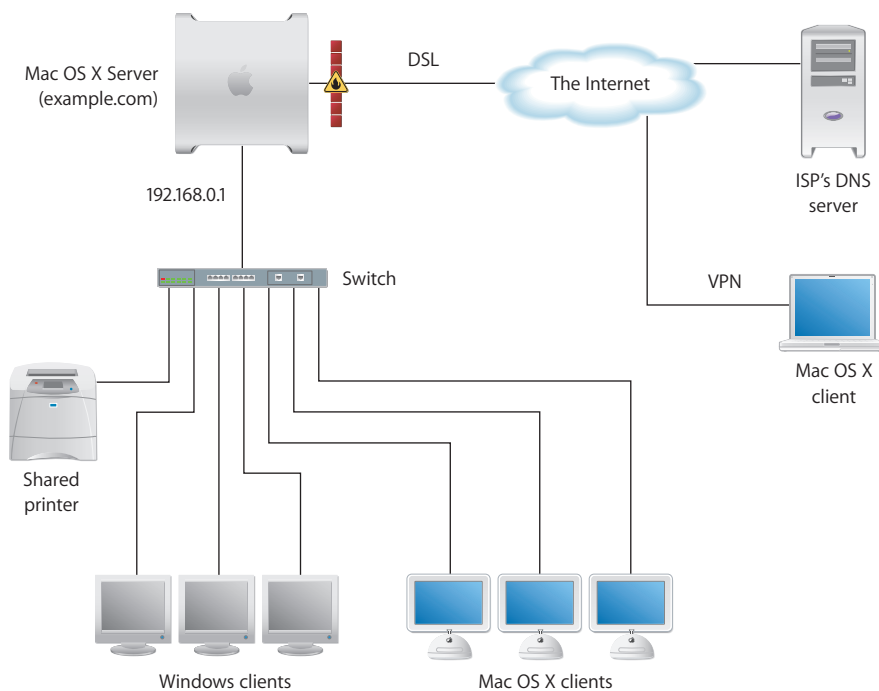
Item	Description	Your information
<p>“Using DHCP with Manual IP address”</p>	<p>Specify these settings if you want to use a DHCP server to assign a static IP address and optionally other settings for the port. Make sure the DHCP server is already set up and DHCP service running when you initiate server setup:</p> <ul style="list-style-type: none"> - IP address (000.000.000.000). A unique static address. - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu. 	
<p>“Using DHCP”</p>	<p>Specify these settings if you want to use a DHCP server to assign a dynamic IP address and optionally other settings for the port. Make sure the DHCP server is already set up and DHCP service running when you initiate server setup:</p> <ul style="list-style-type: none"> - DHCP client ID (optional). A string that's useful for recognizing a port when its IP address changes. Don't specify a DHCP client ID when using Server Assistant to set up the server remotely. Instead, after setup, use the server's Network preferences to define a DHCP client ID. - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu. 	
<p>“Using BOOTP”</p>	<p>Specify these settings if you want to use a Bootstrap Protocol server to assign an IP address for the identified port. With BootP, the same IP address is always assigned to a particular network interface. It's used primarily for computers that start up from a NetBoot image:</p> <ul style="list-style-type: none"> - DNS servers (000.000.000.000) used to convert IP addresses to fully qualified DNS names and vice versa for the port. - Search domains (optional). Names to automatically append to Internet addresses when you don't fully qualify them. For example, if you specify campus.univ.edu as a search domain, you can type server1 in the Finder's Connect To Server dialog box to connect to server1.campus.univ.edu. 	

Item	Description	Your information
IPv6	<p>To configure IPv6 addressing for the port, select Automatically or Manually.</p> <p>Choose Automatically if you want the server to automatically generate an IPv6 address for the port.</p> <p>Choose Manually to specify IPv6 settings:</p> <ul style="list-style-type: none"> - IPv6 address. Generally written in the form 0000:0000:0000:0000:0000:0000:0000. - Router. The IPv6 address of the router on the local subnet. - Prefix length. The number of significant bits in the subnet mask that are used to identify the network. 	
Ethernet settings	<p>To automatically configure Ethernet settings for the port, choose Automatically.</p> <p>You may want to choose Manually (Advanced) to specify settings if you have specific requirements for the network the server's connected to. Note that incorrect Ethernet settings can affect network performance or render a port unusable:</p> <ul style="list-style-type: none"> - Speed. The maximum Ethernet speed, in number of bits per second, that can be transmitted using the port. Select one of these options: autoselect, 10baseT/UTP, 100baseTX, and 1000baseTX. - Duplex. Determine whether input and output packets are transmitted at the same time (full-duplex) or alternately (half-duplex). - Maximum Packet Size (MTU). The largest packet the port will send or receive. MTU stands for maximum transfer unit, expressed in bytes. Increasing the packet size improves throughput, but the devices that receive the packet (switches, routers, and so forth) must support the packet size. Select one of these options: Standard (1500), Jumbo (9000), or Custom (enter a value from 72 to 1500). 	

The setup example in this appendix illustrates one way to set up the directory and network infrastructure of Mac OS X Server in a small business scenario.

Mac OS X Server in a Small Business

In this example, Mac OS X Server provides directory, network, and productivity services to employees in a small business.



