



Mac OS X Server Getting Started

For Version 10.3 or Later



🍏 Apple Computer, Inc.

© 2003 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.

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, AppleScript, AppleShare, AppleTalk, ColorSync, FireWire, iMac, Keychain, Mac, Macintosh, Power Mac, Power Macintosh, QuickTime, Sherlock, WebObjects, and Xserve are trademarks of Apple Computer, Inc., registered in the U.S. and other countries. eMac, Extensions Manager, Finder, and iPod 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.

Netscape Navigator is a trademark of Netscape Communications Corporation.

RealAudio is a trademark of Progressive Networks, Inc.

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

034-2412-A/09-20-03

Contents

Preface	9 About This Guide
	9 What's New in Version 10.3
	9 Superior Performance and Scalability
	10 Improved Setup, Management, and Monitoring
	11 Enhanced Network and Directory Services
	12 Improved Windows Integration
	13 New Workgroup and Desktop Management Features
	13 What's Included in This Guide
	13 Part I: Introduction to Mac OS X Server
	13 Part II: Installation and Initial Setup
	13 Glossary
	14 Getting Additional Information

Part I Introduction to Mac OS X Server

Chapter 1	19 Mac OS X Server in Action
	20 Enterprise Organizations
	21 Higher-Education Facilities
	22 K-12 Labs and Classrooms
	24 Small and Medium Businesses
	25 Computational Clustering
	26 Creative Businesses
	27 Web Service Providers
Chapter 2	29 Inside Mac OS X Server
	29 Core System Services
	30 Open Directory
	30 Using Apple Directories
	31 Using Other Directories
	31 Search Policies
	31 Authentication
	32 Single Signon

32	Discovery of Network Services
32	User Management
32	User Accounts
33	Group Accounts
33	Home Directories
33	Macintosh User Management
34	Windows User Management
34	System Image Services
34	NetBoot
35	Network Install
35	File Services
36	Sharing
36	Apple File Service
36	Windows Services
37	Network File System (NFS) Service
37	File Transfer Protocol (FTP)
38	Print Service
38	Web Service
39	Mail Service
40	Network Services
40	DHCP
40	DNS
41	Firewall
41	NAT
42	VPN
42	IP Failover
42	Media Streaming and Broadcasting
43	Application Server Support
43	Apache Tomcat
44	JBoss
44	WebObjects
44	Integrating Into Existing Environments
45	High Availability
45	Server Administration
47	Server Administration
47	Using the Administration Tools
48	Computers You Can Use to Administer a Server
49	Setting Up an Administrator Computer
49	Using a Non-Mac OS X Computer for Administration
50	Installer
50	Server Assistant
50	Directory Access

Chapter 3

51	Workgroup Manager
51	Opening and Authenticating in Workgroup Manager
52	Using Workgroup Manager
55	Server Admin
55	Opening and Authenticating in Server Admin
55	Using Server Admin
58	System Image Management
58	Server Monitor
59	Media Streaming Management
59	Apple Remote Desktop
60	Command-Line Tools
60	Macintosh Manager
60	Working With Version 10.2 Servers From Version 10.3 Servers

Part II

Installation and Initial Setup

Chapter 4

63	Installation and Setup Overview
63	Planning
64	Installing Server Software
64	Local Installation From the Server Install Discs
65	Remote Installation From the Server Install Discs
66	Automating Server Installation With a Disk Image
67	Initial Server Setup
67	Setting Up Servers Interactively
69	Automating Server Setup
72	Setting Up Services
72	Keeping Current

Chapter 5

73	Before You Begin
73	Set Up a Planning Team
74	Identify the Servers You'll Need to Set Up
74	Determine Services to Host on Each Server
75	Define a Migration Strategy
76	Define an Integration Strategy
76	Define Physical Infrastructure Requirements
77	Define Server Setup Infrastructure Requirements
78	Make Sure Required Server Hardware Is Available
78	Determine the Installation and Setup Strategy to Use
78	Collect and Organize Information

Chapter 6

79	Installing Server Software
79	Understanding System Requirements for Installing Mac OS X Server

80	Information You Need
80	Upgrading From Version 10.1 or 10.2
81	Preparing Disks for Installing Mac OS X Server
82	Hardware-Specific Instructions for Installing Mac OS X Server
82	Identifying Remote Servers When Installing Mac OS X Server
82	Installing Server Software Interactively From the Install Discs
82	Using Installer to Install Locally From the Install Discs
83	Using Server Assistant to Install Remotely From the Install Discs
85	Installing Server Software on a Computer With Mac OS X Version 10.3 Preinstalled
85	Automating Server Software Installation With a Disk Image
85	Using the <code>installer</code> Command-Line Tool to Install Server Software
88	Installing Optional Server Software

Chapter 7

89	Initial Server Setup
90	Information You Need
90	Saving Setup Data
93	Specifying Initial Open Directory Usage
96	Using Interactive Server Setup
96	Setting Up a Local Server Interactively
97	Postponing Local Server Setups Following Installation
97	Setting Up a Remote Server Interactively
98	Setting Up Multiple Remote Servers Interactively in a Batch
99	Setting Up Multiple Remote Servers Interactively One at a Time
100	Using Automatic Server Setup
101	Setting Up Servers Automatically Using Data Saved in a File
103	Setting Up Servers Automatically Using Data Saved in a Directory
106	Determining the Status of Setups
106	Setting Up Services
106	Setting Up Open Directory
107	Setting Up User Management
107	Setting Up File Services
108	Setting Up Print Service
108	Setting Up Web Service
109	Setting Up Mail Service
109	Setting Up Network Services
109	Setting Up System Image Services
109	Setting Up Media Streaming and Broadcasting
110	Setting Up an Application Server

Appendix A

111	Mac OS X Server Worksheet
-----	----------------------------------

Appendix B

119	Setup Example
119	Mac OS X Server in a Small Business

	120	How to Set Up the Server
Glossary	127	
Index	137	

About This Guide

This guide provides an orientation to the features and initial setup of Mac OS X Server version 10.3.

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

What's New in Version 10.3

Mac OS X Server version 10.3 builds on the award-winning capabilities of version 10.2 with major enhancements in the following key areas:

- Performance and scalability
- Setup, management, and monitoring
- Network and directory services
- Windows integration
- Workgroup and desktop management

Superior Performance and Scalability

Performance and scalability enhancements in Mac OS X Server version 10.3 deliver improved performance for key network services. Specific enhancements include:

- **Darwin 7.** Mac OS X Server version 10.3 features Darwin 7, the latest version of Apple's open-source UNIX- based core operating system. Darwin continues to utilize and build on the latest enhancements from the open-source community. Based largely on the highly stable FreeBSD 4.4, Darwin 7 also includes some of the latest enhancements from FreeBSD 5.
- **Enhanced performance.** For improved networking and file system performance, Mac OS X Server version 10.3 now supports asynchronous I/O, up to 16 TB file systems, and Jumbo Frames for large Ethernet packets. HFS+ with journaling is now the default file system, and a new case-sensitive option for HFS+ makes it easier to support legacy UNIX applications on Mac OS X Server.

- **Optimized for the G5.** Mac OS X Server version 10.3 features support for Apple's G5 systems. In addition to benefiting from the increased performance and faster clock speed of the ultrafast 64-bit processor, Mac OS X Server enables users to leverage the advanced capabilities of the G5-based architecture, such as native double-precision (64-bit) arithmetic and support for more than 4 GB of physical memory.

Improved Setup, Management, and Monitoring

Ease of use and simplicity continue to make Mac OS X Server the easiest way to deploy and maintain open-source server solutions. Enhancements to version 10.3 include:

- **Automatic setup.** Automatic setup lets you configure entire racks of servers as easily as you can set up a single server. This powerful new feature lets you set up networking and default services from configuration settings stored in a directory server, on an external FireWire or USB storage device, or even on an iPod. When starting up for the first time, Mac OS X Server systems automatically check available hard drives and the directory server for this configuration information. Within seconds, the server locates the saved setup data and configures itself—automatically.
- **New Server Admin application.** The remote server administration tools in Mac OS X Server have been consolidated and enhanced in version 10.3. Server Admin provides integrated administration of services, now with support for OpenLDAP, DNS, NAT, VPN, QuickTime Streaming Server, NTP, and SNMP. The new Server Admin application provides a single-window interface for managing and monitoring all your network services:
 - You can start and stop services with a single button, modify settings, view real-time logs and activity graphs, monitor disk space, and even check networking and CPU activity.
 - It's easy to manage multiple servers from a single Server Admin window, and you can even drag settings from one server to another to replicate service configurations.
- **Improved Network Image Utility.** The new Network Image Utility makes it easier to create, modify and add packages to disk images for NetBoot and Network Install services. Network Image Utility also provides more administrative options, including easier system cloning and faster software install using Apple Software Restore.
- **New directory Inspector.** A new directory Inspector, available from Workgroup Manager, lets you view and edit raw LDAP data for fine-grained control of directory records.
- **New command-line tools.** New command-line tools allow enhanced server configuration and management from the terminal.

Enhanced Network and Directory Services

Network and directory services in Mac OS X Server version 10.3 have been greatly enhanced to provide more scalability, performance, and enterprise-strength capabilities:

- **Open Directory 2**—robust LDAP solution with Kerberos authentication. Mac OS X Server version 10.3 features Open Directory 2, the latest version of Apple's standards-based directory and authentication services architecture. Open Directory enables Mac OS X Server to provide network-wide directory and authentication services using LDAP, SASL, and Kerberos. Open Directory 2 brings scalability, availability, and advanced features to Mac OS X Server version 10.3.
- **Single signon.** Open Directory 2 now includes MIT's Kerberos Key Distribution Center (KDC) service for secure network-based authentication and single signon. This feature allows users to authenticate once—using a single password—and have access to all Kerberos-enabled services on the network. Single signon simplifies the user experience and provides the security of strong authentication.
- **New high-performance mail server.** Mac OS X Server version 10.3 features an all-new mail server based on the open-source Postfix SMTP and Cyrus IMAP and POP servers. Capable of supporting tens of thousands of users, the new mail server features:
 - Support for standard Internet mail protocols, including SMTP, IMAP, and POP
 - A high-performance database for indexing of mail stored on the server
 - Secure Sockets Layer (SSL) encryption of SMTP, IMAP, and POP for secure, confidential transport of mail messages between the server and mail clients
 - Open architecture for integration with third-party server-side spam and virus filtering solutions
 - Mailman for managing mailing lists.
- **High-performance Java application server.** Mac OS X Server is now the easiest way to develop and deploy applications based on Sun's J2EE (Java 2 Enterprise Edition) standard. It features a built-in JBoss application server for running J2EE applications, including Enterprise Java Bean (EJB) components. Mac OS X Server version 10.3 also features new application deployment tools with a graphical user interface, making it easier to configure existing J2EE applications for hosting on Mac OS X Server.
- **QuickTime Streaming Server 5.** Mac OS X Server version 10.3 features QuickTime Streaming Server 5, the next generation of Apple's industrial-strength, standards-based streaming server. QTSS setup and monitoring are now integrated into Server Admin for easier management. Additional new features and enhancements in QTSS 5 include:
 - QTSS Publisher—This new tool for managing QuickTime media makes it easy to upload and download content to the server, create and schedule playlists, hint movies, and generate reference movies.
 - Real-time playlist updates—You can make changes on the fly without disrupting your viewers.

- Support from home directories—Support for streaming movies from users' network home directories.
- **Apache web server deployment and configuration enhancements.** Mac OS X Server version 10.3 features an enhanced user interface for configuring Apache—the world's most widely used web server. Part of Server Admin, the new web server interface makes it easier to set up and manage multiple websites and deploy advanced configuration options, such as URL redirects, website aliases, and realm support settings.
- **VPN server for secure remote network access.** Mac OS X Server version 10.3 includes a new Virtual Private Network (VPN) server for providing individual computers with secure remote access to your Local Area Network (LAN). VPN technology enables IP traffic to travel securely over a public TCP/IP network by using “tunneling” to encrypt all data between the client system and the host network. Apple's VPN server offers support for hundreds of VPN clients per server, making it ideal for small and medium-sized businesses.

Improved Windows Integration

Mac OS X Server is designed to be a comprehensive server solution for heterogeneous network environments, and version 10.3 expands on this solution with improved support for Windows clients and Windows proprietary directory server.

- **Samba 3.** Mac OS X Server version 10.3 now ships with Samba 3. This latest version of the popular open-source project delivers high-performance, reliable file and print services to Windows clients using the native SMB/CIFS file sharing protocol. It supports Unicode for multilingual file and user names with 16-bit characters. Samba 3 also enables support for Primary Domain Controller (PDC) services, a feature integrated into Open Directory 2 to provide login and authentication for Windows users right from the PC's login window.
- **Network home directories for Windows clients.** Open Directory 2 provides support for roaming profiles, the Windows equivalent of network home directories. Mac OS X Server version 10.3 can now host home and group directories that can be accessed from both Mac and Windows clients.
- **VPN services for Windows.** The built-in VPN server in Mac OS X Server version 10.3 supports Windows clients using PPTP or L2TP/IPSec.
- **Simpler integration with Active Directory.** Mac OS X Server version 10.3 can now access user, group, and computer records stored in Microsoft's proprietary directory server without requiring modifications to the Active Directory schema. It also supports Microsoft's Kerberos implementation for accessing authenticated services hosted on Mac OS X Server.

New Workgroup and Desktop Management Features

Mac OS X Server version 10.3 improves your ability to manage Macintosh client desktops:

- **Enhanced image management.** You can create a NetBoot or Network Install image that mimics an existing system. The source of the image can be a volume or a partition. Other image management enhancements include improved client filtering and diskless NetBoot for Mac OS X clients.
- **Mobile accounts.** Workgroup Manager lets you set up mobile accounts. Mobile accounts let the user of a Mac OS X version 10.3 or later computer work offline, but continue to log in using the network name and password and experience the same managed preference settings.
- **Enhanced preference management.** Workgroup Manager also features new system controls for lab environments, including Energy Saver settings and management of automatic logout.

What's Included in This Guide

This guide is organized into two parts and 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 server software and set up a server for the first time. Part II includes two appendixes.

Appendix A: Mac OS X Server Worksheet

Use this worksheet to record information you'll need when you install and set up Mac OS X Server.

Appendix B: Setup Example

This example illustrates how you might install Mac OS X Server and perform initial server setup in a small business scenario.

