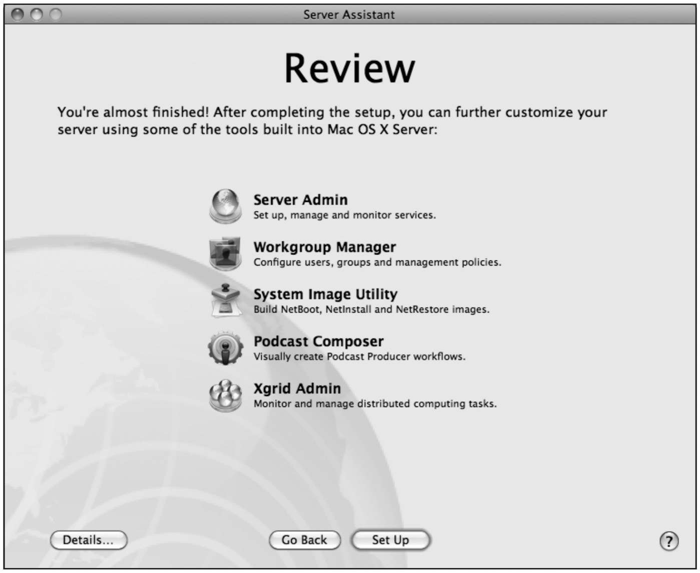
30 You are now at the Review pane. Do *not* click the Set Up button. Instead, leave your Mac OS X Server at this Review pane.

You will save an Auto Server Setup file and use it in the next exercise.



Review

You're almost finished! After completing the setup, you can further customize your server using some of the tools built into Mac OS X Server:

Server Admin
Set up, manage and monitor services.

Workgroup Manager
Configure users, groups and management policies.

System Image Utility
Build NetBoot, NetInstall and NetRestore images.

Podcast Composer
Visually create Podcast Producer workflows.

Xgrid Admin
Monitor and manage distributed computing tasks.

Generating Auto Server Setup Configuration Data

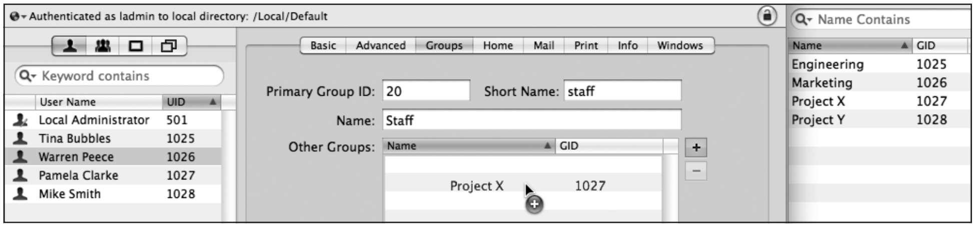
Rather than immediately setting up your server with the information you entered with Server Assistant, you can also generate and save the configuration data in an Auto Server Setup profile for later use.

There are three ways to create an Auto Server Setup profile that you can use later to automatically configure your Mac OS X Server:

- When running Server Assistant at the server itself or remotely, in the Review pane, click Details.
- Open Server Admin, and from the Server menu, choose Create Auto Server Setup Profile.
- Open Server Assistant from /System/Library/CoreServices, and then choose Create Auto Server.

4 Select the Project X group, and drag it from the Groups drawer to the Other Groups list.

Notice that as you drag the group, the pointer changes from an arrow to a plus sign. This indicates that you are adding this group to the text field.



User Name	UID
Local Administrator	501
Tina Bubbles	1025
Warren Peece	1026
Pamela Clarke	1027
Mike Smith	1028

Primary Group ID: 20 Short Name: staff

Name: Staff

Other Groups:

Name	GID
Project X	1027

Name	GID
Engineering	1025
Marketing	1026
Project X	1027
Project Y	1028

5 Click Save.

You have now successfully added Warren Peece as a member of the Project X group. However, Warren Peece also needs access to Project Y.

6 Add the Project Y group to the user account of Warren Peece. Remember that while it seems like you modified this user's account record, you really modified the group account records.

You have just added multiple groups—Project X and Project Y—to the Warren Peece user account.

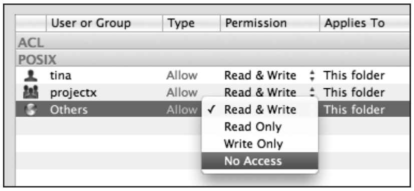
Adding Groups to Groups

Let's say you need a group that enables you to control permissions for the entire Engineering department, which consists of two divisions, Project X and Project Y. You could populate the Engineering group with all the individual engineering user accounts. However, an easier approach is to add the two project groups to the Engineering group. This effectively adds all members of those groups to the main group, which is a more efficient way to manage groups than in ~~previous versions of Mac OS X Server.~~

[replace above text with:]versions of Mac OS X Server prior to v10.5.