The small business in this example had been using an office LAN to share files and a printer. Acquiring Mac OS X Server made it possible to implement an intranet that uses an ISP's DNS and digital subscriber line (DSL) services.

Here's a summary of the scenario's characteristics:

- An Open Directory master LDAP directory on the server centralizes user management, including authentication of Mac OS X and Windows users.
- The ISP's DNS service provides a DNS domain name for the company (example.com).
- A DNS server running on Mac OS X Server provides name services for the server, the printer, and any other intranet device that has a static IP address.
- A firewall between the server and the Internet protects the intranet from unauthorized access.
- NAT service lets intranet users share the ISP's IP address for Internet access, while VPN lets employees access the intranet securely over the Internet when they're working away from the office.
- DHCP service on Mac OS X Server provides dynamic IP addresses to intranet client computers. The server and printer have static addresses, but client computers have dynamic addresses.

How to Set Up the Server

The following steps summarize how to set up Mac OS X Server in this hypothetical small business. For complete information about setting up directory services, see the Open Directory administration guide. For details about network service setup (IP firewall, DHCP, and so forth), see the network services administration guide.

Step 1: Set up the network

- 1 Make sure the server has two Ethernet interfaces (ports), one for the intranet (LAN) connection and one for the DSL modem connection. Use the faster interface for the server connection. A 10-Mbit connection is more than sufficient for the DSL connection.
- 2 Connect the server to the LAN using the faster interface. In this example, the server is plugged in to a switch used to connect the existing client computers and shared printer. We'll refer to this interface as the "internal" interface.

Intranet devices should be connected to a hub or switch using good-quality CAT-5 Ethernet cables. A high-speed 10/100/1000 megabit switch would be able to support advanced server features such as NetBoot that work best over a fast connection.
- 3 Connect the server to the DSL modem using the other Ethernet interface. We'll refer to this interface as the "external" interface.

Step 2: Set up the server and the master directory

- 1 Start the server from the first install CD or from the install DVD. The procedure you use depends on the server hardware.

In this example, assume the computer has a display, keyboard, and optical drive attached. Turn on the computer, insert the first install disc into the optical drive, and restart the computer while holding down the C key on the keyboard.

“Using Server Assistant to Install Remotely From the Install Discs” on page 104 tells you how to start up other kinds of computers to install server software.

- 2 When the Installer opens, proceed through its panes by following the onscreen instructions. If you need to format the target disk, see “Preparing Disks for Installing Mac OS X Server” on page 101 for instructions.

Insert additional install discs when prompted if you’re using install CDs.

When installation is complete, the server restarts and Server Assistant opens.

- 3 Fill out the worksheet on page 137. You’ll need the information as you move through the Assistant’s panes.
- 4 Use the Language and Keyboard panes to reflect the server’s administration language.
- 5 In the Administrator Account pane, enter the server administrator’s names and password. Click Continue.
- 6 In the Network Names pane, enter the computer name and local hostname for your server. Click Continue.
- 7 Make sure the Network Interfaces pane lists your external and internal Ethernet interfaces.

Also make sure that the external interface is the first one listed in the Network Interfaces pane. The first interface listed is the primary, or default, interface. Network traffic initiated by the server is routed through the primary interface. VPN uses it as the Public network, treating all others listed as Private.

Click Continue.

- 8 The TCP/IP Connection pane appears for each Ethernet interface.

For the external interface, choose Manually from the Configure IPv4 pop-up list, then enter the IP address, subnet mask, and DNS server IP address, or addresses, provided to you by the ISP. In addition, make sure you add the local DNS server IP address (192.168.0.1) to those supplied by the ISP. For best performance, make the local DNS server IP address appear first in the list. Click Continue.

If you’ll be using Gateway Setup Assistant to configure network settings, you don’t need to set up an internal interface. Otherwise, enter these values for the internal interface then click Continue:

Configure IPv4: Manually

IP Address: 192.168.0.1 (192.168 values are reserved for internal LANs)

Subnet Mask: 255.255.0.0

Router: 192.168.0.1

DNS Servers: 192.168.0.1

- 9 In the Directory Usage Pane, choose Open Directory Master to set up a shared LDAP directory on the server.

Select Enable Windows Primary Domain Controller and enter a Domain/Workgroup name. These settings will set up a Windows PDC so that employees who use Windows NT, Windows 2000, and Windows XP workstations can log in to the PDC, change passwords during login, and have roaming user profiles and network home directories on the server. With one user account, a user can log in from a Windows workstation or a Mac OS X computer and access the same network home directory.

Click Continue.

- 10 Proceed through the remaining Assistant panes, then click Apply to initiate server setup.

When setup is complete, the server restarts automatically.

- 11 Log in to the server as the administrator you defined when using Server Assistant.
- 12 Configure the server's network settings.

The simplest way to do this is to use the Gateway Setup Assistant, as Step 3 describes. Alternatively, you can individually configure each network service using Server Admin, as Steps 4 through 8 describe.

Step 3: Use Gateway Setup Assistant to automate the server's network configuration

- 1 Open Server Admin by clicking its icon in the Dock.
- 2 Open Gateway Setup Assistant by choosing View > Gateway Setup Assistant.
- 3 Proceed through the panes, specifying information when prompted.
On the WAN Port pane, select the port you configured during initial setup as the external interface.
On the VPN settings pane, enable VPN and specify a shared secret for client connections to use.
On the LAN Ports pane, select the port you want to use as the internal interface.
- 4 When Gateway Setup Assistant has completed network setup and you've quit the application, go to Step 9.