Glossary

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

Getting Additional Information

Mac OS X Server comes with a suite of guides that explain the services and provide instructions for configuring, managing, and troubleshooting them. Most of these documents come on the Mac OS X Server Administration Tools disc. All of them are available in PDF format from www.apple.com/server/documentation/.

This guide	Tells you how to
Mac OS X Server Migration To Version 10.3 or Later	Reuse data and service settings on Mac OS X Server version 10.3 that are currently being used on earlier versions of the server.
Mac OS X Server User Management For Version 10.3 or Later	Create and manage user, group, and computer accounts. Set up managed preferences for Mac OS 9 and Mac OS X clients.
Mac OS X Server File Services Administration For Version 10.3 or Later	Share selected server volumes or folders among server clients using these protocols: AFP, NFS, FTP, and SMB.
Mac OS X Server Print Service Administration For Version 10.3 or Later	Host shared printers and manage their associated queues and print jobs.
Mac OS X Server System Image Administration For Version 10.3 or Later	Create disk images and set up the server so that other Macintosh computers can start up from those images over the network. This guide covers NetBoot and Network Install.
Mac OS X Server Mail Service Administration For Version 10.3 or Later	Set up, configure, and administer mail services on the server.
Mac OS X Server Web Technologies Administration For Version 10.3 or Later	Set up and manage a web server, including WebDAV, WebMail, and web modules.
Mac OS X Server Network Services Administration For Version 10.3 or Later	Set up, configure, and administer DHCP, DNS, VPN, NTP, IP firewall, and NAT services on the server.
Mac OS X Server Open Directory Administration For Version 10.3 or Later	Manage directory and authentication services.
Mac OS X Server QuickTime Streaming Server Administration For Version 10.3 or Later	Set up and manage QuickTime streaming services.
Mac OS X Server Windows Services Administration For Version 10.3 or Later	Set up Mac OS X Server to provide services for Windows computer users.
Mac OS X Server Java Application Server Administration	How to configure and administer a JBoss application server on Mac OS X Server.
Mac OS X Server Command-Line Administration For Version 10.3 or Later	Use commands and configuration files to perform server administration tasks in a UNIX command shell. Using IP failover is documented in this guide.

For more information, consult these resources:

- Read Me documents contain important updates and special information. Look for them on the server discs.
- Online help, available from the Help menu in all the server applications, provides onscreen instructions for administration tasks as well as late breaking news and web updates.
- Apple support web pages and Knowledge Base provide answers to common questions and the latest information updates. These are available at www.info.apple.com/.

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

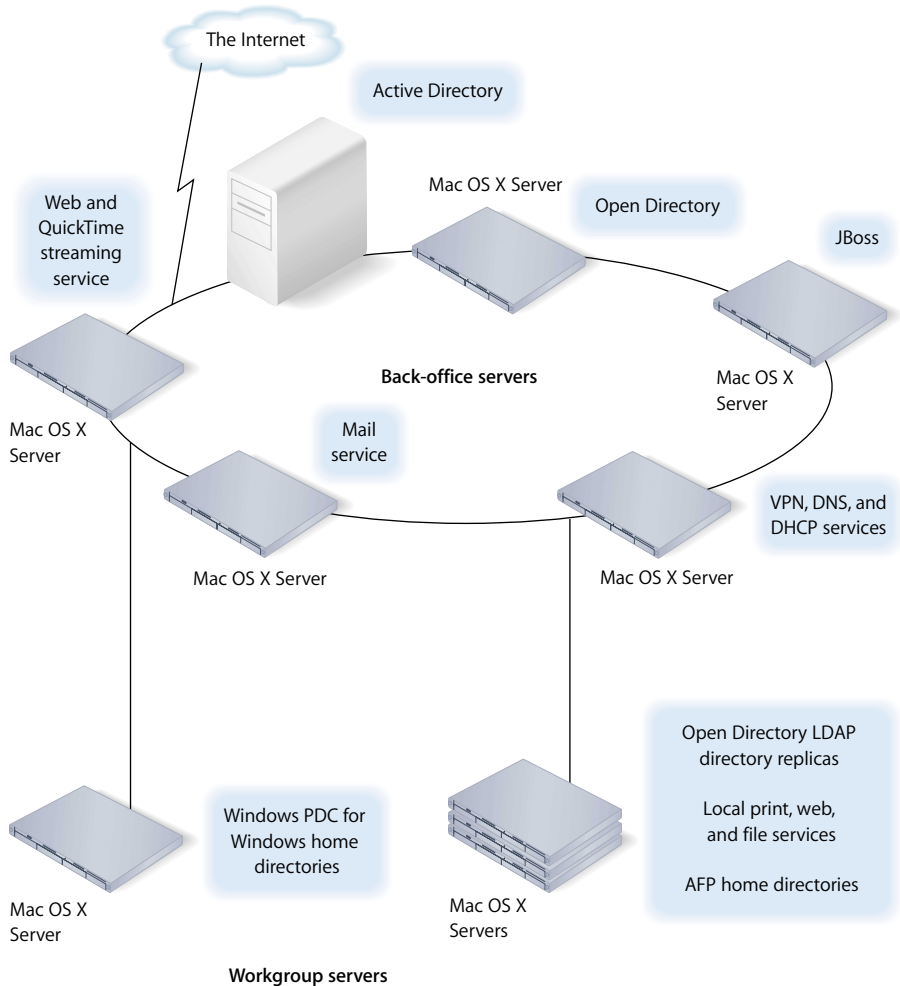
Mac OS X Server addresses the needs of many environments.

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

- Enterprise organizations
- Higher-education facilities
- K-12 labs and classrooms
- Small and medium businesses
- Computational clustering
- Creative businesses
- Web service providers

Enterprise Organizations

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



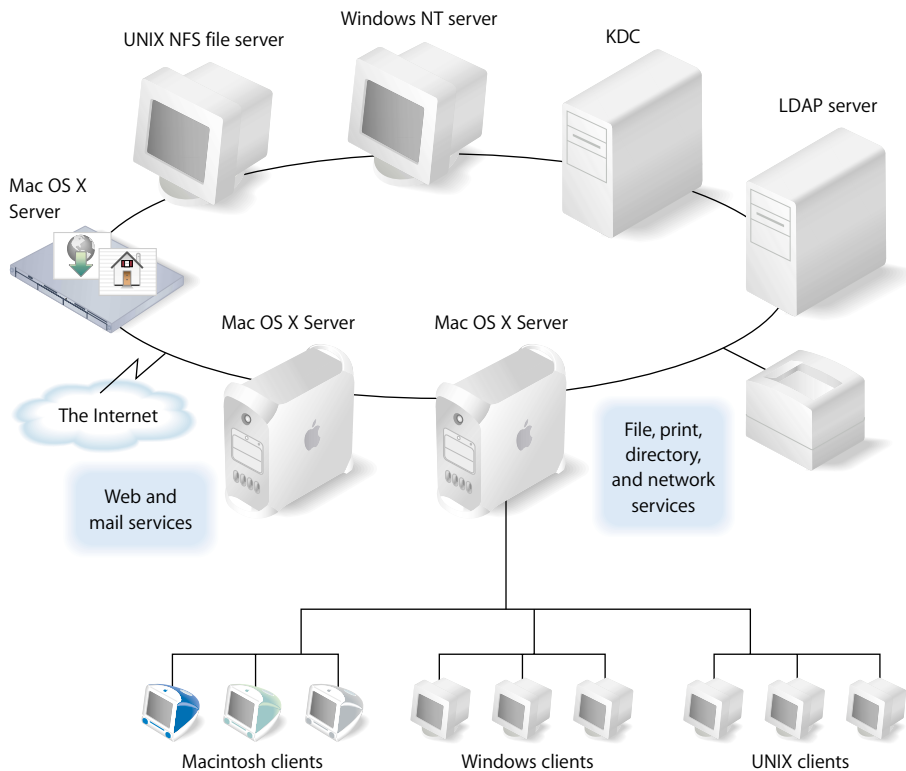
- Open Directory lets you manage directory data centrally, but distribute it geographically using replication.
- Other enterprise-level services might include Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Virtual Private Network (VPN), mail, web, streaming, and JBoss.
- JBoss is an application server that implements the Enterprise Edition (J2EE) technologies; JBoss runs on Java 1.4.1. 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 Xservers.

- Mac OS X Server integrates well with existing corporate services, from directory systems to Simple Network Management Protocol (SNMP) implementations.
- In addition to hosting replicated Open Directory domains for local authentication, departmental servers can be tailored to support workgroup needs.

If a department uses a lot of Windows computers, you can set up the department's Mac OS X Server as a Primary Domain Controller (PDC) so you can host Windows home directories. You can also provide VPN support, file and printer sharing, and Active Directory integration for Windows 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.

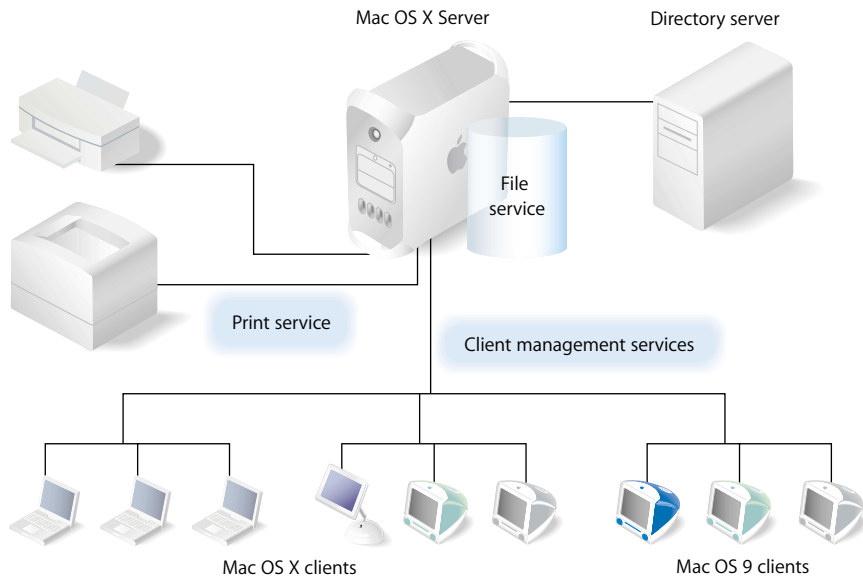


- The wide range of client computers—Macintosh, Windows, UNIX, Linux—demands flexible file access support. The highly scalable IP-based file services in Mac OS X Server support file access from anywhere on the network via Apple Filing Protocol (AFP), Network File System (NFS), File Transfer Protocol (FTP), and Server Message Block (SMB).
- 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.
- Authentication of Mac OS X Server users can also be done using an existing LDAP system or Kerberos Key Distribution Center (KDC).
- Network Install makes it easy to change software configurations—over the network—on hundreds of Macintosh client computers as often as you need to. 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, and the Windows SMB protocol.
- 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 need to be able to turn in assignments electronically or in print. Students also need access to applications (such as iLife) that facilitate learning but 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 perhaps update student records and other administrative information that is centralized on a remote server.

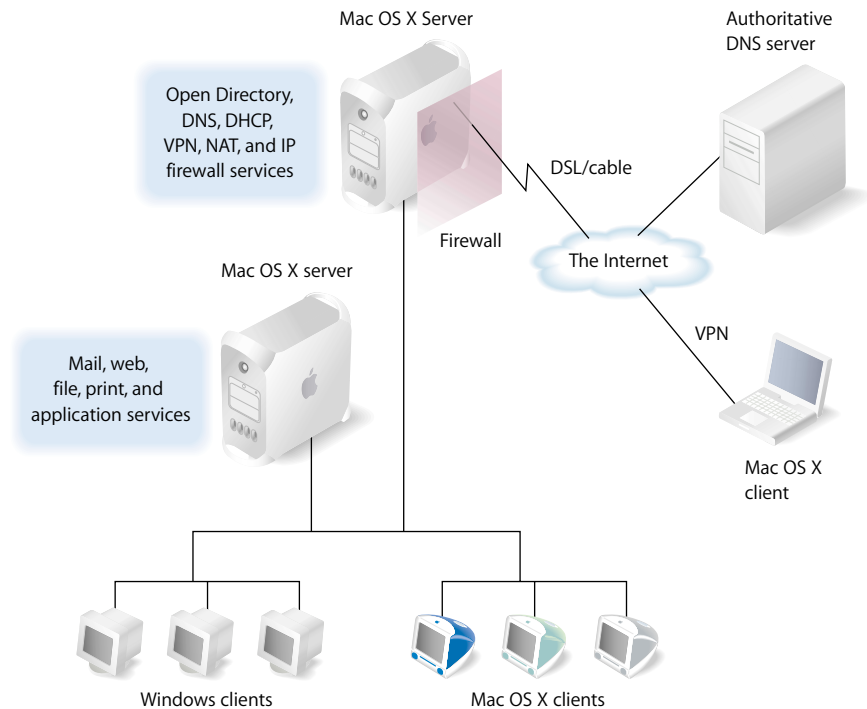


- Mac OS X Server's client management service provides a way to control student Macintosh computer work environments.
For example, you can control which applications students can access. You can also define application preferences, desktop patterns, and other desktop settings so that students experience the same environment on different computers.
- 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.
- For students who use portable Macintosh computers such as iBooks, mobile accounts let students work on assignments at home in an environment that mimics the look and feel and file access of the classroom environment. Preferences are cached on the portable computer, so they are available for offline use.
- Mac OS X Server's print service lets teachers manage student usage of classroom printers, including non-PostScript (inkjet) printers.

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, network services, mail, web, and database applications.

The directory and network services in the following picture reside on one Mac OS X Server, while a second server hosts mail, web, and other employee productivity services. In small businesses, all services might reside on a single server.