1 Click the Groups button, and select the Engineering group from the list of groups.

2 In the Members pane, click the Add (+) button to open the Users and Groups drawer.



	User or Group	Type	Permission	Applies To
ACL				
POSIX				
	tina	Allow	Read & Write	This folder
	projectx	Allow	Read & Write	This folder
	Others	Allow	✓ Read & Write Read Only Write Only No Access	This folder

15 Click Save.

As in Mac OS X, when a user attempts to access a file or folder, the user account is compared with the file or folder's owner and group. If the user account is the owner, the permissions assigned to the owner are enforced, and the permissions for the group and everyone are ignored for that account. If the user account is not the owner but is a member of the group, group permissions are enforced. If the account is neither the owner nor a member of the group, everyone's permissions are enforced.

> **MORE INFO ▶** In an "owner-only delete" scenario such as what may exist in a shared temporary scratch space, an authorized user has read/write access to the file, but only the owner can delete it. This option, known as the sticky bit, can be set only at the command line via `chmod +t`.

Setting ACLs

In both the client and server versions of Mac OS X v10.6, ACLs are enabled by default.

> **TIP ▶** I[Delete this tip.]lar volume, you nal utility.

Setting ACLs with Server Admin

In Mac OS X Server v10.4, you needed to use Workgroup Manager to set file-system ACLs, but in v10.5 and v10.6, you use Server Admin. Managing the ACL is similar to POSIX permissions management except that you drag accounts to the ACL section of the Permissions table instead of the POSIX section of the Permissions table, and a much larger range of permissions types is available.

Control List Canonically to have Mac OS X Server sort the ACEs in a consistent and predictable way.

3. When evaluating an ACL, Mac OS X Server evaluates the first ACE in the list and continues on to the next ACE *until it finds an ACE that matches the permission required for the requested action*, whether that permission is Allow or Deny. Even if a *deny* ACE exists in an ACL, if a similar *allow* ACE is listed first, the allow ACE is the one that is used, because it is listed first. This is why it is so important to use the Sort Access Control List Canonically command.
4. A POSIX permission that is restrictive does not override an ACE that specifically allows a permission.
5. If no ACE applies to the permission required for the requested action, the POSIX permissions apply.

For example, if Warren Peece attempts to create a folder, the requested permission is Create Folder. Each ACE is evaluated until there is an ACE that either allows or denies Create Folder for Warren Peece or a group that Warren Peece belongs to.

Even though this is an unlikely scenario, it illustrates the combination of an ACL and POSIX permissions: If a folder has an ACE that allows Warren Peece full control, but the POSIX permission defines Warren Peece as the owner with no access, Warren Peece effectively has full control. The ACE is evaluated before the POSIX permissions.

As another example, consider a folder with an ACL that has a single ACE that allows Tina Bubbles read permission, and the folder's POSIX permission defines Tina Bubbles as the owner with read and write permission. When Tina Bubbles attempts to create a file in that folder, there is no ACE that specifically addresses the Create Folder request, so no ACE applies to that request, so the POSIX permissions apply, and Tina Bubbles can create the file.

Allow Access Is Cumulative

In the following diagram, assume that algebra tutors are algebra students, and that all algebra students are students. The folder has three entries in the ACL:

[insert "Math":] The Math folder has three entries in the ACL.

- All students can read the contents of the folder (inherited from the parent).
- Algebra students can write to the folder.
- Algebra tutors can administer the folder.

Connecting Mac OS X Server to an Existing Open Directory Service

If you intend to set up multiple servers, it would be extremely inefficient to populate each server with the same user accounts. Instead, you can bind your Mac OS X server to another directory system. In this role, the server gets authentication, user information, and other directory information from some other server's directory service. This way, users can authenticate to your Mac OS X server with an account defined in your server's local directory, or with an account defined in any directory node that your server is bound to. The other directory node could be an Open Directory or an Active Directory directory service.

You can use System Preferences or Directory Utility to bind your Mac OS X server to another directory service. In order to use System Preferences, you need to be able to log in at the server's login window, but you can use Directory Utility remotely from another Mac OS X or Mac OS X Server computer.

Binding with System Preferences

You can configure your server to obtain directory services from an existing Open Directory server just like you would for a Mac OS X computer: Use System Preferences. This exercise assumes:

- You have a replica configured at 10.1.18.1 from the previous exercise.
- You have a third server that you set up with the same instructions that you used in Chapter 1, "Installing and Configuring Mac OS X Server," except you used 10.1.19.1 as the IP address and Server 19 as the computer name.
- You will configure a standalone Mac OS X server at 10.1.19.1 to bind to the replica at 10.1.18.1.
- You have forward and reverse DNS records available for these servers.

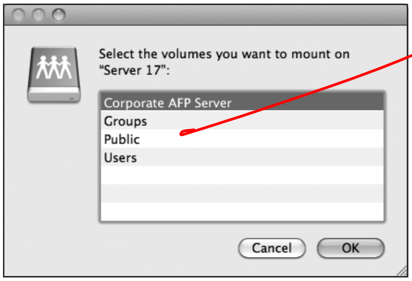
If you do not meet these requirements, you can read through this exercise but not complete it.