Step 4: Set up the firewall

- 1 Open Server Admin by clicking its icon in the Dock.
- 2 Authenticate as the server administrator.
- 3 In the Computers & Services list, click Firewall.
- 4 Click Start Service in the toolbar.
- 5 Click Settings, and in the Address Groups pane select the IP address group named 192.168-net. The group includes 65,535 IP addresses.

- 6 Click Services and select "Allow" for services you want employees working at the office to be able to access. At a minimum select Domain Name Service, DHCP, and NetBoot.
- 7 Click Address Groups, then select the IP address group named "any."
- 8 Click Services and select "Allow" for services you want external clients to be able to access behind the firewall.
- 9 Click Save.

Step 5: Set up DNS service

- 1 In Server Admin, select DNS in the Computers & Services list.
- 2 Click Settings.
- 3 Make sure that "Zone transfers" isn't enabled and that "Recursion" is enabled.
- 4 Click Zones, then click the Add button (+) under the Zones list to set up a zone for the intranet.

Enter the following values using the General pane, then click OK:

Zone Name: example.com

Server Name: myserver

Server IP Address: 192.168.0.1

Administrator email: admin@example.com

Using the Machines pane, add machines to the zone. For example, to add a printer, click the Add button and specify values for the printer, then click OK:

IP address: 192.168.100.2

Name: hp_laserjet_2000

- 5 Click Save, then click Start Service.

Step 6: Set up DHCP service

This step sets up a DHCP server that provides employee computers dynamic IP addresses as well as the identity of the DNS, LDAP, and WINS servers they should use. When a client computer's search policy is set to Automatic (using the Directory Access application on the client computer), the identity of the DNS, LDAP, and WINS servers is supplied automatically at the same time an IP address is supplied.

- 1 In Server Admin, make sure that DNS is running.
- 2 Select DHCP in the Computers & Services list.
- 3 Click Settings.

- 4 Click the Add button to define the range of addresses to dynamically assign. The range should be large enough to accommodate current and future client computers. But make sure you exclude some addresses (at the start or end of the range) so they're reserved for devices that need static IP addresses or for VPN users.

Here are some sample values:

Starting IP Address: 192.168.0.2

Ending IP Address: 192.168.0.102

Subnet Mask: 255.255.0.0

Network Interface: En1

Router: 192.168.0.1

- 5 Make sure the DNS pane contains the following values:

Default Domain: example.com

Name Servers: 192.168.0.1

- 6 Click LDAP to configure DHCP to identify the server you're configuring as the source of directory information for clients who are served dynamic IP addresses.

The server you're setting up should be identified in the Server Name field, because you set up the server as an Open Directory master when you used Server Assistant. Other settings are optional for this example.

- 7 Click WINS to configure DHCP to serve Windows-specific settings to clients who are served dynamic IP addresses.

Supply these values:

WINS/NBNS Primary Server: 192.168.0.1

NBT Node Type: Broadcast (b-node)

- 8 Click Save, click the back arrow, enable the internal Ethernet interface, then click Start Service.

Step 7: Set up NAT service

- 1 In Server Admin, select NAT in the Computers & Services list.
- 2 Click Settings.
- 3 Select the external interface from the "External network interface" pop-up menu.
- 4 Click Save, then click Start Service.

Step 8: Set up VPN service

- 1 In Server Admin, select VPN in the Computers & Services list.
- 2 Click Settings.
- 3 Enable L2TP over IPSec (Layer Two Tunneling Protocol, Secure Internet Protocol) for Mac OS X version 10.4 computer users, Linux or UNIX workstation users, and Windows XP users. While PPTP, described in the next step, can also be used, L2TP provides the greatest security because it runs over IPSec.

Enter a starting and ending IP address to indicate which addresses the VPN server can assign to clients. Avoid addresses the DHCP server is set up to serve. Also avoid addresses you specify if you enable PPTP.

Specify the shared secret by typing a string in “Shared secret”. Enter a string that isn’t intuitive. For example, specify digits, symbols, and uppercase and lowercase characters in unusual combinations. The recommended string length is 8 to 12 characters.

- 4 Enable PPTP (Point to Point Tunneling Protocol) if employees will need to access the intranet from Windows workstations other than Windows XP computers or from Mac OS X version 10.2 computers when they’re away from the office. If you need to support older Windows clients that don’t have 128-bit PPTP support, select “Allow 40-bit encryption keys in addition to 128-bit”.

Enter a starting and ending IP address to indicate which addresses the VPN server can assign to clients. Avoid addresses the DHCP server is set up to serve. Also avoid addresses you specified when you enabled L2TP over IPSec.

- 5 Click Save, then click Start Service.

Step 9: Set up productivity services

The infrastructure you need to set up file, print, and other productivity services is now available. Follow the instructions in the relevant administration guides, listed on page 13, to configure the services of interest. Many services, such as Apple file service, require minimal setup. Simply start them using Server Admin.

Step 10: Create user accounts and home directories

- 1 Open Workgroup Manager. The Open Directory master LDAP directory is automatically available for editing. You’ll add an account for each employee to this master directory.
- 2 Click the New User button.
- 3 Specify user settings in the panes that appear.