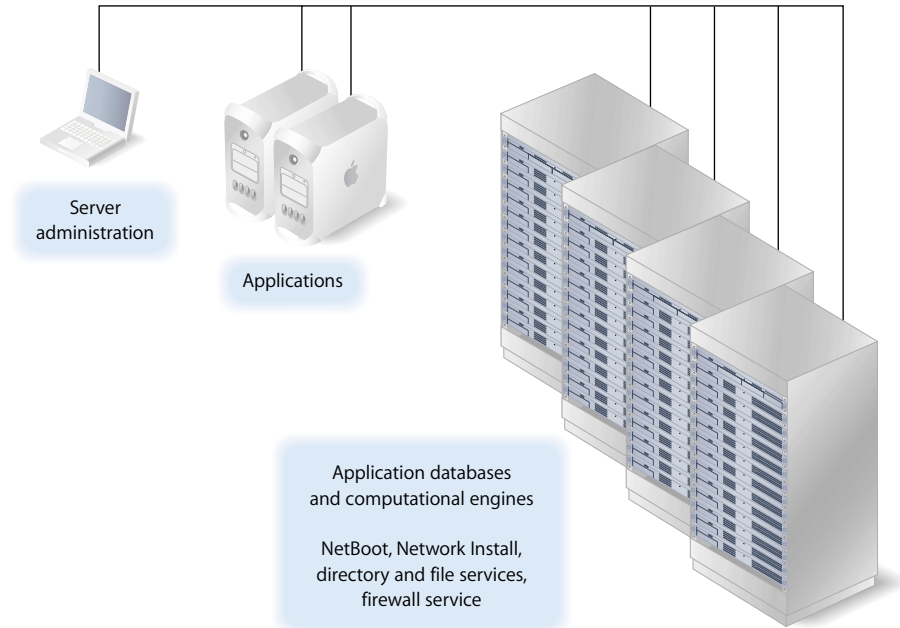


- The firewall between Mac OS X Server and the Internet protects the company intranet from access by unauthorized users.
- An authoritative DNS server hosted by another company provides domain name (example.com) resolution, while DNS services on Mac OS X Server provide names for the intranet devices (such as printers and client computers) that have static IP addresses.
- DHCP services provide dynamic IP addresses to some of the Macintosh and Windows clients.
- VPN service lets employees access the intranet to use mail, file, and other services when they are away from the office. Like all the other services shown, VPN supports both Macintosh and Windows clients.

- Network Address Translation (NAT) service lets employees share a single Internet connection. NAT converts all client IP addresses to one IP address for Internet communications.

Computational Clustering

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



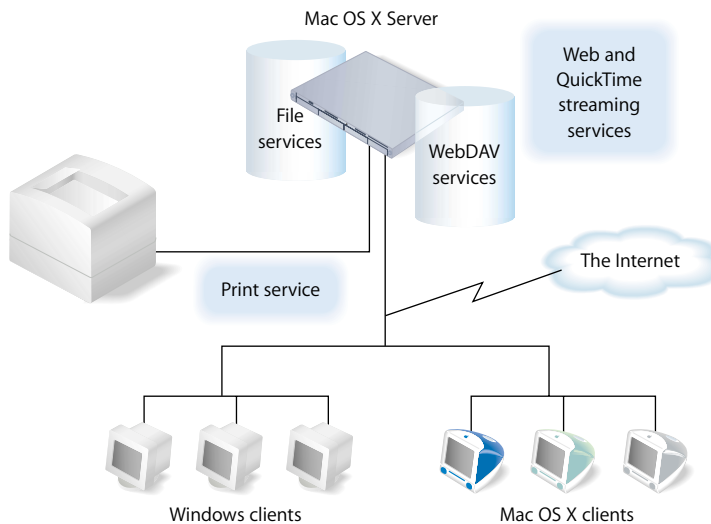
- One Xserve in a rack is usually set up as a master computer, called the *head node*. The head node runs NetBoot and Network Install and hosts directory services and other shared facilities for other computers in the rack, which are used for data processing and numerical computations.
- The head node 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.
- Scientists, videographers, and other application users work at Mac OS X computers to remotely configure and monitor applications and databases residing on the Xserves.
- 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 Project Builder.

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.

Creative Businesses

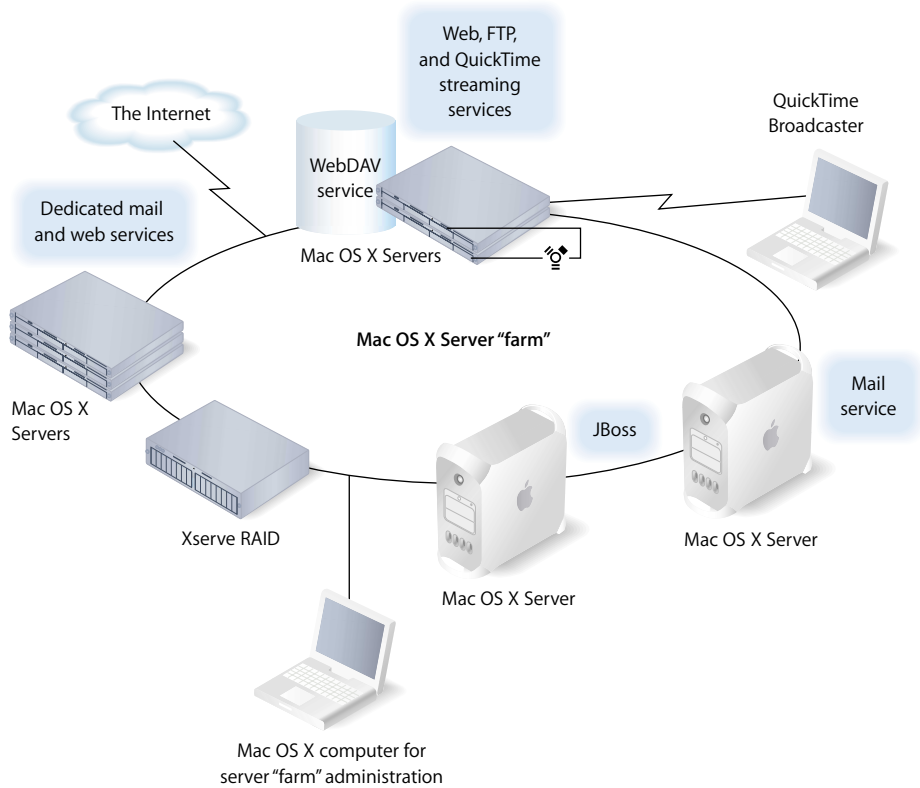
Mac OS X Server supports the workflow needs of creative professionals who design and produce video and audio projects.



- The popular open-source Apache HTTP web server is built into Mac OS X Server.
- Web-based Distributed Authoring and Versioning (or 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 an industry-standard streaming protocol.
- AFP lets you transfer large files among workgroup members. On an Xserve, you can increase the bandwidth of your file-transfer infrastructure by using jumbo frame Ethernet packets or utilizing both built-in Ethernet interfaces.

Web Service Providers

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.



You can configure Mac OS X Server computers for shared access by multiple users and companies. The term *server farm* is sometimes used to describe a collection of networked web servers that each has access to content on the same site and that together provide services for a particular group of users; if one server fails, another can act as its backup. Or you can dedicate servers for exclusive use by companies that don't want to host their own services.

- 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).

- QuickTime Streaming Server lets you broadcast multimedia in real time, including live QuickTime Broadcaster streams.
- Xserve RAID provides extended storage.
- High availability support includes automatic restart following a service or power failure and IP failover. IP failover can be configured using IP over FireWire, which lets you interconnect redundant servers without using up gigabit Ethernet ports.

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 4.4 BSD (Berkeley Software Distribution), high-performance networking facilities, and support for multiple integrated file systems.

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 their own unique address space. The Mach kernel augments standard virtual memory semantics with the abstraction of memory objects, providing support for separate simultaneous application environments while presenting users with a seamless experience.

Ease of use and simplicity are hallmarks of Mac OS X. Mac OS X is 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. Yet 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 47.

Open Directory

Open Directory is Mac OS X Server's directory services framework.

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 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:

- Rendezvous
- Server Message Block (SMB)
- 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 Apple Directories

Mac OS X Server can host LDAP directories and legacy NetInfo domains:

- NetInfo is the legacy Mac OS X directory system. Every Mac OS X computer has a local NetInfo directory, which stores information visible only to the computer on which it resides.

While version 10.3 of Mac OS X Server can be configured to support existing NetInfo directories, Open Directory LDAP, based on OpenLDAP, is the primary way to store directory information that you want to share with other computers.

- Open Directory LDAP directories are LDAPv3 directories that host shared directory data—data you want to be used by other computers. Open Directory LDAP directories are easy to manage, can be replicated for performance and backup, and support a much higher volume of information than NetInfo directories.

Apple directories offer you read-write control over directory data.

Using Other Directories

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

- On other LDAPv3 servers
- On Active Directory servers
- In Berkeley Software Distribution (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.

Search Policies

Before a user can log in to or connect with a Mac OS X client or server, he or she 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 DHCP Option 95 support, which lets a DHCP server send out information about the server from which a Mac OS X computer should obtain directory data at the same time it provides an IP address to the computer.

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, NT/LAN Manager 2, and SHA-1. It is the preferred way to authenticate Windows users.

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 offers the opportunity to integrate into existing Kerberos environments. You can also set up a Key Distribution Center (KDC) on Mac OS X Server, which offers support for password policies you set up on the server. Using Kerberos also provides a feature known as *single signon*, described in the next section.

The following services on Mac OS X Server support Kerberos authentication: AFP, mail, FTP, SSH, and login window.

- **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 Signon

When a Mac OS X user is authenticated using Kerberos, the user does not have to enter a user name and password every time he or she uses a Kerberized service.

The user enters the Kerberos name and password at login, but does not need to reenter it when using Apple file service, mail service, or other 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:

- Rendezvous, the Apple protocol that uses multicast DNS
- SMB, the protocol used by Microsoft Windows
- AppleTalk, the legacy Mac OS protocol for file services
- SLP, an open standard for discovering file and print services

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.

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 9 and Mac OS X computer users:

- Preference management and mobile accounts are summarized next.
- For information about automating the operating system images on Macintosh client computers, see "System Image Services" on page 34.

Preference Management

You can use Mac OS X Server to manage the work environments of Mac OS 9 and Mac OS X clients. To manage Mac OS 9 clients, you use Macintosh Manager. To manage Mac OS X clients, you use Workgroup Manager.

Preferences you define for individual accounts (for users, groups, and computers) provide your Macintosh users with a consistent desktop, application, and network appearance regardless of the Macintosh computer they use.

Mac OS X client management offers several advantages:

- When you update user, group, or computer accounts, managed Mac OS X users inherit changes automatically. Mac OS 9 accounts must be updated independently, using Macintosh Manager.
- You have more direct control over individual system preferences.
- Network home directories and directories you can set up for use by individual groups can be mounted automatically at login.
- You can use DHCP Option 95 to identify a server from which a client computer retrieves directory information at login. The directory service configuration is automatically downloaded from the network, setting up the user's network access policies, preferences, and desktop configuration without the need to configure the client computer directly.

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

Mobile Accounts

Mobile accounts let the user of a Mac OS X version 10.3 or later computers work offline but continue to

- Log in using the network name and password
- Experience the same managed preference settings

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

A user account can contain both Macintosh and Windows attributes, so users can log in from both kinds of computers.

Windows users can also use Mac OS X Server's VPN, file, and print services, as later sections in this chapter describe.

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 so that Mac OS 9 or Mac OS X computers can start up from 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 that's already been 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 Xserves. It's ideal for an organization with a number of 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 9 or 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 simply 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 just 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 CDs 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 an excellent solution for operating system migrations, installing software updates, installing site-licensed or custom applications, restoring computer classrooms and labs, and reimaging 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, it installs its contents on the client machine without user intervention.

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 four file services:

- Apple file service, which uses the Apple Filing Protocol (AFP), lets you share resources with clients who use Mac OS 8, Mac OS 9, and Mac OS X.
- Windows services use Server Message Block (SMB) 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 (Millennium Edition), 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).

The file services administration guide describes how to set up and manage Mac OS X Server file services. The Windows services administration guide provides information on sharing files with Windows users.

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, Windows, 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 Mac OS 9 computers, users access share points using the Chooser. On Windows computers, users use Network Neighborhood.

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 after a period of inactivity
- IPv6 support for AFP clients and server

AFP also lets you reshare NFS mounts using AFP. This feature provides a way for clients not on the local network to access NFS volumes via a secure, authenticated AFP connection. It also lets Mac OS 9 clients access NFS file services on traditional UNIX networks.

Windows Services

Windows file service in Mac OS X Server allows Windows clients to connect to Mac OS X Server using SMB 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

Windows file service provides several ways to manage locks for Windows share points:

- Opportunistic locking offers a way to optimize performance for share points used only by Windows clients. Opportunistic locking is disabled by default because it is not compatible with NFS or AFP. Opportunistic locks, which allow clients to do more dynamic client-side caching, are only enforced by SMB.
- Strict locking enables lock checking every time files are accessed for either read or write operations. It is useful for applications that do not manage locking. Strict locking is enabled by default.

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 does not support name/password authentication. It relies on client IP addresses to authenticate users and on client enforcement of privileges—not a secure approach in most networks. Therefore use NFS only if you are on a local area network (LAN) with trusted client computers or if you are 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.

FTP is generally considered to be an insecure protocol, since user names and passwords are distributed across the Internet in clear text. Because of the security issues associated with FTP authentication, most FTP servers are used as Internet file distribution servers for anonymous FTP users. Starting with Mac OS X Server version 10.3, however, FTP supports Kerberos authentication, which offers a secure means for authenticating to an FTP 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 the server administrator to allow uploads from anonymous FTP users, and then only into a specific share point.

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, LPR/LPD), Windows (SMB/CIFS), and UNIX (LPR/LPD) 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 direct-connect USB printers with Mac OS X version 10.2 and later clients
- 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 print quotas to limit printer usage on a per-user or per-printer basis

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.

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 is 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, and 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 Secure Sockets Layer (SSL) support enables secure encryption and authentication for ecommerce websites and confidential materials. An easy-to-use digital certificate provides non-forgable proof of your website identity.

Mac OS X Server offers extensive support for dynamic websites:

- Web service supports Java Servlets, JavaServer Pages, MySQL, PHP, Perl, and UNIX and Mac CGI scripts.
- Mac OS X Server includes a JBoss server and high-level administration tools for configuring and managing it. See "Application Server Support" on page 43 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.

Mac OS X Server also supports 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 includes these network services for helping you manage Internet communications on your TCP/IP network:

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

The network services administration guide provides complete information about all these services except IP failover, which is described in the command-line administration guide.

DHCP

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. 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 are not needed they are available for use by other clients.

As you learned in “Search Policies” on page 31, you can automate the directory services setup of Mac OS X clients using your DHCP server’s Option 95 support. This recommended 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 host name (such as `server.apple.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.

You will use DNS if you use SMTP mail service or if you want to create subdomains within your primary domain. You will also use DNS if you are hosting multiple websites. 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.