1 On your Mac OS X computer, open Server Admin, connect to the server you want to bind, and authenticate as ladmin (password: `ladmin`).

2 In the server list, select the server you want to bind.

6 ~~Select the Corporate AFP Server share point and click OK.~~

[Delete sentence and image.]

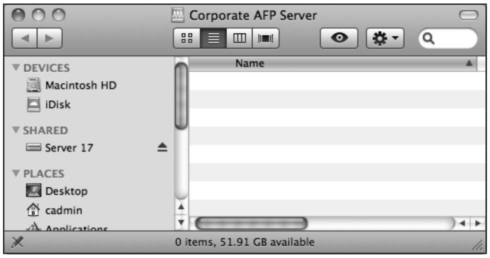


Select the volumes you want to mount on "Server 17":

Corporate AFP Server
Groups
Public
Users

The Corporate AFP Server share point should open in your Finder as a folder.

Note that an icon for the network volume does *not* appear on your desktop, but an eject icon does appear next to your server in the Finder window sidebar.



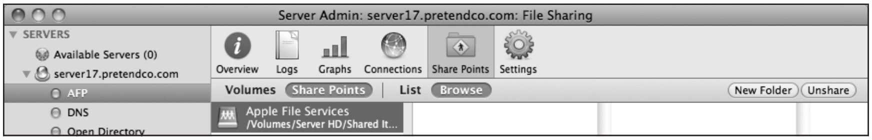
0 items, 51.91 GB available

7 Unmount the Corporate AFP Server share point.

Restrict Access to Files

Now that you have shared the Apple File Services folder, modify the permissions to restrict access to the files.

1 On your Mac OS X computer in Server Admin, click the File Sharing button in the toolbar, and then click the Share Points button, followed by the Browse button. Select the Apple File Services share point.



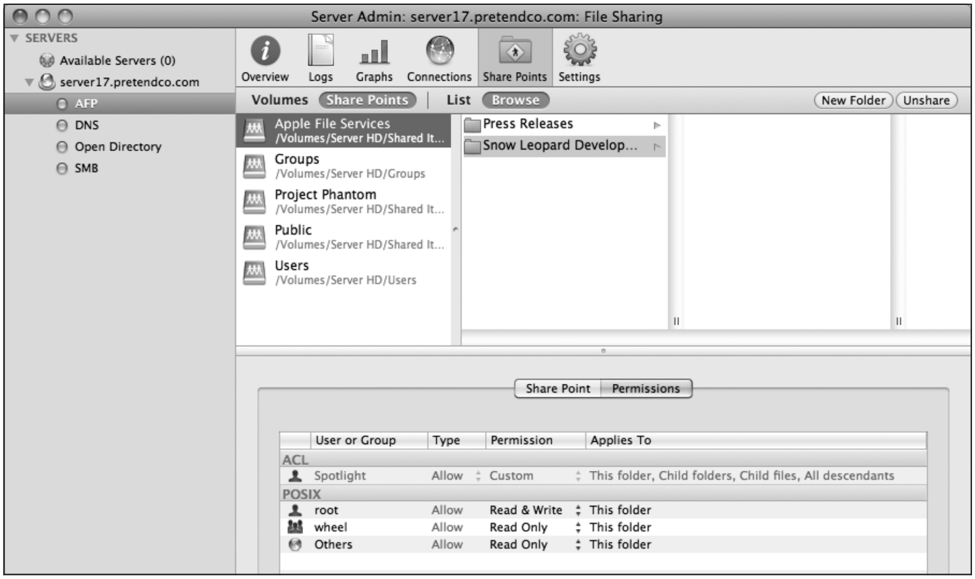
Server Admin: server17.pretendco.com: File Sharing

Apple File Services
/Volumes/Server HD/Shared It...

2 Click the New Folder button in the upper-right corner of Server Admin and create a folder inside Apple File Services called `Press Releases`. Click Save.

You can create folders and share points using Server Admin without actually going to your server computer.

3 Create a second new folder inside Apple File Services called `Snow Leopard Development`. Click Save.



	User or Group	Type	Permission	Applies To
ACL				
	Spotlight	Allow	Custom	This folder, Child folders, Child files, All descendants
POSIX				
	root	Allow	Read & Write	This folder
	wheel	Allow	Read Only	This folder
	Others	Allow	Read Only	This folder

4 Click the Snow Leopard Development folder in Server Admin.

5 In the Permissions pane, change the POSIX permissions as follows:

- Owner: student1, Read & Write
- Group: admin, Read & Write
- Others: No Access

	AFP	SMB	NFS	FTP
Native platform	Mac OS	Windows	UNIX	Multi-platform
Security	Authentication is normally encrypted	Authentication is normally encrypted	Authentication only if using Kerberos	Uses clear text passwords
Browsable	Bonjour	NetBIOS	Bonjour	Bonjour
Example URL	afp://server17.example.com/SharePoint	smb://server17.example.com/Share	nfs://server17.example.com/Volumes/Data/	ftp://server17.example.com nfs_share

["nfs_share" is in the wrong place. It's the end of the path in the "NFS" column; it doesn't belong in the "FTP" column.]