The user management guide tells you how to set up all the user account attributes, including home directories. It also describes how to manage users by setting up group accounts and computer lists and how to set up preference settings that customize the work environments of Macintosh clients.

The Windows administration guide focuses on how to implement support specifically for Windows workstation users. Use this document to supplement the user management guide and the Open Directory administration guide if your server will support Windows users.

Step 11: Configure client computers

The information that follows applies to Mac OS X version 10.4 computers. For information about how to support Windows client computers, see the Windows administration guide.

- 1 If necessary, configure Mac OS X clients to retrieve information from the DHCP server.

Mac OS X version 10.4 computers are preconfigured to use DHCP to obtain IP addresses and retrieve information about an LDAP directory from the DHCP server. After you configure DHCP service with information about an LDAP directory, that information is delivered automatically to Mac OS X clients when they receive IP addresses from the DHCP server.

These are the settings that are preconfigured:

Network preferences are set to use DHCP. To access the setting, select System Preferences, open Network preferences, select the internal Ethernet interface, and select "Using DHCP with manual address" or "Using DHCP" from the Configure IPv4 pop-up menu.

The computer's search policy is set to be defined automatically. To access this setting, open Directory Access (in /Applications/Utilities/) and click Authentication. If the lock icon is locked, click it and authenticate as an administrator. Choose Automatic from the Search pop-up menu, then click Apply.

The use of DHCP-supplied LDAP information is enabled. To access this setting, open Directory Access and click Services. If the lock icon is locked, click it and authenticate as an administrator. Select LDAPv3 in the list of services, then click Configure. Click "Use DHCP-supplied LDAP Server," then click OK.

- 2 Configure Mac OS X clients so they can use the VPN server.

Open the Internet Connect application (in /Applications/) and click VPN in the toolbar. Select L2TP over IPSec or PPP and click Continue. Choose Edit Configurations from the Configurations pop-up menu. Enter the external IP address from the ISP, the user name and password for the computer user, and, for L2TP over IPSec, the shared secret. Click OK.

administrator A user with server or directory domain administration privileges. Administrators are always members of the predefined “admin” group.

administrator computer A Mac OS X computer onto which you’ve installed the server administration applications from the Mac OS X Server Admin CD.

AFP Apple Filing Protocol. A client/server protocol used by Apple file service on Macintosh-compatible computers to share files and network services. AFP uses TCP/IP and other protocols to communicate between computers on a network.

Apache An open-source HTTP server integrated into Mac OS X Server. You can find detailed information about Apache at www.apache.org.

application server Software that runs and manages other applications, usually web applications, that are accessed using a web browser. The managed applications reside on the same computer where the application server runs.

authentication The process of proving a user’s identity, typically by validating a user name and password. Usually authentication occurs before an authorization process determines the user’s level of access to a resource. For example, file service authorizes full access to folders and files that an authenticated user owns.

authorization The process by which a service determines whether it should grant a user access to a resource and how much access the service should allow the user to have. Usually authorization occurs after an authentication process proves the user’s identity. For example, file service authorizes full access to folders and files that an authenticated user owns.

BIND Berkeley Internet Name Domain. The program included with Mac OS X Server that implements DNS. The program is also called the name daemon, or named, when the program is running.

BootP An older method of allocating IP addresses to clients on a network. See also DHCP.

boot ROM Low-level instructions used by a computer in the first stages of starting up.

BSD Berkeley System Distribution. A version of UNIX on which Mac OS X software is based.

CGI Common Gateway Interface. A script or program that adds dynamic functions to a website. A CGI sends information back and forth between a website and an application that provides a service for the site.

computer list A list of computers that have the same preference settings and are available to the same users and groups.

computer name The default name used for SLP and SMB/CIFS service registrations. The Network Browser in the Finder uses SLP to find computers advertising Personal File Sharing and Windows File Sharing. It can be set to bridge subnets depending on the network router settings. When you turn on Personal File Sharing, users see the computer name in the Connect To Server dialog in the Finder. Initially it is “<first created user>’s Computer” (for example, “John’s Computer”) but can be changed to anything. The computer name is used for browsing for network file servers, print queues, Bluetooth discovery, Apple Remote Desktop clients, and any other network resource that identifies computers by computer name rather than network address. The computer name is also the basis for the default local hostname.

CUPS Common UNIX Printing System. A cross-platform printing facility based on the Internet Printing Protocol (IPP). The Mac OS X Print Center, its underlying print system, and the Mac OS X Server print service are all based on CUPS. For more information, visit www.cups.org.

DHCP Dynamic Host Configuration Protocol. A protocol used to dynamically distribute IP addresses to client computers. Each time a client computer starts up, the protocol looks for a DHCP server and then requests an IP address from the DHCP server it finds. The DHCP server checks for an available IP address and sends it to the client computer along with a lease period—the length of time the client computer may use the address.

directory domain A specialized database that stores authoritative information about users and network resources; the information is needed by system software and applications. The database is optimized to handle many requests for information and to find and retrieve information quickly. Also called a directory node or simply a directory.

directory node See **directory domain**.

directory services Services that provide system software and applications with uniform access to directory domains and other sources of information about users and resources.

disk image A file that, when opened, creates an icon on a Mac OS desktop that looks and acts like an actual disk or volume. Using NetBoot, client computers can start up over the network from a server-based disk image that contains system software. Disk image files have a filename extension of either .img or .dmg. The two image formats are similar and are represented with the same icon in the Finder. The .dmg format cannot be used on computers running Mac OS 9.