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

- Enable zone transfers and recursion
- Specify interfaces on which to listen for DNS requests
- Maintain blocked host lists
- Work with log files
- Manage zones and their records

Firewall

Firewall service protects your server and the content you store on it 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

Network Address Translation (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, and 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.

Mac OS X Server's Server Admin application helps you administer NAT. You can also use the command-line tool `ipfw` or the Firewall service to configure the NAT translations specific to your network.

VPN

You can set up a Virtual Private Network (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.

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 and IPsec.

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 that is 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 are interested in J2EE programming, see "Java Enterprise Applications," 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, if you wish.

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. 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/.

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 to authenticate users.
- 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, file and printer sharing, and Open Directory authentication. You can also host Windows user home directories if you set up a Windows PDC on Mac OS X Server.

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 as well as PDC support for Windows users.
- The user management guide describes how to configure Windows options for individual users.

High Availability

Mac OS X Server features that promote high availability include:

- Open Directory Apple LDAP replication (see the Open Directory administration guide)
- IP failover (see the command-line administration guide)
- Automatic restart after hardware or software failures
- Disk space monitoring (see the command-line administration guide for information about log-rolling scripts and the `diskspacemonitor` tool)
- Software RAID (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 47)

Server Administration

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

From initial server setup to service configuration and day-to-day server management, administrators can use graphical applications or command-line tools available on the server or on a Mac OS X computer onto which you've installed the applications that come with the server.

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

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 are 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 49.
- 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, set up as described in "Using a Non-Mac OS X Computer for Administration" on page 49.

Using the Administration Tools

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

Application or tool	Use to	For more information, see
Installer	Install server software or upgrade it from version 10.1 or 10.2	page 50
Server Assistant	Set up a version 10.3 server for the first time	page 50

Application or tool	Use to	For more information, see
Directory Access	Configure access to data in directories, define a search policy, and enable service discovery protocols	page 50
Workgroup Manager	Administer user, group, and computer accounts; manage share points; and administer client management for Mac OS X users	page 51
Server Admin	Configure and monitor services Set up and manage QuickTime media streaming	page 55 page 59
System image tools	Manage NetBoot and Network Install disk images	page 58
Server Monitor	Monitor Xserve hardware	page 58
Apple Remote Desktop	Monitor and control other Macintosh computers	page 59
Command-line tools	Administer a server using a UNIX command shell	page 60
Macintosh Manager	Administer client management for Mac OS 9 users	page 60

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 local server using the graphical administration applications (they're in `/Applications/Server/`), log in to the server as an administrator and open them. To administer a remote server, open the applications on an administrator computer—any Mac OS X Server or Mac OS X version 10.3 or later computer onto which they've been installed.

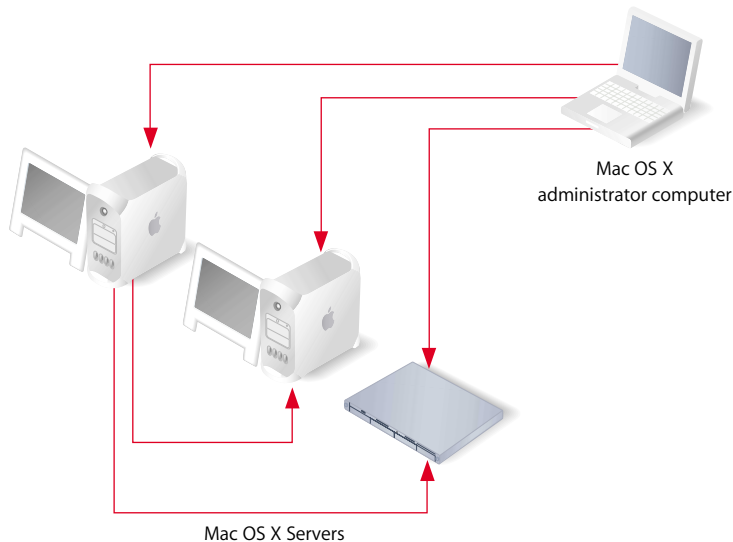
You can run command-line tools from the Terminal Application (it's in `/Applications/Utilities/`) on any Mac OS X Server or Mac OS X computer. You can also run command-line tools from a UNIX workstation.

Setting Up an Administrator Computer

An administrator computer is a computer with Mac OS X or Mac OS X Server version 10.3 or later that you use to manage remote servers.

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

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



To make a computer with Mac OS X into an administrator computer:

- 1 Make sure the Mac OS X computer has Mac OS X version 10.3 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 disc.
- 3 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 install discs that came with your server. The Installer lets you perform:

- A clean installation of Mac OS X Server, which installs version 10.3 after erasing and formatting a target disk
- An upgrade installation, which upgrades version 10.1 or 10.2 servers to version 10.3 without erasing any data

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 initial server setup and remote installations.

This flexible application supports many setup scenarios:

- Local and remote setups
- Remote server installations
- Single and multiserver setups
- Preparing data for automated server setups

See Chapter 7, “Initial Server Setup,” for information about how to use Server Assistant.

Directory Access

Directory Access is the primary application for setting up a local or remote Mac OS X computer's connections with Open Directory directories 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/`.

The Directory Access application that comes with version 10.3 can be used to configure both version 10.2 and version 10.3 computers.

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

Workgroup Manager

You use Workgroup Manager to administer user, group, and computer accounts, work with managed client preferences for Mac OS X users, manage share points, 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.
- 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.

Opening and Authenticating in Workgroup Manager

Workgroup Manager is installed in `/Applications/Server/`. To open Workgroup Manager, click the Workgroup Manager icon in the Dock or in the toolbar of Server Admin:

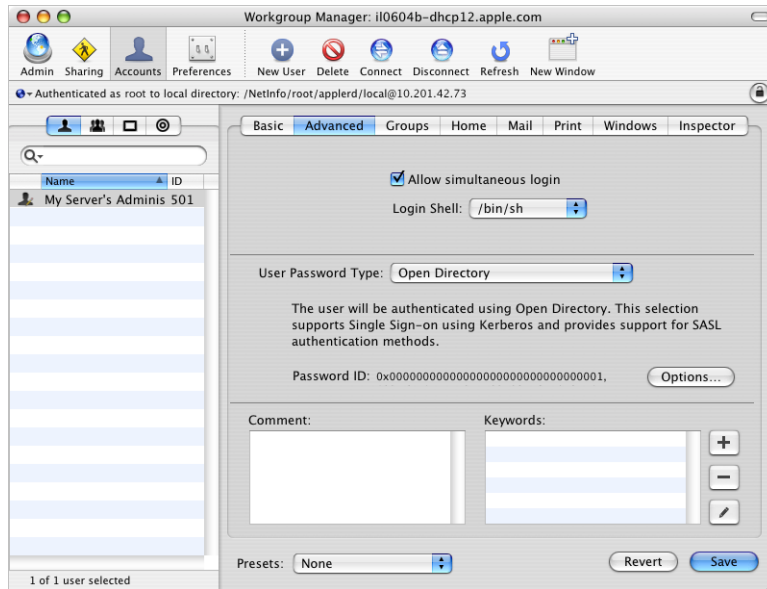
- To open Workgroup Manager on the server you are using without authenticating, choose View Directories from the Server menu when you see the Workgroup Manager login dialog. You have read-only access to information displayed in Workgroup Manager. To make changes, click the lock icon to authenticate as an administrator. This approach is most useful when you are 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, 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 will 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.

Using Workgroup Manager

After login, the user account window appears, showing a list of user accounts. Initially, the accounts listed are those stored in the last directory node of the server's search path. Here is how to get started with the major tasks you perform with this application:

- To administer user, group, or computer accounts, click the Accounts icon in the toolbar. Click the user, group, or computer button on the left side of the window to list the accounts that currently exist in the directory or directories you are working with.



To specify the directories that store accounts you want to work with, click the small globe icon above the accounts list. You can list accounts in directories in the search path of the server you are connected to.

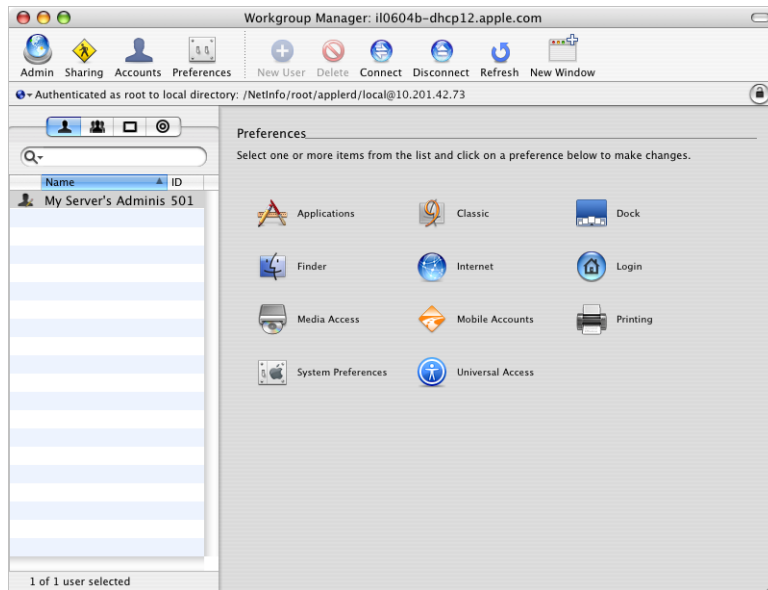
To work with accounts in different directories at the same time or to work with different views of accounts in a particular directory, open multiple Workgroup Manager windows by clicking the New Window icon in the toolbar.

To filter the account list displayed, use the pop-up search list above the accounts list.

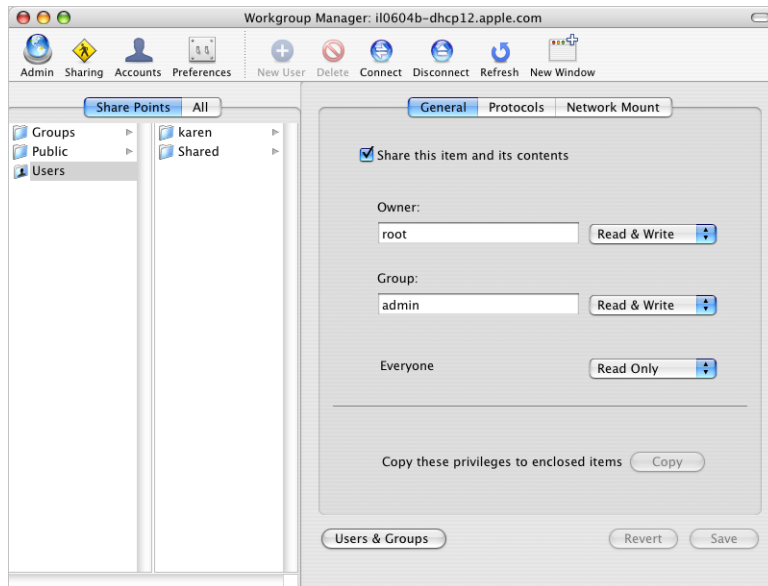
To refresh the accounts list, click the Refresh button in the toolbar.

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.

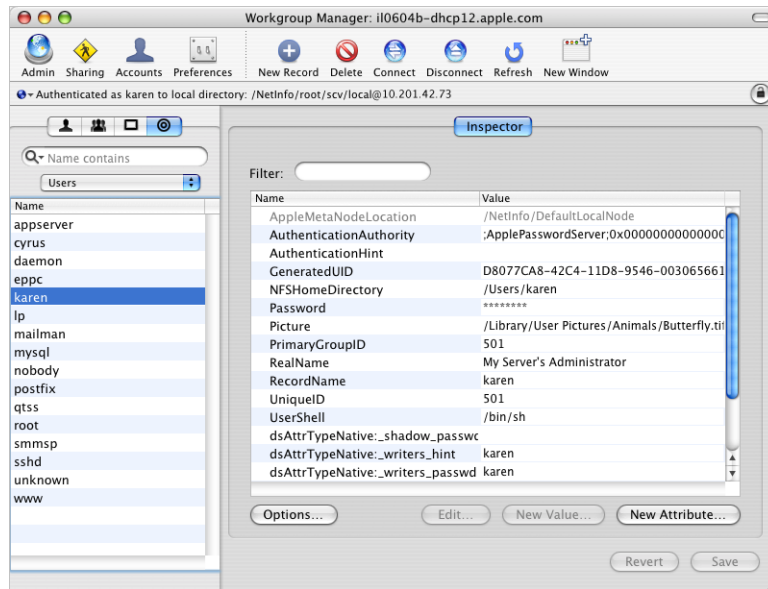
- To work with managed client preferences for user, group, or computer accounts, click the Preferences icon in the toolbar.



- To work with share points, click the Sharing icon in the toolbar.



- To display the Inspector, choose Workgroup Manager > Preferences. Enable the setting that shows the Inspector and click OK. Select the “All records” button (which looks like a bull’s-eye) to access the Inspector.



- To control the Workgroup Manager environment, you have several options. To control the way Workgroup Manager lists users and groups, whether it should use SSL transactions, and other behaviors, choose Workgroup Manager > Preferences. To customize the toolbar, choose View > Customize Toolbar.
- To import or export user and group accounts, choose Server > Import or Server > Export, respectively.
- 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.
- 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.

Opening and Authenticating in Server Admin

Server Admin is installed in `/Applications/Server/`. To open Server Admin, click the Server Admin icon in the Dock or click 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, or click Browse to choose from a list of servers. Specify the user name and password for an administrator, then click Connect.

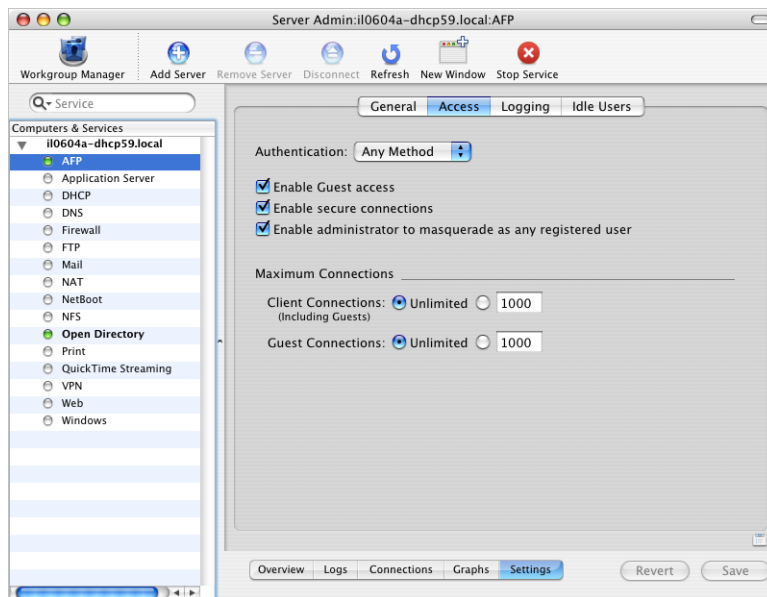
To manage multiple servers from one Server Admin window, simply click Add Server in the toolbar after opening Server Admin, and log in to the server. The next time you open Server Admin, any server you have added appears in the list.