AFP and SMB are both full-featured file-sharing protocols with reasonably good security.

NFS (without Kerberos) is not as secure as the other protocols, but it is very convenient for UNIX clients. Be careful before you "export" (share) a volume over NFS. With a Mac OS X server and a Mac OS X client, NFS volumes are browsable in Connect to Server; that is, a user can find them by browsing through a list of servers in the Connect to Server window.

FTP is useful because it offers maximum compatibility. However, FTP also offers a minimal feature set, and its passwords are sent over the network as clear text unless you are using the Kerberos option and a supported Kerberos FTP client—something the Mac OS X Finder lacks.

Mac OS X supports secure File Transfer Protocol (SFTP), a secure alternative for FTP that uses SSH to encrypt the FTP connection. Of the four file-sharing protocols, only AFP has simple built-in support for encrypting connections. If you're in a fully Kerberized environment, you can also use NFS in an encrypted fashion, but you still must deal with its other shortcomings.

What You've Learned

- The first step when implementing file-sharing services is to plan out the shared services needed.
- A share point is any folder, drive, or partition that you make available to network clients. Share points are created and configured in Server Admin. A share point can be shared over AFP, SMB, NFS, or FTP. Access control lists can be used to set very flexible restrictions on share points and folders.
- Mac clients normally access share points over AFP, which is configured in Server Admin.

- Windows service allows share points to be accessed by Windows clients over SMB.
- NFS provides UNIX systems with access to share points. Unlike AFP and SMB, NFS relies upon the IP address of the computer for authentication (unless you're using Kerberos).
- Mac OS X Server provides FTP access for share points as well. Mac OS X Server's FTP service provides the additional feature of automatically encoding, archiving, or compressing a file on the fly, based upon the extension that the client adds to the filename.
- Automount share points and network home folders also can be configured on Mac OS X Server.

References

Apple's support page for file sharing is at: http://www.apple.com/support/macosxserver/filesharing

Mac OS X Server Administration Guides

The following documents provide more information about installing Mac OS X Server. All of these and more are available at http://www.apple.com/server/macosx/resources/documentation.html.

Getting Started

Upgrading and Migrating

File Services Administration

~~*Windows Services Administration*~~ [delete]

User Management

Command-Line Administration

Apple Knowledge Base Documents

You can check for new and updated Knowledge Base documents at http://www.apple.com/support.

Document HT1822, "Mac OS X Server: Admin Tools compatibility information"

Document TA23008, "Mac OS X 10.4 Tiger: 'Connection failed' error when connecting to an AFP server"

Document HT2202, “Mac OS X Server 10.5: Setting a custom umask”

Document TA24986, “Mac OS X Server 10.5: About Kerberized NFS”

URLs

Mac OS X Server File-Sharing Issues: http://www.afp548.com

Network File System (NFS) version 4 Protocol: http://www.ietf.org/rfc/rfc3530.txt

AFP Reconnect/Timeout Definitions and Behavior: http://support.grouplogic.com/?p=1568

Chapter Review

1. Name four file-sharing protocols supported by Mac OS X Server and their principal target clients.
2. How does Mac OS X Server support browsing for Windows clients?
3. What is the primary security concern with NFS?
4. What does FTP file conversion do?

Answers

1. AFP for Mac clients; SMB for Windows clients; NFS for UNIX clients; and FTP for multiple cross-platform client access are four file-sharing protocols supported by Mac OS X Server.
2. On smaller networks, Mac OS X Server uses NetBIOS to advertise its presence. On larger networks, Mac OS X can be a WINS server, or it can use an existing WINS server. If there are no other servers on the network, Mac OS X Server can be a workgroup master browser or a domain master browser.
3. Normally, NFS has no user-authentication process: NFS trusts that the client is who it claims to be. Beyond a security concern, this can also be a management issue if the client and server aren’t working with a unified user list. If you’re using Kerberos with NFS, you can authenticate the connection process, however.
4. FTP file conversion is a feature of the FTP server that automatically encodes a file or folder requested by an FTP client. The client appends .tar, .bin, or .gz to the end of the filename, and the server does the appropriate encoding. [insert ".dmg"]

3 Open Safari on Mac OS X and connect to `http://10.1.17.1`. Observe the page, and then enter the FQDN (`http://server17.pretendco.com`) and make sure you can observe the page again. Refresh the page if necessary.

NOTE ▶ Notice that you did not configure the website in any way. Mac OS X Server's web service is set to serve up the default webpages automatically.

4 Select the web service in Server Admin and go to Settings, then Modules. Turn on the apple_userdir_module by checking the box, then restart the web service.

NOTE ▶ Unlike in prior versions of OS X, user websites are not on by default. It is necessary to turn on this module to allow user websites. The change was made in an effort to increase security and limit access to user information.