DNS Domain Name System. A distributed database that maps IP addresses to domain names. A DNS server, also known as a name server, keeps a list of names and the IP addresses associated with each name.

DNS domain A unique name of a computer used in the Domain Name System to translate IP addresses and names. See also **domain name**.

DNS name A unique name of a computer used in the Domain Name System to translate IP addresses and names. See also **domain name**.

domain Part of the domain name of a computer on the Internet. It does not include the Top Level Domain designator (for example, .com, .net, .us, .uk). Domain name "www.example.com" consists of the subdomain or host name "www," the domain "example," and the top level domain "com."

DSL Digital subscriber line. A broadband data transmission technology that operates over telephone lines.

everyone Any user who can log in to a file server: a registered user or guest, an anonymous FTP user, or a website visitor.

export In the Network File System (NFS), a way of sharing a directory with clients on a network. TBD for RAID context.

filter A "screening" method used to control access to a server. A filter is made up of an IP address and a subnet mask, and sometimes a port number and access type. The IP address and the subnet mask together determine the range of IP addresses to which the filter applies.

firewall Software that protects the network applications running on your server. IP firewall service, which is part of Mac OS X Server software, scans incoming IP packets and rejects or accepts these packets based on a set of filters you create.

FireWire A hardware technology for exchanging data with peripheral devices, defined by IEEE Standard 1394.

FTP File Transfer Protocol. A protocol that allows computers to transfer files over a network. FTP clients using any operating system that supports FTP can connect to a file server and download files, depending on their access privileges. Most Internet browsers and a number of freeware applications can be used to access an FTP server.

gateway A network node that interfaces one network to another. Often, it refers to a computer that links a private LAN to a public WAN, with or without Network Address Translation. A router is a special kind of gateway that links related network segments.

group A collection of users who have similar needs. Groups simplify the administration of shared resources.

group folder A directory that organizes documents and applications of special interest to group members and allows group members to pass information back and forth among themselves.

guest computer An unknown computer that isn't included in a computer list on your server.

guest user A user who can log in to your server without a user name or password.

home directory A folder for a user's personal use. Mac OS X also uses the home directory, for example, to store system preferences and managed user settings for Mac OS X users.

host Another name for a server.

HTML Hypertext Markup Language. The set of symbols or codes inserted in a file to be displayed on a World Wide Web browser page. The markup tells the web browser how to display a webpage's words and images for the user.

HTTP Hypertext Transfer Protocol. The client/server protocol for the World Wide Web. The HTTP protocol provides a way for a web browser to access a web server and request hypermedia documents created using HTML.

IANA Internet Assigned Numbers Authority. An organization responsible for allocating IP addresses, assigning protocol parameters, and managing domain names.

ICMP Internet Control Message Protocol. A message control and error-reporting protocol used between host servers and gateways. For example, some Internet software applications use ICMP to send a packet on a round-trip between two hosts to determine round-trip times and discover problems on the network.

IGMP Internet Group Management Protocol. An Internet protocol used by hosts and routers to send packets to lists of hosts that want to participate in a process known as multicasting. QuickTime Streaming Server (QTSS) uses multicast addressing, as does Service Location Protocol (SLP).

IMAP Internet Message Access Protocol. A client-server mail protocol that allows users to store their mail on the mail server rather than download it to the local computer. Mail remains on the server until the user deletes it.

Internet Generally speaking, a set of interconnected computer networks communicating through a common protocol (TCP/IP). The Internet (note the capitalization) is the most extensive publicly accessible system of interconnected computer networks in the world.

intranet A network of computers operated by and for the benefit of an organization's internal users. Access is commonly restricted to members of the organization. Many times, it refers to a web site for the organization which is accessible only from within the organization. Intranets use the same networking technologies as the Internet (TCP/IP), and sometimes bridge legacy information systems with modern networking technologies.

IP Internet Protocol. Also known as IPv4. A method used with Transmission Control Protocol (TCP) to send data between computers over a local network or the Internet. IP delivers packets of data, while TCP keeps track of data packets.

IP address A unique numeric address that identifies a computer on the Internet.

IPP Internet Printing Protocol. A client-server protocol for printing over the Internet. The Mac OS X printing infrastructure and the Mac OS X Server print service that's built on it support IPP.

IP subnet A portion of an IP network, which may be a physically independent network segment, that shares a network address with other portions of the network and is identified by a subnet number.

ISP Internet service provider. A business that sells Internet access and often provides web hosting for ecommerce applications as well as mail services.

Jboss A full-featured Java application server that provides support for Java 2 Platform, Enterprise Edition (J2EE) applications.

Kerberos A secure network authentication system. Kerberos uses tickets, which are issued for a specific user, service, and period of time. Once a user is authenticated, it's possible to access additional services without retying a password (this is called single sign-on) for services that have been configured to take Kerberos tickets. Mac OS X Server uses Kerberos v5.

Kerberos realm The authentication domain comprising the users and services that are registered with the same Kerberos server. The registered services and users trust the Kerberos server to verify each other's identities.