You can connect to a version 10.2 server using Server Admin. In this case, you can't make changes to its services, but you can monitor its status.

Using Server Admin

Here are general tips for using Server Admin. Detailed instructions for using it to manage individual services appear in the service-specific administration guides.

- The servers you can administer after opening Server Admin appear in the Computers & Services list.



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 have added is displayed in the list.

To limit the items that appear in the Computers & Services list, use the pop-up menu above the list to select the items you want to see 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 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 remove a server from the Computers & Services list, select the server, choose Server > Disconnect, and choose Server > Remove Server.

- 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 is not 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 any remote server you want to manage using Server Admin to ensure that the remote server is a valid server. Before enabling this option, use the instructions in the web technologies 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/`.

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

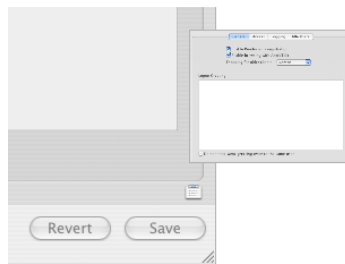
- To work with general server settings, select a server in the Computers & Services list.
 - Click Overview to view information about the server.
 - Click Logs to view the system log, software update log, and others.
 - Click System to view information about ports and volumes the server uses.
 - Click Graphs to view a graphical history of server activity.
 - Click Update to use Software Update to update the server’s software.
 - Click Settings to edit such values as the server’s computer name and its serial number and to enable SNMP, NTP, and Macintosh Manager services.

- To work with a particular service on a server, click the service in the list under the server in the Computers & Services list. You can view information about a service (logs, graphs, and so forth) and manage its settings. Administration guides for individual services provide detailed instructions.

To start or stop a service, select it in the Computers & Services list, 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.

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.

- 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 reenable changes, choose View > Unlock View and reauthenticate using the name and password used to log in to the system.

- To retrieve online information, use the Help menu. It provides help for administration tasks you accomplish using Server Admin as well as other Mac OS X Server topics.
- To control the Server Admin environment, you have several options.

To control the appearance of the Server Admin lists, autorefresh rates, and other behaviors, choose Server Admin > Preferences.

To customize the toolbar, choose View > Customize Toolbar.

To add a button to the toolbar that is a shortcut to a particular Server Admin view, go to the pane you want then choose View > Add Shortcut to View.

- To access Workgroup Manager, click the Workgroup Manager icon in the toolbar.

System Image Management

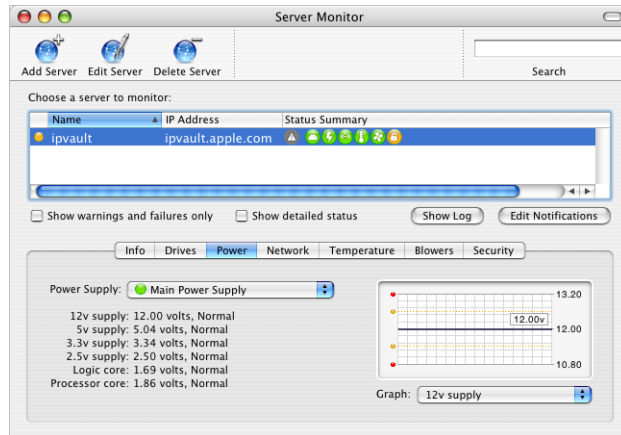
To create and manage NetBoot and Network Install images, you use several applications:

- NetBoot Desktop Admin lets you modify Mac OS 9 images.
- Network Image Utility lets you create and modify Mac OS X images, including Network Install images that re-create an existing volume or partition.
- Server Admin lets you organize NetBoot images and work with filters that control the visibility of images from client computers.
- PackageMaker is used to create Network Install packages.

The system image administration guide provides instructions for using all these applications.

Server Monitor

You use Server Monitor to monitor 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/`. Use the application to monitor local or remote Xserve servers:

- 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, the times Server Monitor attempted to contact the server, and whether a connection was successful. The log also shows server status changes. (The logs do not include system activity on the server.)

Media Streaming Management

The QuickTime streaming services administration guide provides instructions for administering QuickTime streaming services.

To administer QuickTime streaming services, you use Server Admin.

Apple Remote Desktop

Apple Remote Desktop, which you can optionally purchase, simplifies changing the settings of multiple client computers. From one administrator computer in a computer lab, for example, you can easily set up all of the clients to use a NetBoot image at startup.

For more information on Apple Remote Desktop, go to www.apple.com/remotedesktop/.

Command-Line Tools

If you are 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.

Macintosh Manager

You use Macintosh Manager to administer client management for Mac OS 9 client computers. You can use it locally (at the server) or remotely (from a Mac OS 9 or Mac OS X computer on the same network as your Mac OS X Server).

Open Macintosh Manager by clicking its icon in the Dock. Log in using a server, Macintosh Manager, or workgroup administrator user name and password. As a server administrator, you automatically have global administrator privileges for Macintosh Manager.

Macintosh Manager support is also provided by Server Admin.

See the user management guide for information about using Macintosh Manager.

Working With Version 10.2 Servers From Version 10.3 Servers

When you're logged in to Mac OS X Server version 10.3, you can administer a version 10.2 server:

- Server Admin, located in /Applications/Server/, lets you monitor the status of a version 10.2 server.
- Directory Access, located in /Applications/Utilities/, can be used to configure version 10.2 servers and computers.
- Workgroup Manager, located in /Applications/Server/, lets you manage version 10.2 accounts, preferences, and sharing settings.

Part II: Installation and Initial Setup

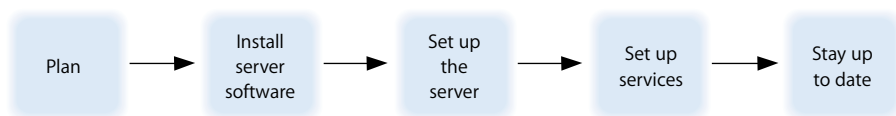


The chapters in this part of this guide tell you how to install server software and set up a server for the first time.

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 familiarize yourself 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 10.3 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 73 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 suite your needs. Appendix B, "Setup Example," on page 119 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 10.3 software already installed. Nonetheless, there are several times you need to install server software, as when you want to upgrade from a version 10.1 or 10.2 server, change a computer with Mac OS X into a server, or completely refresh your server environment.

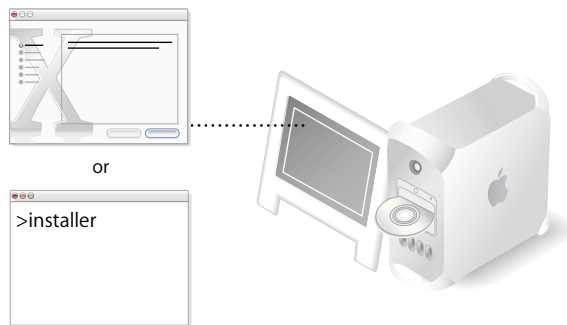
You can install server software:

- 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 79 provides detailed instructions for all the installation options, which are summarized in the following sections.

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 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 82 for instructions.

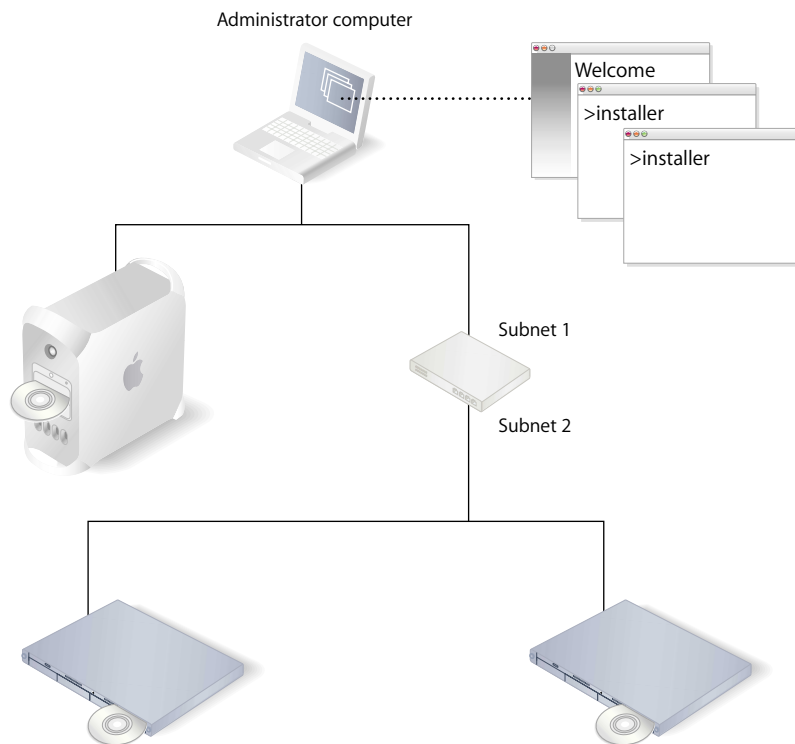
If you prefer using the command line, start the Terminal application from the Installer menu and follow the instructions in “Using the `installer` Command-Line Tool to Install Server Software” on page 85.

Remote Installation From the Server Install Discs

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

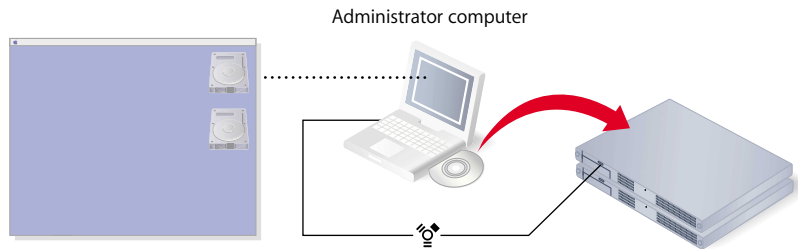
An administrator computer is a version 10.3 Mac OS X Server or version 10.3 Mac OS X computer onto which you've installed server management software. "Setting Up an Administrator Computer" on page 49 tells you how to set up a Mac OS X administrator computer. The target server can be on the same subnet 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 83 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 85. 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 that is equipped with one. 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 automate installation by using an installation image that resides on disk rather than on the installation discs.

See the system image administration guide for instructions on creating and deploying network install images created from a CD, a DVD, or an existing volume or partition.

Initial Server Setup

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

During server setup, basic server characteristics are established. For example:

- The language to use for server administration and the computer keyboard layout are defined.
- An administrator user is defined and the user's home directory is created.
- 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 Apple LDAP domain.
- The server's host, computer, and Rendezvous names are set.
- The network interfaces (ports) are configured.
- 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.

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.

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.

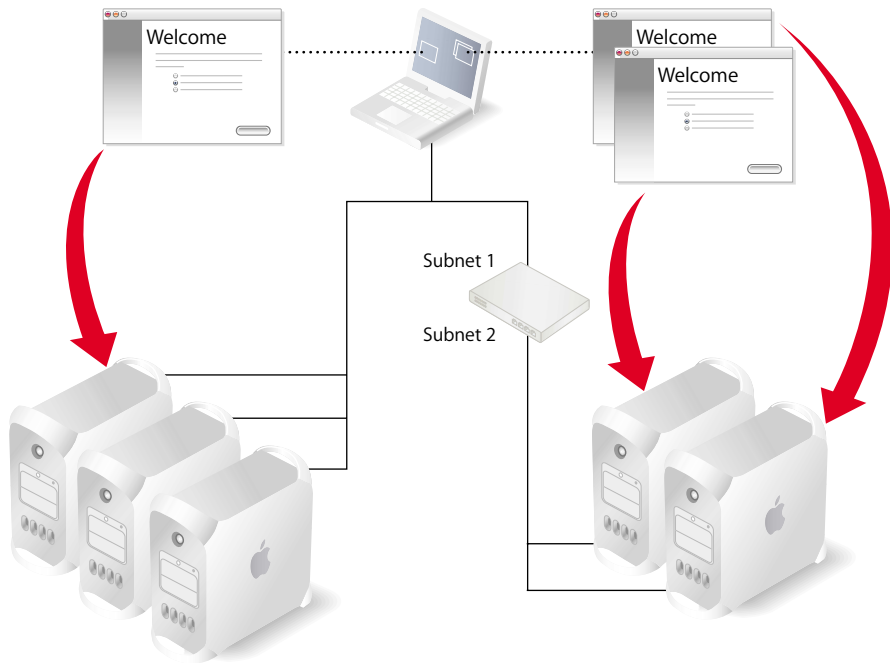
Chapter 7, "Initial Server Setup," on page 89 provides detailed instructions for all the server setup options, summarized next.

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, and 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 96 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 97 for instructions.

When multiple remote servers can use the same setup data, you can supply the data, and then initiate setup of all the servers at once, using a batch approach. This technique, shown on the left side of the picture below, 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 98 for instructions.



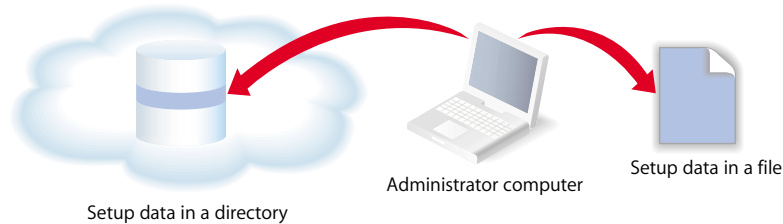
When you want to customize the setup of individual servers, you can manage each setup individually from a different Server Assistant window. This approach is shown on the right side of the picture above. See “Setting Up Multiple Remote Servers Interactively One at a Time” on page 99 for instructions.

Although the picture above 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 scenarios can be used to set up computers on 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 automated server setup. This approach also provides a way to preserve setup data so it can be reused should you want or need to reinstall server software.