5 Enter a tilde (~) and the short name `tina` after http://server17.pretendco.com/ and view that user's personal default webpage. The entry should appear like this: *http://server17.pretendco.com/~tina.*

NOTE ▶ Again, notice that you did not configure the personal website in any way. Mac OS X Server, like Mac OS X's web service, is set to serve up the default user webpages automatically once the web service is started.

NOTE ▶ It is important to note that the preceding exercises showcase the default behavior of Mac OS X and Mac OS X Server with respect to starting web services without any other configuration.

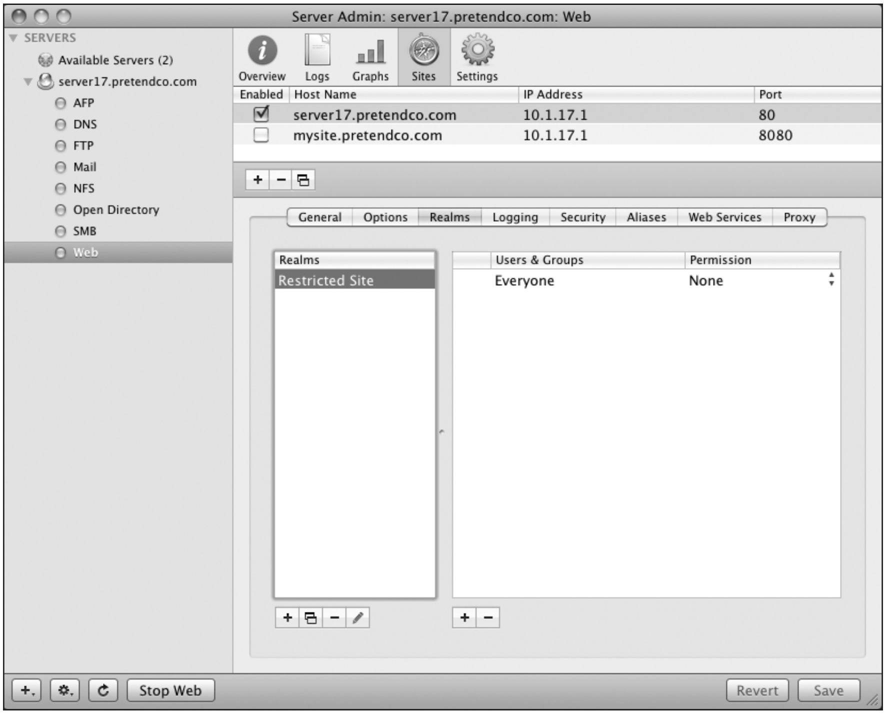
6 Quit Safari by using Command-Q or choosing Quit from the Safari menu.

You will now examine some basic options for managing websites on Mac OS X Server.

Managing Websites

You can manage many websites with Mac OS X Server. Each website can be distinguished by a different IP address, domain name, or port over which everyone accesses the site. Before you change any parameters on your existing site or add a new site, it is worth learning how Apple configures the defaults for the original site.

3 Click the Add (+) button under the Realms pane and give the realm a name. Then choose Digest as the authentication type. Leave the directory path at the default.



Server Admin: server17.pretendco.com: Web

Enabled	Host Name	IP Address	Port
☑	server17.pretendco.com	10.1.17.1	80
□	mysite.pretendco.com	10.1.17.1	8080

Realms
Restricted Site

Users & Groups	Permission
Everyone	None

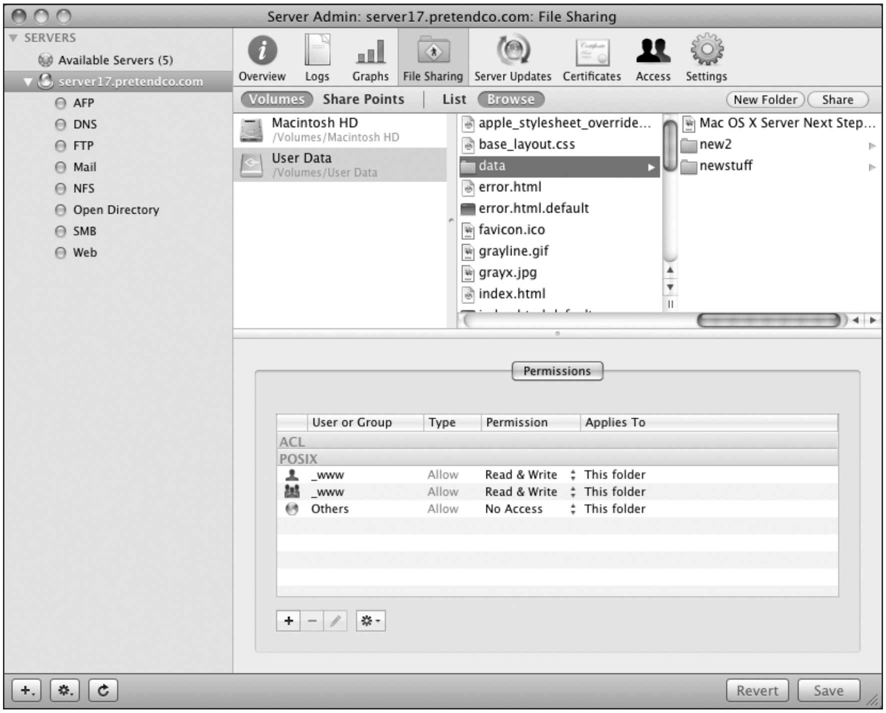
4 Click Save to save the realm. Click the realm to select it.