LAN Local area network. A network maintained within a facility, as opposed to a WAN (wide area network) that links geographically separated facilities.

LDAP Lightweight Directory Access Protocol. A standard client-server protocol for accessing a directory domain.

lease period A limited period of time during which IP addresses are assigned. By using short leases, DHCP can reassign IP addresses on networks that have more computers than available IP addresses.

load balancing The process of distributing client computers' requests for network services across multiple servers to optimize performance.

local domain A directory domain that can be accessed only by the computer on which it resides.

local home directory A home directory that resides on disk on the computer a user is logged in to. It's accessible only by logging directly in to the computer where it resides unless you log in to the computer using SSH.

local hostname A name that designates a computer on a local subnet. It can be used without a global DNS system to resolve names to IP addresses. It consists of lower-case letters, numbers, or hyphens (except as the last characters), and ends with ".local" (e.g, bills-computer.local). Although the name is derived by default from the computer name, a user can specify this name in the Network pane of System Preferences. It can be changed easily, and can be used anywhere a DNS name or fully qualified domain name is used. It can only resolve on the same subnet as the computer using it.

long name The long form of a user or group name. See also **user name**.

LPR Line Printer Remote. A standard protocol for printing over TCP/IP.

mail host The computer that provides your mail service.

managed client A user, group, or computer whose access privileges and/or preferences are under administrative control.

managed network The items managed clients are allowed to "see" when they click the Network icon in a Finder window. Administrators control this setting using Workgroup Manager. Also called a "network view."

managed preferences System or application preferences that are under administrative control. Workgroup Manager allows administrators to control settings for certain system preferences for Mac OS X managed clients.

MTA Mail Transfer Agent. A mail service that sends outgoing mail, receives incoming mail for local recipients, and forwards incoming mail of nonlocal recipients to other MTAs.

multihoming The ability to support multiple network connections. When more than one connection is available, Mac OS X selects the best connection according to the order specified in Network preferences.

MySQL An open-source relational database management tool frequently used by web servers.

name server A server on a network that keeps a list of names and the IP addresses associated with each name. See also **DNS**, **WINS**.

NAT Network Address Translation. A method of connecting multiple computers to the Internet (or any other IP network) using one IP address. NAT converts the IP addresses you assign to computers on your private, internal network into one legitimate IP address for Internet communications.

nested group A group that is a member of another group. Nested groups enable administrators to manage groups of users at a global level (to influence all members of a group) and at a smaller level (to influence only certain members of a group).

NetBoot server A Mac OS X server on which you've installed NetBoot software and have configured to allow clients to start up from disk images on the server.

NetInfo One of the Apple protocols for accessing a directory domain.

network installation The process of installing systems and software on Mac OS X client computers over the network. Software installation can occur with an administrator attending the installations or completely unattended.

NFS Network File System. A client/server protocol that uses Internet Protocol (IP) to allow remote users to access files as though they were local. NFS exports shared volumes to computers according to IP address, rather than user name and password.

Open Directory The Apple directory services architecture, which can access authoritative information about users and network resources from directory domains that use LDAP, NetInfo, or Active Directory protocols; BSD configuration files; and network services.

Option 95 A new option in the Bootstrap Protocol (BootP) and the Dynamic Host Configuration Protocol (DHCP) that lets clients find LDAP servers, their ports, base distinguished names (DNs), and other attributes. The configuration is returned to the DHCP client as a list of LDAP URLs according to a predefined syntax.

owner The owner of an item can change access permissions to the item. The owner may also change the group entry to any group in which the owner is a member. By default the owner has Read & Write permissions.

PAP Printer Access Protocol. The standard protocol based on AppleTalk that is used on Mac OS X, Mac OS X Server, and other platforms for transmitting print job data to a printer or print server.

PHP PHP Hypertext Preprocessor (originally Personal Home Page). A scripting language embedded in HTML that's used to create dynamic webpages.

POP Post Office Protocol. A protocol for retrieving incoming mail. After a user retrieves POP mail, it's stored on the user's computer and is usually deleted automatically from the mail server.

predefined accounts User accounts that are created automatically when you install Mac OS X. Some group accounts are also predefined.

preference manifest A file that describes the structure of and default values for an application's preferences (for example, what the various preference keys do). Workgroup Manager's preferences editor uses these files to make it easier for an administrator to edit an application's managed preferences.

preferences cache A storage place for computer preferences and preferences for groups associated with that computer. Cached preferences help you manage local user accounts on portable computers.

presets Initial default attributes you specify for new accounts you create using Workgroup Manager. You can use presets only during account creation.

primary group A user's default group. The file system uses the ID of the primary group when a user accesses a file he or she doesn't own.

primary group ID A unique number that identifies a primary group.

privileges The right to access restricted areas of a system or perform certain tasks (such as management tasks) in the system.

QTSS QuickTime Streaming Server. A technology that lets you deliver media over the Internet in real time.

RAID array A group of physical disks organized and protected by a RAID scheme and presented by RAID hardware or software as a single logical disk. In Xsan, RAID arrays appear as LUNs, which are combined to form storage pools.