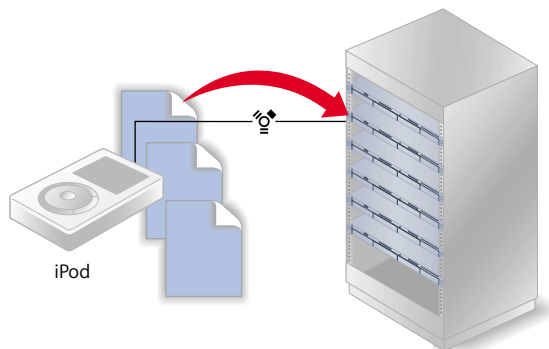
Use Server Assistant to specify setup data, then save the data in a file or in a directory.



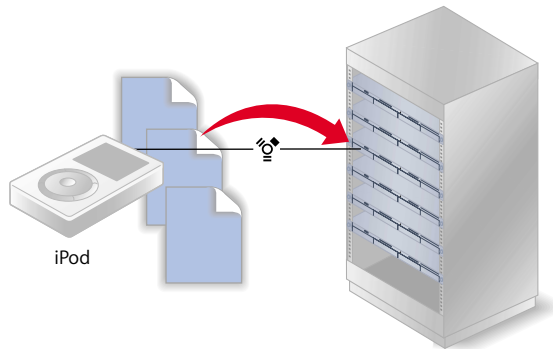
Using Setup Data Stored in a File

When you place a setup file on a volume (CD, 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 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`. Alternatively, a server's IP address can be used as an identifier. A server with the IP address 10.0.0.4 would use `/Volumes/MyIPod/Auto Server Setup/10.0.0.4.plist`.

You could also use a single file, which you would 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.

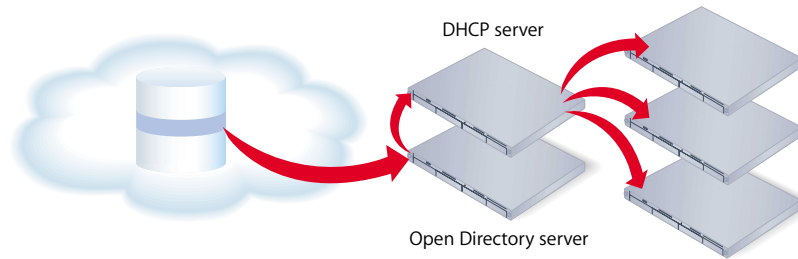
See "Setting Up Servers Automatically Using Data Saved in a File" on page 101 for instructions.

Using Setup Data Stored in a Directory

A target server can also set itself up using setup data you've stored in a directory the server is configured to access. In fact, a server looks for setup data in any directory it's configured to use before consulting locally mounted file systems for setup data.

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 103 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 a dongle, then plug the dongle into each server that needs the passphrase. A server with the IP address 10.0.0.4 would use `/Volumes/MyIPod/SA_Keys/10.0.0.4.pass`.

Setting Up Services

After initial server setup is complete, you can:

- Finish migrating data from a previous server, if you still need to do so.
- Set up individual services you want to provide, using the server administration tools described in Chapter 3, “Server Administration,” on page 47.

Keeping Current

As update releases of Mac OS X Server become available, use the Software Update pane of System Preferences, the `softwareupdate` command-line tool, or the Update button in Server Admin to stay current.

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 are 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 fulfill.

Use this chapter to stimulate your thinking. It does not 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, is not necessarily a linear process. The sections in this chapter had to be in some particular order, but the order does not imply a mandatory sequence. Different sections in this chapter present suggestions that could be implemented simultaneously or iteratively.

Set 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 likely to manage its services and administer 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 that they better 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, to do so. 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 111.

Identify 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 10.3?
- How many new Mac OS X Server computers will you need to set up?

Determine 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 existing directories and Kerberos authentication hosted on non-Apple servers to setting up replicated Apple LDAP directories on servers distributed throughout the world. More than probably any other service, 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 will 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, and other factors, and DHCP services need to be available. See the system image 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

When you are using computers with Mac OS X Server versions earlier than 10.3, consider updating them to version 10.3.

When you are using Mac OS X Server version 10.1 or 10.2, you can often simply upgrade your server during the installation process. This approach is simple, because it automatically preserves the data and settings you've been using.

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

- A version 10.1 or 10.2 server's hard disk needs reformatting, or does not meet the minimum version 10.3 hardware requirements (see "Understanding System Requirements for Installing Mac OS X Server" on page 79).
- You want to move data and settings you've been using on a version 10.1 or 10.2 server to a different server.
- The server version you've been using is earlier than version 10.1.

Read the migration guide to understand what data and service settings can be preserved and reused on version 10.3. The migration guide provides instructions for both reusing existing server hardware—called migrating in place—and migrating from one computer to another.

Define 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 involves primarily 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 to offer Windows computer users of Mac OS X Server. The Windows services administration guide tells you what's available.

Define 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 very few times a server 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?

Define 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 will 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. 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.

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 is 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 119 illustrates the steps you might take to set up the directory and network infrastructure of Mac OS X Server in a small business scenario.

Make 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 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.

Determine the Installation and Setup Strategy to Use

Review the installation and server setup options in Chapter 4, “Installation and Setup Overview,” on page 63.

Select the option or options you want to use, then address any prerequisites for installation on page 80 and for initial server setup on page 90.

Collect and Organize Information

For each server you set up, fill out the worksheet on page 111. It captures all the data you’ll need to quickly move through any of the installation and setup options you decide to use.

You can upgrade to Mac OS X Server version 10.3 from version 10.1 or 10.2 or you can perform a clean installation of Mac OS X Server version 10.3.

Review the system requirements below and “Information You Need” on page 80 before using the detailed installation instructions, which you’ll find as indicated in the following table.

Instructions for	Are on
Using the Installer application to install locally from the install discs	page 82
Using Server Assistant to install remotely from the install discs	page 83
Installing server software on a computer with Mac OS X version 10.3 preinstalled	page 85
Automating server software installation	page 85
Using the <code>installer</code> command-line tool	page 85
Installing optional server software	page 88

Understanding System Requirements for Installing Mac OS X Server

You can install Mac OS X Server version 10.3 on any of these computers:

- Xserve
- G5
- Power Mac G4
- Macintosh Server G4
- Macintosh Server G3
- Power Mac G3
- iMac
- eMac

The computer must have:

- 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 built-in USB port.

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 49 describes how to set one up.

Information You Need

Use Appendix A, “Mac OS X Server Worksheet,” on page 111 to record information for each server you want to install. The information below provides some supplemental explanations for items on the worksheet.

Upgrading From Version 10.1 or 10.2

If you are using Mac OS X Server version 10.1 or 10.2, you can upgrade your server to version 10.3. The upgrade process installs and sets up Mac OS X Server version 10.3 while automatically preserving existing data and service settings.

You can upgrade your version 10.1 or 10.2 server to version 10.3 if:

- You don’t need to reformat the current server’s hard drive.
- Your current server hardware meets the minimum system requirements for installing version 10.3. See “Understanding System Requirements for Installing Mac OS X Server” on page 79 for details.

When you upgrade a version 10.1 or 10.2 server, the following are automatically upgraded if they have been set up:

- DNS settings
- Firewall setting
- IP failover settings
- Mail settings and database
- MySQL settings and database
- QTSS playlists, admin, and core server settings
- Web service settings and files
- Directory services settings, including password services
- Directory Access settings, including search policy and plug-in configurations
- Home directories
- Share points
- AFP settings
- SMB settings
- FTP settings
- Macintosh Manager data

- NetBoot settings and images
- DHCP settings

Preparing Disks for Installing Mac OS X Server

When you perform a clean installation, the target disk or partition is erased and there are several disk-preparation tasks to perform:

- Preserve any user data you want to save on the target disk or partition. See the migration guide for information on migrating data and settings.
- 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. Case-sensitive HFS+ format is useful if case-sensitive file names are important, as when you need to support legacy UNIX applications on Mac OS X Server. All case-sensitive disks are also journaled.
- Optionally, partition the target disk and set up one of the partitions as the destination for server software. The minimum recommended size for an installation partition is 4 GB.

Important: Don't store data on the hard disk or hard disk partition where the operating system is installed. With this approach, you will not risk losing data should you need to reinstall or upgrade system software.

- Optionally configure the target disk for RAID mirroring, which creates a backup disk that is used automatically if the primary disk isn't available.

You can format a disk or partition as Mac OS Extended (Journaled) from the Installer application and as Mac OS Extended from the Disk Utility application. 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, DNS 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.

Installing Server Software Interactively From the Install Discs

You can use the install disks to install server software interactively:

- On a local server
- On a remote server
- 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 will 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 When Installer opens, if you want to perform a clean installation, optionally use the Installer 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 data on the hard disk or hard disk partition where the operating system is installed. With this approach, you will not risk losing data should you need to reinstall or upgrade system software.

- 5 Proceed through the Installer's panes by following the onscreen instructions.
- 6 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 are doing a clean installation, you can choose Installer > Open Disk Utility or Installer > 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 and format" to format the disk in Mac OS Extended (Journaled) format; then click OK.

If the volume you selected contains Mac OS X Server version 10.1 or 10.2 and you want to upgrade, click Options and select "Don't erase." Click OK.

- 7 During installation, progress information is displayed. Insert the next installation disc when prompted.

After installation is complete, the server restarts automatically and you can perform initial server setup. Chapter 7, "Initial Server Setup," on page 89 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 will be performing a clean installation rather than upgrading from Mac OS X Server version 10.2, 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 data on the hard disk or hard disk partition where the operating system is installed. With this approach, you will not risk losing data should you need to reinstall or upgrade system software.

- 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. 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 are 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 Select a Destination 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 Mac OS X Server version 10.1 or 10.2 and you want to upgrade, click Options and select “Don’t erase.” Otherwise, you can select “Erase and format” to format the disk in Mac OS Extended (Journaled) format. Click OK.

During installation, progress information is displayed. Insert the next installation disc when 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 server restarts automatically and you can perform initial server setup. Chapter 7, “Initial Server Setup,” on page 89 describes how.

Installing Server Software on a Computer With Mac OS X Version 10.3 Preinstalled

Follow these instructions to install server software on a computer that came with Mac OS X version 10.3 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 the first install disc.
- 2 Insert the second install disc, then 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.

See the system image administration guide for instructions on creating and deploying Network Install images created from a CD, a DVD, or an existing volume or partition.

After booting an Xserve computer from a NetBoot installation image in NetBoot mode, you can use Server Assistant to set up the server remotely. See “Setting Up a Remote Server Interactively” on page 97 for instructions.

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 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.

- 2 Before starting the installation, identify the target-server volume onto which you want to install the server software.

To list the volumes available for server software installation, type:

```
/usr/sbin/installer -volinfo  
-pkg /Volumes/Mac\ OS\ X\ Server\ Install\ Disk\ 1/  
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
```

- 3 If the target volume has Mac OS X Server version 10.1 or 10.2 installed, when you run `installer` it will upgrade the server to version 10.3 and preserve user files.

If you are 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 `diskutil`.

Important: Don’t store data on the hard disk or hard disk partition where the operating system is installed. With this approach, you will not risk losing data should you need to reinstall or upgrade system software.

- 4 If you are installing a local server, when Server Assistant opens choose `Installer > Open Terminal` to open the Terminal application.

If you are 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 all computers on the local subnet:

```
cd /  
/system/library/serversetup/sa_srchr 224.0.0.1  
mycomputer.example.com#PowerMac4,4#<ip address>#<mac address>  
#Mac OS X Server 10.3#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 the information.

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

- 6 Install the operating system on a volume from the list generated in step 2. For example, to use Mount 01 in the example in step 2, type:

```
/usr/sbin/installer -verboseR -lang English  
-pkg /Volumes/Mac\ OS\ X\ Server\ Install\ Disk\ 1/  
System/Installation/Packages/OSInstall.mpkg  
-target "/Volumes/Mount 01"
```

- 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
```

- 9 To use an additional install disc to complete the installation, type the `sa_srchr` command to locate the server that's waiting. For <ip address>, specify the address you used in step 4:

```
/system/library/serversetup/sa_srchr <ip address>
```

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

```
mycomputer.example.com#PowerMac4,4#<ip address>#<mac address>  
#Mac OS X Server 10.3#InstallInProgress#2.0#2080
```

- 11 Server Assistant opens automatically when installation is complete.

Installing Optional Server Software

To install Macintosh Manager, insert the Mac OS X Server Administration Tools disc and read the installation information provided on the disc.

To install NetBoot for Mac OS 9, download a copy of the “NetBoot for Mac OS 9” CD image from www.info.apple.com.

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

Review “Information You Need” on page 90 before using the detailed installation instructions, which you’ll find as indicated in the following table.

For information about	See instructions for	On
Setting up servers interactively	Using interactive server setup	page 96
	Setting up a local server interactively	page 96
	Postponing local server setups following installation	page 97
	Setting up a remote server interactively	page 97
	Setting up multiple remote servers interactively in a batch	page 98
	Setting up multiple remote servers interactively one at a time	page 99
Setting up servers automatically	Using automatic server setup	page 100
	Setting up servers automatically using data saved in a file	page 101
	Setting up servers automatically using data saved in a directory	page 103
Monitoring and troubleshooting	Determining the status of setups	page 106
What to do after initial setup	Setting up basic services	page 106

Information You Need

See Appendix A, “Mac OS X Server Worksheet,” on page 111 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 are upgrading from Mac OS X Server version 10.1 or 10.2, Server Assistant displays the version 10.1 or 10.2 server settings, but you can change them. Use the worksheet to record settings you want the version 10.3 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 A server first 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 built-in hardware serial number, its host name, or “generic”.
- 2 Next the server 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 built-in hardware serial number, its host name, or `generic.plist`.

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/*/SA_Keys/<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 built-in hardware serial number, its host name, or `generic.pass`, in that order.

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 is not found in a directory the server is configured to use. See “Using Setup Data Saved in a Directory” on page 92 for information on how a server detects and uses directory data to set itself up.
- The setup file resides 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, 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-host-name-of-server>.plist`. For example, `myserver.plist`.

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

For example, `ABCD1234.plist`.

`<full-host-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).

- 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/*/SA_Keys/<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-host-name-of-server>.pass`. For example, `myserver.pass`.

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

For example, `ABCD1234.pass`.

`<full-host-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 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 is not erased when you reinstall the server. The setup files are automatically detected and reused after each installation.