NOTE ▶ When you create a realm, no one has access to the realm by default. You must now add users and/or groups to have access to the realm.

5 Click the Add (+) button under the Users & Groups pane and add a group to the list. Once added, change the permissions to Browse Only for the group and click Save.

10 Click Browse to navigate to the /Library/WebServer/share/httpd folder and view the POSIX permissions at the bottom of the window.

11 Within the Documents folder, scroll down and locate the data folder, select it, and view the permissions. This is the folder we want to restrict.



User or Group	Type	Permission	Applies To
ACL			
POSIX			
_www	Allow	Read & Write	This folder
_www	Allow	Read & Write	This folder
Others	Allow	No Access	This folder

12 Change the POSIX permissions on the data folder as follows.

- _www: Allow Read & Write, This folder
- _www: Allow Read & Write, This folder
- Others: Allow No Access, This folder

13 Click Save.

2 Click File Sharing, and then Volumes, and then Browse.

3 Select your User Data volume, and then click New Folder.

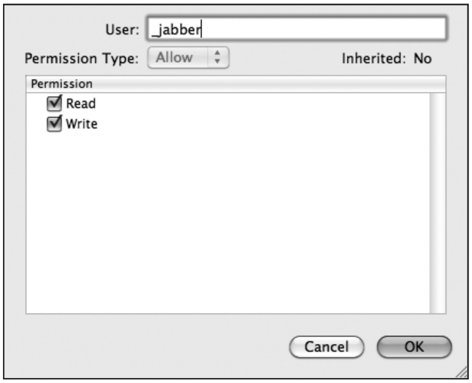
4 Name the new folder `Jabber`, and then click Create.

5 Select the Jabber folder you just created, and then click Share.

6 Click Permissions.

7 Double-click root in the owner row, and then change the User to `_jabber`.

Click OK.



User: _jabber

Permission Type: Allow

Inherited: No

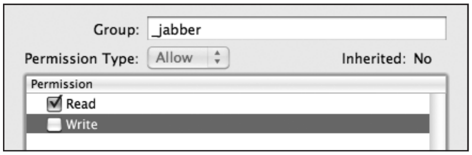
Permission

☑ Read

☑ Write

8 Double-click admin in the group row, and then change the Group to `_jabber`.

9 Deselect the checkbox for the Write permission.



Group: _jabber

Permission Type: Allow

Inherited: No

Permission

☑ Read

☐ Write

10 Click OK to dismiss the User and Permission pane.

You can also enable the Directory Gateway to allow users to search public contacts that were created with the utility named Directory in Mac OS X v10.5 (there is no utility named Directory for Mac OS X v10.6).

The Address Book service uses open source technologies including CardDAV (an extension to WebDAV), HTTP, and HTTPS, as well as vCard, a file format for contact information. You must use Open Directory user accounts to access the Address Book service, so your server must either be an Open Directory server or be bound to one.

When you create a contact with the Address Book service, you use CardDAV, not LDAP, to copy the changes to the server.

Configuring the Address Book Service with Server Admin

Although Server Preferences allows you to configure only the maximum size of each user's total Address Book, Server Admin allows you to configure:

- The data store
- User quota
- Log level (Error, Warning, Info, or Debug)
- A Directory Gateway for user accounts
- A Directory Gateway for shared accounts (from the utility named Directory in Mac OS X v10.5)
- Authentication method (Digest, Kerberos, or Any Method [Kerberos and then Digest])
- Host name for the Address Book service
- Port
- Whether or not to use SSL for CardDAV

In this exercise, before you start the Address Book service, you will change the data store, enable the Directory Gateway, and specify an SSL certificate for the service to use. If you do not have multiple volumes, skip the steps to choose a different data store.

1 On your Mac OS X computer, open Server Admin and connect to your Mac OS X Server as ladmin.

2 Click th

3 Select t

4 Select A

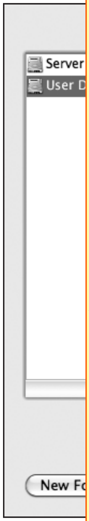
5 Click th

6 Click th

7 For the

8 Select y

9 Name t



10 In the s
click Cl

[replace steps 2 thru 10 with the following:]