RAID level A storage allocation scheme used for storing data on a RAID array. Specified by a number, as in RAID 3 or RAID 0+1.

realm Definition TBD; general term with multiple applications. See **WebDAV realm**, **Kerberos realm**.

search path See **search policy**.

search policy A list of directory domains searched by a Mac OS X computer when it needs configuration information; also the order in which domains are searched. Sometimes called a search path.

shadow image A file created by the NetBoot daemon process for each NetBooted client where applications running on the client can write temporary data.

share point A folder, hard disk (or hard disk partition), or CD that's accessible over the network. A share point is the point of access at the top level of a group of shared items. Share points can be shared using AFP, Windows SMB, NFS (an "export"), or FTP protocols.

short name An abbreviated name for a user. The short name is used by Mac OS X for home directories, authentication, and email addresses.

Simplified Finder A user environment featuring panels and large icons that provide novice users with an easy-to-navigate interface. Mounted volumes or media to which users are allowed access appear on panels instead of on the standard desktop.

SMB/CIFS Server Message Block/Common Internet File System. A protocol that allows client computers to access files and network services. It can be used over TCP/IP, the Internet, and other network protocols. Windows services use SMB/CIFS to provide access to servers, printers, and other network resources.

SMTP Simple Mail Transfer Protocol. A protocol used to send and transfer mail. Its ability to queue incoming messages is limited, so SMTP usually is used only to send mail, and POP or IMAP is used to receive mail.

SNMP Simple Network Management Protocol. A set of standard protocols used to manage and monitor multiplatform computer network devices.

spam Unsolicited email; junk mail.

SSL Secure Sockets Layer. An Internet protocol that allows you to send encrypted, authenticated information across the Internet. More recent versions of SSL are known as TLS (Transport Level Security).

static IP address An IP address that's assigned to a computer or device once and is never changed.

subnet A grouping on the same network of client computers that are organized by location (different floors of a building, for example) or by usage (all eighth-grade students, for example). The use of subnets simplifies administration. See also **IP subnet**.

system-less client A computer that doesn't have an operating system installed on its local hard disk. System-less computers can start up from a disk image on a NetBoot server.

TCP Transmission Control Protocol. A method used along with the Internet Protocol (IP) to send data in the form of message units between computers over the Internet. IP takes care of handling the actual delivery of the data, and TCP takes care of keeping track of the individual units of data (called packets) into which a message is divided for efficient routing through the Internet.

Tomcat The official reference implementation for Java Servlet 2.2 and JavaServer Pages 1.1, two complementary technologies developed under the Java Community Process.

UID User ID. A number that uniquely identifies a user within a file system. Mac OS X computers use the UID to keep track of a user's directory and file ownership.

URL Uniform Resource Locator. The address of a computer, file, or resource that can be accessed on a local network or the Internet. The URL is made up of the name of the protocol needed to access the resource, a domain name that identifies a specific computer on the Internet, and a hierarchical description of a file location on the computer.

USB Universal Serial Bus. A standard for communicating between a computer and external peripherals using an inexpensive direct-connect cable.

user name The long name for a user, sometimes referred to as the user's "real" name. See also **short name**.

virtual user An alternate email address (short name) for a user. Similar to an alias, but it involves creating another user account.

VPN Virtual Private Network. A network that uses encryption and other technologies to provide secure communications over a public network, typically the Internet. VPNs are generally cheaper than real private networks using private lines but rely on having the same encryption system at both ends. The encryption may be performed by firewall software or by routers.

WAN Wide area network. A network maintained across geographically separated facilities, as opposed to a LAN (local area network) within a facility. Your WAN interface is usually the one connected to the Internet.

WebDAV Web-based Distributed Authoring and Versioning. A live authoring environment that allows client users to check out webpages, make changes, and then check the pages back in while a site is running.

WebDAV realm A region of a website, usually a folder or directory, that's defined to provide access for WebDAV users and groups.

Windows domain The Windows computers on a network that share a common directory of user, group, and computer accounts for authentication and authorization. An Open Directory master can provide the directory services for a Windows domain.

WINS Windows Internet Naming Service. A name resolution service used by Windows computers to match client names with IP addresses. A WINS server can be located on the local network or externally on the Internet.

workgroup A set of users for whom you define preferences and privileges as a group. Any preferences you define for a group are stored in the group account.

A

- access control lists (ACLs) 43
- Active Directory 34
- administrator computer setup 59
- AirPort 49
- Apache 46
- Apple File Service (AFP) 43
- Apple Remote Desktop (ARD) 75
- AppleTalk 37
- application servers 51
 - AXIS 52
 - JBoss 52
 - SOAP 52
 - Tomcat 52
 - WebObjects 53
- automatic restart 54
- automating server setup 124
- automating server software installation 106

B

- basic password validation 36
- Berkeley Software Distribution (BSD) 33, 34

C

- CGI scripts 46
- collaboration services 53
- command-line tools 75
- core system services 33

D

- Darwin 33
- Directory Access 60
- directory services 34
- disk space monitoring 54
- diskspacemonitor tool 54
- Disk Utility 54
- documentation 13
- Domain Name System (DNS) 48
- Dynamic Host Configuration Protocol (DHCP) 48
- dynamic websites 46

E

- example setup 149
- exporting NFS volumes 44
- exporting users and groups 62

F

- file services 42
 - Apple File Service (AFP) 43
 - File Transfer Protocol (FTP) 44
 - Network File System (NFS) 44
 - sharing 42
 - Windows 43
- file sharing 42
- File Transfer Protocol (FTP) 44