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 are 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. Apple OpenLDAP directories have built-in support for stored setup data. If you want to store setup data in a different 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 Rendezvous name) 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-host-name-of-server>`. For example, myserver.

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

`<full-host-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).

- 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/*/SA_Keys/<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-host-name-of-server>.pass. For example, myserver.pass.

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

<full-host-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).

Keeping Backup Copies of Saved Setup Data

Saved setup data is not 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 10.1 or 10.2
- **Standalone Server**, used to set up only a local NetInfo directory domain on the server
- **Open Directory Master**, used to set up an Apple LDAP domain 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 are 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.

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 with multiple directory domains and specify a search policy—the order in which the server should search through the domains. Server Admin lets you set up replication 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 are upgrading, the best choice is usually “No change,” and if you are 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 you are setting up a server that you are upgrading from version 10.1 or 10.2 to version 10.3, 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 are 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 *Migrating to Mac OS X Server Version 10.3* for information on how to continue using existing directory data when you change directory service settings.

When you use the “No change” option, Open Directory authentication is set up if Password Server was not being used on the server. 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 are 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 is a local domain, the data stored in it is accessible only to the server you are 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 to Host an Open Directory Master

When you want a server you are setting up to host an Apple LDAP directory for use by itself and other computers, choose the directory usage option called Open Directory Master in Server Assistant. This option:

- Sets up the Apple LDAP domain on the server
- Turns on Open Directory authentication for validating all users defined in the local NetInfo domain and the shared Apple LDAP domain
- Sets up a Kerberos KDC on the server
- 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 replication for the Apple LDAP directory, 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 are 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 receive the identity of a shared LDAP or NetInfo directory server from the DHCP server that provides its IP address. The LDAP directory can be an Apple LDAP directory or another vendor's LDAP directory.
- **Apple LDAP Directory**, 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 domain name of the server.
- **NetInfo Directory**, 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 System**, which is the selection to make when you want to use a directory option different from the three above. 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 use a NetInfo directory on Mac OS X Server version 10.0 and later or an LDAP directory on version 10.2. However, you may not be able to take advantage of some version 10.3 features:

- Windows PDC service requires a version 10.3 LDAP master directory.
- VPN needs version 10.3 if you want to use MS-CHAP2 authentication.
- Password Server on version 10.2 can't be replicated.
- Kerberos configuration is much more complex on version 10.2.

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 111. Supplemental information appears in "Information You Need" on page 90.
- 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 reuse (a saved setup file or saved directory record), click Save As. All the settings you specified except the server serial number are saved. When you use setup data saved in a file or directory to set up a server, you need to use Server Admin to enter the serial number after the server setup is complete.

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.

- 7 To initiate server setup, click Apply.

When server setup is complete, click Restart. Now you can log in as the 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 111. Supplemental information appears in "Information You Need" on page 90.
- 2 Make sure the target server is running.
- 3 On an administrator computer, open Server Assistant. It's located in /Applications/Server/.
- 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, then click Continue.
- 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 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 reuse (a setup file or directory record), click Save As. All the settings you specified except the server serial number are saved. When you use setup data saved in a file or directory to set up a server, you need to use Server Admin to enter the serial number after the server setup is complete.

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 To initiate server setup, click Apply.

When server setup is complete, click Continue. The target server restarts automatically and you can log in as the 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 network identities (host name, computer name, and Rendezvous name) and server software serial number
- 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 111. Supplemental information appears in “Information You Need” on page 90.
- 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/.
- 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 servers 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, then click Continue.
- 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 Enter the setup data as you move through the Assistant's panes, following the onscreen instructions. When prompted, enter the 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 reuse (a setup file or directory record), click Save As. All the settings you specified except the server serial number are saved. When you use setup data saved in a file or directory to set up a server, you need to use Server Admin to enter the serial number after the server setup is complete.

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 To initiate server setup, click Apply.

When server setup is complete, click Continue. The target servers restart automatically and you can log in as the 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 111. Supplemental information appears in "Information You Need" on page 90.
- 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/.
- 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, then click Continue.
- 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 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 reuse (a setup file or directory record), click Save As. All the settings you specified except the server serial number are saved. When you use setup data saved in a file or directory to set up a server, you need to use Server Admin to enter the serial number after the server setup is complete.
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 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 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 are not available yet
- 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. Target servers on which Mac OS X Server version 10.3 software has been installed automatically detect the presence of the saved setup information and use it to set themselves up.

You can create a generic saved setup, which lets you use it to set up any server, such as a server that is on order or fifty Xserves that can be identically configured, at least initially. Alternatively, you can save setup data that is specifically tailored for a particular server.

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 111. Supplemental information appears in “Information You Need” on page 90.
- 2 On an administrator computer, open Server Assistant. It’s located in /Applications/Server/.
- 3 In the Welcome pane, select “Save setup information in a file or directory record” to work in offline mode, which does not require a server connection.
- 4 In the Language pane, specify the language you want to use to administer the target server or servers, then click Continue.
- 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, make sure that you do not specify network names (host name, computer name, and Rendezvous name) and that the network interface (port) is set to be configured “Using DHCP” or “Using BootP.”

- 6 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.” All the settings you specified except the server serial number are saved. Later in this process you’ll use Server Admin to enter the serial number after a target server has been set up.
- 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-host-name-of-server>.plist. For example, myserver.plist.
 - <built-in-hardware-serial-number-of-server>.plist (first 8 characters only). For example, ABCD1234.plist.
 - <full-host-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, CD, FireWire drive, USB drive, or other device plugged into the server.

For example, if you have an iPod named AdminiPod, the path consulted 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-host-name-of-server>.pass. For example, myserver.pass.
 - <built-in-hardware-serial-number-of-server>.pass (first 8 characters only). For example, ABCD1234.pass.
 - <full-host-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).

Place the passphrase file on a volume mounted locally on the target server in `/Volumes/*/SA_Keys/<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 pane, choose File > Supply Passphrase. In the dialog, enter the target server's IP address, password, and the passphrase.

Click Send.

- 17 Use Server Assistant to enter the server software serial number for the target server.

See the command-line administration guide for a description of the layout of a saved setup file.

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 are 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 111. Supplemental information appears in "Information You Need" on page 90.
- 3 On an administrator computer, open Server Assistant. It's located in `/Applications/Server/`.
- 4 In the Welcome pane, select "Save setup information in a file or directory record" to work in offline mode, which does not require a server connection.
- 5 In the Language pane, specify the language you want to use to administer the target server or servers, then click Continue.
- 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 are creating generic setup data, make sure that you do not specify network names (host name, computer name, and Rendezvous name) and that the network interface (port) is set to be configured "Using DHCP" or "Using BootP".

- 7 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." All the settings you specified except the server serial number are saved. Later in this process you'll use Server Admin to enter the serial number after a target server has been set up.
- 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 Navigate to /AutoServerSetup/ in 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 domain administrator.

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-host-name-of-server>. For example, myserver.

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

<full-host-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 host names.

See “Define Server Setup Infrastructure Requirements” on page 77 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-host-name-of-server>.pass. For example, myserver.pass.

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

<full-host-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).

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

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

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

Click `Send`.

- 18 Use Server Assistant to enter the server software serial number for the target server.

See the Open Directory administration guide for a description of the schema of setup data saved in a directory.

Determining the Status of Setups

There are several ways to view setup status information in Server Assistant:

- After you've interactively initiated the setup of one or more servers, progress information is displayed. If setup is successful, a target server reboots when setup is complete. If setup is not successful, Server Assistant displays error information.
- You can use the Destination pane available during interactive remote server setups to assess whether any setup you have initiated needs your attention. If a server has an error icon, select the server and review the error information displayed. For example, you can determine whether a saved setup file could not be used by a particular server because the setup data is encrypted and a passphrase could not be found.

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, use File > Load Server List.

- When a server setup fails, an error log is created in `/System/Library/ServerSetup/Configured/POR.err` on the target server. Setup cannot be reinitiated until this file has been deleted.

The contents of this log can be displayed, and the log file deleted, using Server Assistant. In the Welcome pane, select "Set up a remote server" and click Continue. In the Destination pane, list the server(s) of interest. If an error log exists for a server, the server's row in the list contains an error icon. Select the row and double-click the error icon. If prompted, supply the preset password and click Send. The log contents are displayed, and you can click Delete to delete the log file.

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 are 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 signon
- Using Kerberos and other authentication techniques

Setting Up User Management

Unless you are 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 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.

The user management guide tells you how to manage users by setting up group and computer accounts. It also describes how to set up preference settings in order to customize the work environments of Mac OS X and Mac OS 9.1 users.

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 did not 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.

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 Protocols, then select the protocols you want to use for sharing.

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.

When you turn on print service in Server Admin, a queue is set up for any USB printer connected to the server. No printer queues are set up automatically for network printers, but they are 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 If it is not running, click the Start Service button in the toolbar.
- 4 Click the Settings button at the bottom of the application window, then click the Queues tab.
- 5 Click the Add (+) button.
- 6 Choose a connection protocol, identify a printer, then click OK.

Users of Mac OS X computers can now add the printer using Print Center. Mac OS 9 users add the printer using the Chooser.

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.

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 is not 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 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 image 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.

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.

Identify the server for which information appears in the table below:

Item	Description	Your information
Identity of server for installation and setup	<p>For interactive installation and setup of a 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)- DNS 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 version 10.1 or 10.2 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>	

Item	Description	Your information
Disk format (for clean installations only)	In most cases, use Mac OS Extended (Journaled). You can also use Mac OS Extended or case-sensitive HFS+.	
Disk partitioning (for clean installations only)	The minimum recommended size of a target disk partition is 4 GB.	
Disk mirroring (for clean installations only)	If you have a second disk in your target server, you can mirror the startup disk onto the second disk. If the primary disk is unavailable, the second disk is used.	
Saving 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 this server's setup data in a file, identify the setup file and optionally the key file. Also identify a backup location for the files.</p> <p>If you want to save this server's setup data in a directory, identify a directory and the key file name and location.</p>	
Language	The language to use for server administration (English, Japanese, French, or German).	
Keyboard layout	The keyboard for server administration.	
Serial number	The serial number for your copy of Mac OS X Server. Look on your installation disc envelopes or on your server hardware as its documentation describes.	
Administrator's full name (sometimes called long name or real name)	A full 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. This name is case sensitive in the login window, but not when accessing file servers.	

Item	Description	Your information
Administrator's short name	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, or _ (underscore).	
Administrator's password	If you record this value, be sure to keep this worksheet in a safe place. This value is case sensitive. It is also the password for the root user.	
Host name	The name you want DNS to use for your server. You specify the part of the DNS name that appears before the domain name (MyComputer.<domain-name> or MyComputer.example.com). The host name should begin with a letter and contain only letters, numbers, - (hyphen), or . (dot). Windows clients use host names no longer than 15 ASCII characters; they can contain a-z, A-Z, 0-9, -, but no . or space and can't contain only numbers.	
Computer name	The AppleTalk name.	
Rendezvous name	The name Mac OS X users see when viewing the computers listed under /Network/Local/.	
Network interface data	Your server has a built-in Ethernet port and may have additional ports installed on an Ethernet card. Record information for each port you want to activate.	Use the table provided later in this worksheet to record data for each port.

Item	Description	Your information
Open Directory usage	Select one: <ul style="list-style-type: none"> - Standalone Server (use only the local domain). - Connected to a Directory System (get information from an existing directory). If you choose this option, use one of the next four rows in this table to indicate how the server will locate 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"	The directory to use will be identified by a DHCP server.	
Using "Apple LDAP Directory"	The directory to use will be an Apple LDAP directory identified by a DHCP server or identified by specifying an IP address or domain name for the LDAP server.	
Using "NetInfo Directory"	The directory to use will be a NetInfo directory. Choose one or more of these 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 System"	The directory to use will be configured using the Directory Access application after you are finished setting up the server.	

Item	Description	Your information
Using “Open Directory Master”	<p>Optionally indicate you want to enable a Windows Primary Domain Controller on the server. Provide a computer name and a domain name for the controller. The computer name can contain a-z, A-Z, 0-9, -, but no . or space and can't contain only numbers.</p> <p>Finish setting up the directory you want to host by using Server Admin after completing server setup.</p>	
Automating service startup	<p>Indicate whether you want any of the following services to start automatically every time the server starts; these services need no additional configuration to be useful:</p> <ul style="list-style-type: none"> Apple file service FTP service Windows file service Mail service Web service WebDAV Network time service NetBoot service QuickTime Streaming service 	
Time zone	Choose the time zone you want the server to use.	
Network time	Optionally indicate a Network Time Server for the server to use.	