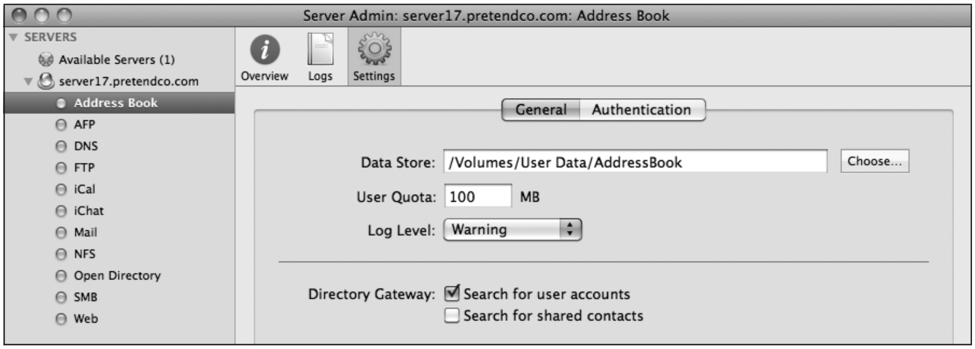
2 Select your server in the list of servers on the left.
3 Click File Sharing, and then Volumes, and then Browse.
4 Select your User Data volume, and then click New Folder.
5 Name the new folder AddressBook, and then click Create.
6 Select the AddressBook folder you just created.
7 Click Permissions.
8 Double-click root in the owner row, and then change the User to _carddav. Click OK.
9 Double-click admin in the group row, and then change the Group to _carddav.
10 Deselect the checkbox for the Write permission.
11 Click OK to dismiss the User and Permission pane.
12 Change the Permission for Others to No Access.
13 Click OK to dismiss the Group and Permission pane.
14 Click Save.
15 Click Settings in the toolbar.
16 Select the checkbox for Address Book, and click Save.
17 Select Address Book in the left column.
18 Click the Settings button in the toolbar, then click the General tab.
19 For the data store, click Choose.
20 Select your User Data volume, then select AddressBook, then click Choose.

[if possible, retain the figure between steps 9 and 10, but for space, you can remove the figure]

21 [include and renumber steps 11-16 on page 408 as steps 21-26]

[insert this note after Step 26:]
Note:
Changing location and migrating data after the Address Book service has already been used is beyond the scope of this book.

21 ~~11~~ Select the checkbox labeled “Search for user accounts.”


Server Admin: server17.pretendco.com: Address Book

Data Store: /Volumes/User Data/AddressBook

User Quota: 100 MB

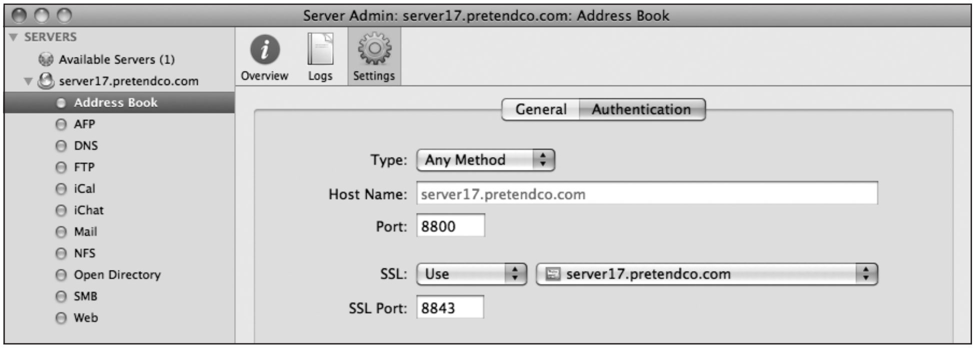
Log Level: Warning

Directory Gateway: ☑ Search for user accounts
□ Search for shared contacts

22 ~~12~~ Click the Authentication tab.

23 ~~13~~ Leave Type as Any Method, which attempts Kerberos authentication before trying the Digest method.

24 ~~14~~ In the SSL pop-up menu, choose Use, and then choose the certificate for server17.pretendco.com. Note that the SSL port used is 8843.


Server Admin: server17.pretendco.com: Address Book

Type: Any Method

Host Name: server17.pretendco.com

Port: 8800

SSL: Use server17.pretendco.com

SSL Port: 8843

25 ~~15~~ Click Save.

26 ~~16~~ Click Start Address Book.

- iChat service servers can be joined together in a process called federation.
- The new Address Book service uses such open source technology as CardDAV, an initiative based on WebDAV; vCard; and HTTP and HTTPS.

References

The following documents provide more information about the Mac OS X Server collaboration services. All of these and more are available at http://www.apple.com/server/macosx/resources/.