G

- Gateway Setup Assistant 72
- group accounts 37

H

- high availability 54
- home directories 38

I

- iChat service 53
- importing accounts 62
- installation 79
- installation and setup worksheet 137
- installation planning
 - changing the server's host name after setup 98
 - collecting and organizing information 98
 - defining a migration strategy 94, 100
 - defining an integration strategy 95
 - defining physical requirements 95
 - determining a strategy 98
 - determining server setup infrastructure requirements 96
 - determining services to host 92
 - goals 91
 - identifying servers you'll set up 92
 - making sure hardware is available 97

- minimizing the need to relocate servers after setup 97
- setting up a team 91
- Installer 60
- installing server software
 - automating installation 106
 - disk preparation 101
 - hardware-specific tasks 102
 - information you need 100
 - interactive remote installation 104
 - on Mac OS X version 10.4 computers 106
 - preset password 102
 - system requirements 100
 - using Installer locally 103
 - using the installer tool 107
- integrating into existing networks 54
- IP failover 50

J

- J2EE 52
- Java 46
- JBoss 52
- journalized HFS disks 54

K

- Kerberos 36

L

- LDAP 34
- link aggregation 55
- log rolling 54

M

- Macintosh user management
 - mobile accounts 39
 - preference management 38
- mail service
 - authentication 47
 - Cyrus 47
 - filtering junk mail and viruses 47
 - Mailman 47
 - Postfix 47
 - SpamAssassin 47
 - SquirrelMail 47
- managed network views 39
- migration 94, 100
- mobile accounts 39
- multicast DNS 37
- MySQL 46

N

- nested groups 37
- NetBoot 41
- NetInfo 34
- Network Address Translation (NAT) 49

- network browsing using managed Network views 39
- Network File System (NFS) 44
- Network Information System (NIS) 34
- Network Install 41
- network services 48
 - DHCP 48
 - DNS 48
 - Gateway Setup Assistant 50
 - IP failover 50
 - IP firewall 49
 - managed network views 39
 - NAT 49
 - VPN 49
- non-Mac OS X workstation setup 59

O

- Open Directory
 - automatic LDAP schema replication 35
 - definition 34
 - directory access controls 35
 - discovery of network services 37
 - Kerberos authentication 36
 - LDAP replication 54
 - password validation 36
 - search policies 35
 - trusted binding 35
 - using Apple directories 34
 - using non-Apple directories 34
- OpenLDAP 34
- operating system image services 40
- opportunistic locking 43

P

- PackageMaker 73
- password validation 36
- Perl 46
- PHP 46
- POR.err 130
- POR.status 131
- preference editor 39
- preference manifests 39
- preparing disks for installing server software 101
- preset 62
- print service 45
- Property List Editor 73

Q

- QTSS Publisher 51
- QuickTime Broadcaster 51
- QuickTime Streaming Server (QTSS) 51

R

- resharing NFS mounts 44

S

- scenarios
 - computational clustering 29
 - data centers 31
 - departments and workgroups 20
 - higher-education facilities 25
 - K–12 labs and classrooms 27
 - small and medium businesses 23
- search policies 35
- Server Admin 67
 - administering services 70
 - controlling access to services 71
 - customizing the Server Admin environment 72
 - opening and authenticating 68
 - using SSL for remote server administration 71
 - working with servers 68
- server administration guides 13
- Server Assistant 60
- Server Message Block /Common Internet File System (SMB/CIFS) 37
- Server Monitor 73
- server setup 79
 - automated setup using directory data 127
 - automatic setup using data in a file 124
 - basic settings that are established 84
 - example 149
 - information you need 112
 - keeping backup copies of saved setup data 115
 - local interactive setup 120
 - offline mode 124
 - Open Directory usage 116
 - remote interactive batch setup 121
 - remote interactive multiserver setup 123
 - remote interactive setup 120
 - saving setup data in a directory 114
 - saving setup data in a file 113
 - status monitoring 130
- service discovery 34
- Service Location Protocol (SLP) 37
- service setup 131
- share points 42
- sharing files 42
- Simple Authentication and Security Layer (SASL)
 - password validation 36
- single sign-on 36
- software RAID 54
- software update service 41
- SquirrelMail 47
- SSH 75
- strict locking 43

System Image Utility 73

T

- Terminal 75
- Tomcat 52

U

- unified file locking 43
- UNIX shells 75
- upgrading from an earlier server version 94
- user management
 - group accounts 37
 - home directories 38
 - Macintosh user management 38
 - user accounts 37
 - Windows user management 40

V

- version 10.3 server management 76
- Virtual Private Network (VPN) 49

W

- Web-Based Distributed Authoring and Versioning (WebDAV) 46
- web cache 46
- Weblog service 53
- web service 46
- Windows
 - browsing 43
 - file service 43
 - integration 54
 - migration from 94
 - user management 40
- Windows Internet Naming Service (WINS) 43
- Workgroup Manager 61
 - administering accounts 62
 - configuring managed network views 66
 - customizing the Workgroup Manager environment 67
 - defining managed preferences 63
 - managing sharing 65
 - opening and authenticating 61
 - working with directory data 64
- worksheet 137

X

- Xgrid Admin 76
- Xgrid computational service 55