Network interface data for this server is in the table below:

Port	Characteristic	Your information
Built-in Ethernet (en0)	Whether to use the port for TCP/IP connections	
	Whether to use the port for AppleTalk connections. Mac OS 9 clients use AppleTalk for Chooser browsing, and some printers require AppleTalk. Enable no more than one port for AppleTalk per AppleTalk network.	
	If IP address is configured manually: IP address Subnet mask Router (use server IP address if in doubt or leave it blank) DNS servers Search domains (optional)	
	If IP address is configured using DHCP with Manual IP address: IP address DNS servers Search domains (optional)	
	If IP address is configured using DHCP: DHCP client ID (optional) DNS servers Search domains (optional)	
	If IP address is configured using BootP: DNS servers Search domains (optional)	
Port name:	Whether to use for TCP/IP	
	Whether to use for AppleTalk	
	If TCP/IP connection is configured manually: IP address Subnet mask Router (use server IP address if in doubt) DNS servers Search domains (optional)	

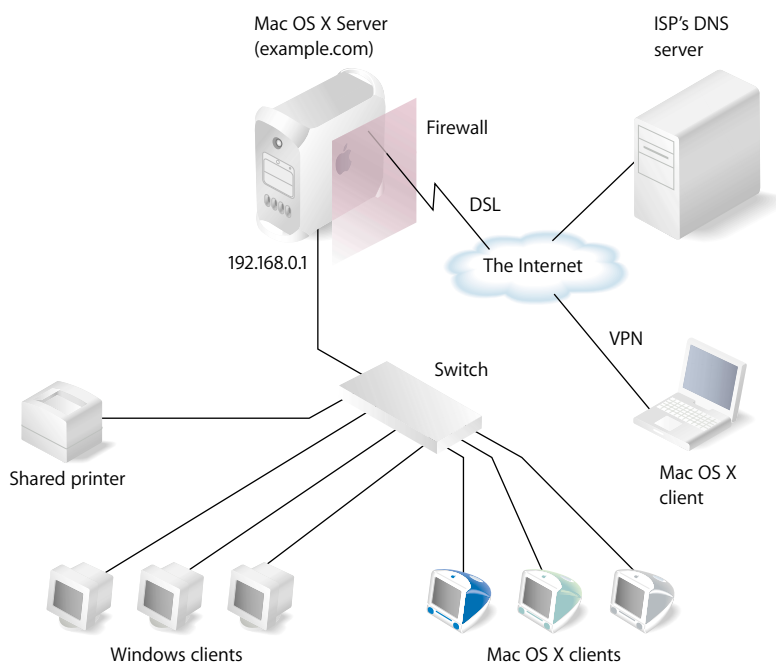
Port	Characteristic	Your information
	If TCP/IP connection is configured using DHCP with Manual IP address: IP address DNS servers Search domains (optional)	
	If TCP/IP connection is configured using DHCP: DHCP client ID (optional) DNS servers Search domains (optional)	
	If TCP/IP connection is configured using BootP: DNS servers Search domains (optional)	
Port name:	Whether to use for TCP/IP	
	Whether to use for AppleTalk	
	If TCP/IP connection is configured manually: IP address Subnet mask Router (use server IP address if in doubt) DNS servers Search domains (optional)	
	If TCP/IP connection is configured using DHCP with Manual IP address: IP address DNS servers Search domains (optional)	
	If TCP/IP connection is configured using DHCP: DHCP client ID (optional) DNS servers Search domains (optional)	
	If TCP/IP connection is configured using BootP: DNS servers Search domains (optional)	
Port name:	Whether to use for TCP/IP	
	Whether to use for AppleTalk	

Port	Characteristic	Your information
	If TCP/IP connection is configured manually: IP address Subnet mask Router (use server IP address if in doubt) DNS servers Search domains (optional)	
	If TCP/IP connection is configured using DHCP with Manual IP address: IP address DNS servers Search domains (optional)	
	If TCP/IP connection is configured using DHCP: DHCP client ID (optional) DNS servers Search domains (optional)	
	If TCP/IP connection is configured using BootP: DNS servers Search domains (optional)	

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 is a summary of the scenario's characteristics:

- An Open Directory master LDAP domain on the server centralizes user management, including authentication of Mac OS X and Windows users.
- The ISP's DNS service provides a 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 disc. 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 83 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 81 for instructions.

Insert the second install disc when prompted.

When installation is complete, the server restarts and Server Assistant opens.

- 3 Fill out the worksheet on page 111. You’ll need the information as you move through the Assistant’s panes.
- 4 Use the Language and Keyboard panes to select a server 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 host, computer, and Rendezvous names for your server. Click Continue.

For this example, presume the host name is myserver.

- 7 Make sure the Network Interfaces pane lists your external and internal Ethernet interfaces. If you need to add an interface, click Add.

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. VPN uses it as the public network, treating all others listed as private.

Click Continue when both interfaces are listed.

- 8 The TCP/IP Connection pane appears for each Ethernet interface.

For the external interface, choose Manually from the Configure pop-up list, then enter the IP address, subnet mask, and DNS server IP address, or addresses, provided to you by the ISP. Click Continue.

For the internal interface, enter these values then click Continue:

Configure: 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 master 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.

Step 3: 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 Select the IP address group named 192.168.0.0/16. Then 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.

The group includes 255 IP addresses. The notation /16 is a shortcut for the subnet mask 255.255.255.0.

- 6 Select the IP address group named "Any," and select "Allow" for services you want external clients to be able to access behind the firewall.
- 7 Click Save.

Step 4: Set up DNS service

- 1 In Server Admin, select DNS in the Computers & Services list.
- 2 Click Settings.
- 3 Make sure that "Zone transfers" is not enabled and that "Recursion" is enabled.
- 4 Click Zones, and then click the Add button (+) under the Zones list to set up a zone for the intranet. Enter the following values, then click OK:

Zone Name: example.com. (The trailing period is required.)

Type: Master

SOA: myserver.example.com. (The period at the end is required.)

Admin email: admin.example.com. (The period at the end is required.)

- 5 To define the master zone's records, select the master zone in the Zone list. You'll see that a Name Server (NS) record already exists; it was created when the zone was created.

Click the Add button (+) under the Records in Zone list to add an Address (A) record for your server. Enter these values, then click OK:

Map from: myserver.example.com. (The trailing period is required.)

Map to: 192.168.0.1

Create reverse mapping record: enable this option

Add additional Address records for each intranet device (other servers, printers, and so forth) that has a static IP address. Make sure that you enable "Create reverse mapping record" for each additional Address record.

- 6 Click Save, and then click Start Service.

Step 5: 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 Enable and select the internal Ethernet interface.
- 5 Click the Edit 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 are reserved for devices that need static IP addresses or for VPN users.

Most of the data is already filled in for you. Here are some sample values:

Starting IP Address: 198.168.0.2

Ending IP Address: 98.168.0.102

Subnet Mask: 255.255.0.0

Router: 192.168.0.1

- 6 Click DNS and make sure it displays the following values:

Default Domain: example.com

Name Servers: 198.168.0.1

- 7 Click LDAP to configure DHCP to identify the server you are configuring as the source of directory information for clients who are served dynamic IP addresses.

The server you are setting up is automatically identified in the Server Name field, because you set up a master LDAP domain on the server when you used Server Assistant. Other settings are optional for this example.

- 8 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: 198.168.0.1

NBDD Node Type: Broadcast (b-node)

- 9 Click Save, then click Start Service.

Step 6: 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 “Share your connection from” pop-up menu.
- 4 Click Save, then click Start Service.

Step 7: 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 10.3 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.

Specify the shared secret by typing a string in “IPsec 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.

To restrict VPN connections to members of a group, select “Restrict access to group” and select the group. Click the Users & Groups button to open a drawer from which you can drag a group name into the field.

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.

- 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 are 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".

To restrict VPN connections to members of a group, select "Restrict access to group" and select the group. Click the Users & Groups button to open a drawer from which you can drag a group name into the field.

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 8: 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 9, to configure the services of interest. Many services, such as Apple file service, require minimal setup—simply start them using Server Admin.

Step 9: 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 and computer accounts 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 10: Configure client computers

The information that follows applies to Mac OS X version 10.3 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 10.3 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 have 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 that is 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.

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. For example, if a user fills out a form on the site, a CGI could send the message to an application that processes the data and sends a response back to the user.

computer account A list of computers that have the same preference settings and are available to the same users and groups.

DHCP (Dynamic Host Configuration Protocol) A protocol used to 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 (using Disk Copy) 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.

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.

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 The Network File System (NFS) term for sharing.

filter A “screening” method used to control access to your 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.

group A collection of users who have similar needs. Groups simplify the administration of shared resources.

group directory A directory that organizes documents and applications of special interest to group members and allows group members to pass information back and forth among them.

guest computer An unknown computer that is not included in a computer account 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.

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.

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.

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.

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 is possible to access additional services without retyping a password (this is called single-signon) for services that have been configured to take Kerberos tickets. Mac OS X Server uses Kerberos v5.

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 the demands by client computers for network services across multiple servers in order to optimize performance by fully utilizing the capacity of all available servers.

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 is accessible only by logging directly in to the computer where it resides unless you log in to the computer using SSH.

long name See *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 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. Macintosh Manager allows administrators to control both system preferences and application preferences for Mac OS 9 and Mac OS 8 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 for web servers.

name server See *DNS (Domain Name System)*.

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.

NetBoot server A Mac OS X server on which you have 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 File System (NFS) A client/server protocol that uses TCP/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.

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.

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.

owner The person who created a file or folder and who therefore has the ability to assign access privileges for other users. The owner of an item automatically has read/write privileges for that item. An owner can also transfer ownership of an item to another user.

PHP (PHP: Hypertext Preprocessor) A scripting language embedded in HTML that is used to create dynamic webpages.

POP (Post Office Protocol) A protocol for retrieving incoming mail. After a user retrieves POP mail, it is stored on the user's computer and usually is 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.

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 Settings that define the kind of access users have to shared items. You can assign four types of privileges to a share point, folder, or file: read/write, read-only, write-only, and none (no access).

QTSS (QuickTime Streaming Server) A technology that lets you deliver media over the Internet in real time.

RAID (Redundant Array of Independent Disks) A hard disk array that either increases the speed of disk input and output or mirrors the data for redundancy, or provides both of these features. Users may access the RAID as if it were one drive, although it may be divided into multiple partitions.

realm See *WebDAV realm*.

Rendezvous A protocol developed by Apple for automatic discovery of computers, devices, and services on IP networks. This proposed Internet standard protocol is sometimes referred to as "ZeroConf" or "multicast DNS." For more information, visit www.apple.com or www.zeroconf.org.

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, hidden from regular system and application software, used by NetBoot to write system-related information while a client computer is running off a server-based system disk image.

share point A folder, hard disk (or hard disk partition), or CD that is 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 (Server Message Block) 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 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.

static IP address An IP address that is 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.

System-less clients Computers that do not have operating systems installed on their local hard disks. 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. 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 is defined to provide access for WebDAV users and groups.

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

- Active Directory 31
- administrator computer setup 49
- AirPort 41
- Apache 38
- Apple File Service (AFP) 36
- Apple LDAP 30
- Apple Remote Desktop (ARD) 59
- AppleTalk 32
- application servers 43
 - AXIS 43
 - JBoss 44
 - SOAP 43
 - Tomcat 43
 - WebObjects 44
- automatic restart 45
- automating server setup 101
- automating server software installation 85

B

- basic password validation 31
- Berkeley Software Distribution (BSD) 29, 31

C

- CGI scripts 39
- command-line tools 60
- core system services 29

D

- Darwin 29
- Directory Access 50
- directory services 30
- disk space monitoring 45
- diskspacemonitor tool 45
- Disk Utility 45
- documentation 14
- Domain Name System (DNS) 40
- Dynamic Host Configuration Protocol (DHCP) 40
- dynamic websites 39

E

- exporting NFS volumes 37

- exporting users and groups 54

F

- file services 35
 - Apple File Service (AFP) 36
 - File Transfer Protocol (FTP) 37
 - Network File System (NFS) 37
 - sharing 36
 - Windows 36
- file sharing 36
- File Transfer Protocol (FTP) 37

G

- group accounts 33

H

- high availability 45
- home directories 33

I

- importing users and groups 54
- Inspector 54
- installation 63
- installation and setup worksheet 111
- installation planning
 - collecting and organizing information 78
 - defining a migration strategy 75
 - defining an integration strategy 76
 - defining physical requirements 76
 - determining a strategy 78
 - determining server setup infrastructure requirements 77
 - determining services to host 74
 - goals 73
 - identifying servers you'll set up 74
 - making sure hardware is available 78
 - setting up a team 73
- Installer 50
- installing server software
 - automating installation 85
 - disk preparation 81
 - hardware-specific tasks 82

- information you need 80
- interactive remote installation 83
- on Mac OS X version 10.3 computers 85
- optional software installation 88
- preset password 82
- system requirements 79
- using Installer locally 82
- using the installer tool 85

integrating into existing networks 44

IP failover 45

J

- J2EE 44
- Java 39
- JBoss 44
- journaled HFS disks 45

K

- Kerberos 31

L

- LDAP 30, 31
- log rolling 45

M

- Macintosh Manager 60
- Macintosh user management
 - mobile accounts 34
 - preference management 33
- mail service
 - authentication 39
 - Cyrus 39
 - filtering spam and viruses 39
 - Postfix 39
 - SquirrelMail 39
- migration 75
- MySQL 39

N

- NetBoot 34
- NetBoot Desktop Admin 58
- NetInfo 30
- Network Address Translation (NAT) 41
- Network File System (NFS) 37
- Network Image Utility 58
- Network Information System (NIS) 31
- Network Install 35
- network services 40
 - DHCP 40
 - DNS 40
 - IP failover 42
 - IP firewall 41
 - NAT 41
 - VPN 42
- new features in version 10.3 9

- non-Mac OS X workstation setup 49

O

- Open Directory
 - definition 30
 - discovery of network services 32
 - Kerberos authentication 31
 - LDAP replication 45
 - password validation 31
 - search policies 31
 - using Apple directories 30
 - using non-Apple directories 31
- OpenLDAP 30
- operating system image services 34
- opportunistic locking 36

P

- PackageMaker 58
- password validation 31
- Perl 39
- PHP 39
- preparing disks for installing server software 81
- preset 52
- print service 38

Q

- QTSS Publisher 43
- QuickTime Broadcaster 43
- QuickTime Streaming Server (QTSS) 42

R

- Rendezvous 32
- resharing NFS mounts 37

S

- scenarios
 - computational clustering 25
 - creative businesses 26
 - enterprise organizations 20
 - higher-education facilities 21
 - K-12 labs and classrooms 22
 - small and medium businesses 24
 - web service providers 27
- search policies 31
- Server Admin 55
 - opening and authenticating 55
 - using 55
- server administration guides 14
- Server Assistant 50
- Server Message Block (SMB) 32
- Server Monitor 58
- server setup 63
 - automated setup using directory data 103
 - automatic setup using data in a file 101
 - information you need 90

- keeping backup copies of saved setup data 93
- local interactive setup 96
- offline mode 100
- Open Directory usage 93
- remote interactive batch setup 98
- remote interactive multiserver setup 99
- remote interactive setup 97
- saving setup data in a directory 92
- saving setup data in a file 90
- status monitoring 106
- service discovery 30
- Service Location Protocol (SLP) 32
- service setup 106
- share points 36, 53
- sharing files 36
- Simple Authentication and Security Layer (SASL)
 - password validation 31
- single signon 32
- software RAID 45
- SquirrelMail 39
- SSH 60
- strict locking 36

T

- Terminal 60
- Tomcat 43

U

- UNIX shells 60
- user management
 - group accounts 33
 - home directories 33
 - Macintosh user management 33
 - user accounts 32
 - Windows user management 34

V

- version 10.2 server management 60
- Virtual Private Network (VPN) 42

W

- Web-Based Distributed Authoring and Versioning (WebDAV) 38
- web cache 38
- web service 38
- Windows
 - browsing 36
 - file service 36
 - integration 45
 - user management 34
- Windows Internet Naming Service (WINS) 36
- Workgroup Manager 51
 - opening and authenticating 51
 - using 52
- worksheet 111