Administration Guides

Web Technologies Administration

Wiki Server Administration

Wiki Tools Deployment Guide

iCal Service

iChat Service

Address Book Server Administration

User Management

Getting Started

Advanced Server Administration

Upgrading and Migrating

URLs

Wiki site: http://www.wiki.org

CalConnect site: http://www.calconnect.org

CardDAV: http://www.ietf.org/id/draft-ietf-vcarddav-carddav-07.txt

Jabber site: http://www.jabber.org

"'Well known' TCP and UDP ports used by Apple software products":
http://support.apple.com/kb/TS1629

4. What is a NetBoot shadow file?
5. What are the major differences between NetBoot, NetInstall, and NetRestore?

Answers

1. Because NetBoot unifies and centralizes the system software that NetBoot clients use, software configuration and maintenance are reduced to a minimum. A single change to a NetBoot image propagates to all client computers on the next startup. NetBoot also decouples the system software from the computer, decreasing potential time invested in software troubleshooting.
2. A client must have selected a network disk image via the Startup pane within System Preferences, or the user must hold down the N key at startup to boot from the default NetBoot image, or use Remote Desktop Admin.
3. NetBoot makes use of DHCP, TFTP, NFS, and HTTP during the NetBoot client startup sequence. DHCP provides the IP address, TFTP delivers the boot ROM ("booter") file, and NFS or HTTP is used to deliver the network disk image.
4. Because the NetBoot boot image is read-only, anything that the client computer writes to the volume is cached in the shadow file. This allows a user to make changes to the boot volume, including setting preferences and storing files; however, when the computer is restarted, all changes are erased.
5. NetBoot allows multiple machines to boot into the same environment. NetInstall provides a convenient way to install operating systems and packages onto multiple machines. NetRestore provides a way to clone an existing image to multiple machines.

Setting Up a Network Home Folder Review

As discussed in Chapter 4, "Using File Services," you also use Workgroup Manager to set up a network home folder for a network user.

Set and create home folders for all users who do not yet have home folders.

1. On your Mac OS X computer, open Workgroup Manager and authenticate as necessary.

2. Click the Accounts button in the toolbar, and then click the globe icon below the toolbar. Choose /LDAPv3/127.0.0.1 from the pop-up menu.

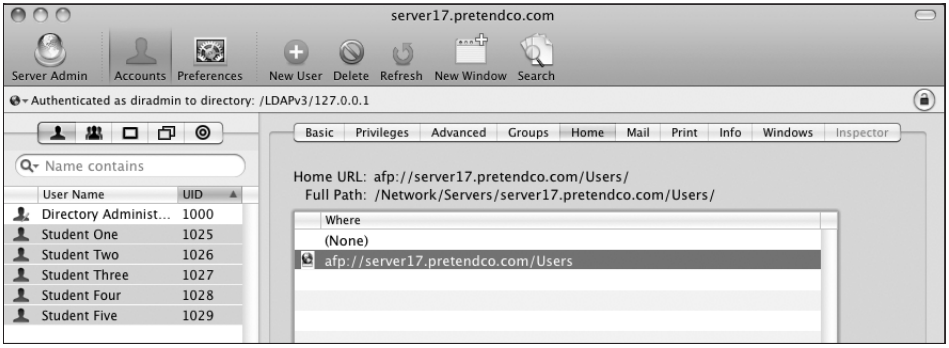
3. Select all the users and deselect the Directory Administrator account.

4. Click the Home tab.

5. Select the path afp://server17.pretendco.com/Users.

6. Click the Create Home Now button, and then click Save.

   If you already have home folders for some of the users, this will not change those settings.



Authenticated as diradmin to directory: /LDAPv3/127.0.0.1

User Name	UID
Directory Administ...	1000
Student One	1025
Student Two	1026
Student Three	1027
Student Four	1028
Student Five	1029

Home URL: afp://server17.pretendco.com/Users/
Full Path: /Network/Servers/server17.pretendco.com/Users/

Where
(None)
afp://server17.pretendco.com/Users

7. On your server, navigate to the /Users folder and verify that all the home folders were created.

8. Verify that you have a home folder for Student One by logging in as Student One from your Mac OS X computer, and then log out and log in as Local Administrator.

Managing Preferences for Users in a Workgroup

Although you can set up preferences individually for users with network accounts, it's more efficient to manage preferences for the workgroups to which they belong. Using workgroups allows you to manage users regardless of which computers they use. Using Workgroup Manager, you can provide all users in a workgroup with the same access permissions for media, printers, and volumes. A workgroup is group of users with managed preferences.

> **NOTE ▸** It is important to understand the difference between a workgroup and a group. A group is a file-system designation. It is used to handle access to the file system (as in owner, group, others). It is specific to the file system, server, or computer. A workgroup is a directory service record separate from any specific file system or server. It is used as a method of associating similar preferences for sets of user records.

A user can be assigned to one or more workgroups, and during login, the user is presented with a list of the workgroups to which he or she belongs. At login he or she can select which workgroup's settings should preside over that login session. The user then has all the permissions and access privileges assigned to that workgroup.

> **TIP** Administrative users are given an option to disable management. Once selected, this option is hidden but is visible again if the Option key is pressed during login.

Setting Up a Group Folder

You can use Workgroup Manager to set up a *group folder* for use by members of a particular workgroup. A group folder offers a way to organize documents and applications of special interest to group members and gives group members a way to pass information back and forth.

To set up a group folder in Workgroup Manager (you will do this in a later exercise):

1. Select the group and click the Group Folder tab.

2. Select a listed share point in which to set up a group folder.