Mac OS X Server

Migrating to Mac OS X Server
From Windows NT
For Version 10.4 or Later

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

Apple
1 Infinite Loop
Cupertino CA 95014-2084
www.apple.com

019-0351/03-24-05

Contents

About This Guide

Use this guide when you want to move to Mac OS X Server version 10.4 from a Windows NT server.

This guide contains instructions for transferring data and settings from a Windows NT server to a computer running Mac OS X Server version 10.4.

What's in This Guide

This guide includes the following chapters:

- Chapter 1, "Before You Begin," summarizes migration options and requirements.
- Chapter 2, "Migrating Users, Groups, and Computers," tells you how to transfer user, group, and computer records from a Windows NT primary domain controller (PDC) to a Mac OS X Server PDC. It also tells you how to set up home directories and roaming user profiles on Mac OS X Server for Windows users.
- Chapter 3, "Migrating Windows File Service," describes how to set up shared folders on Mac OS X Server and copy shared folders and files to them from Windows NT network folders.
- Chapter 4, "Providing Windows Access to Print Service," explains how you set up Mac OS X Server print queues for Windows access and how to add them as printers on client Windows computers.

For additional information on setting up and managing services for Windows users, see the Windows services administration guide. It also describes how to manage user, group, and computer records for Windows clients.

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

Using This Guide

Using this guide is easy. Simply read Chapter 1 to make sure you understand your options. Then work your way through the other chapters in turn. You'll find step-by-step instructions for preserving and reusing server data by using various tools and manual techniques. You'll also find references to instructions and supplemental information in other guides in the Mac OS X Server documentation suite; the next page tells you about the documents in the suite and where to find them.

Using Onscreen Help

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

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

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

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

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

The Mac OS X Server Suite

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

www.apple.com/server/documentation/

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

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

Getting Documentation Updates

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

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

Getting Additional Information

For more information, consult these resources:

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

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

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

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

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

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

Samba website—information about Samba, the open source software on which the Windows services in Mac OS X Server are based.
www.samba.org

Before You Begin

1

Take a few moments to become familiar with migrating options and requirements.

When you migrate users, groups, and computers from a Windows NT server to Mac OS X Server, it becomes a primary domain controller (PDC). Then migrated users can:

- Log in to the new PDC's domain using the same user names, passwords, and workstations as before.
- Have their roaming profiles automatically stored and retrieved from a Mac OS X Server system.
- Use network home directories located on a Mac OS X Server system.
- Remain members of the same groups.
- Access the contents of network folders that you have copied to Mac OS X Server share points.
- Use print queues that you have set up on Mac OS X Server and added as printers to users' Windows workstations.

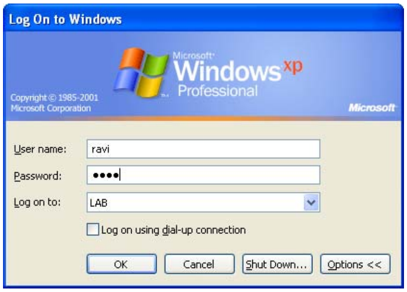
Other users for whom you set up Mac OS X Server user accounts can also use these services. In addition, Mac OS X Server can provide Windows Internet Naming Service (WINS) and Windows domain browsing across subnets for migrated and new Windows users.

Mac OS X Server can provide additional services to Windows, Mac OS X, and UNIX users, including mail, web, weblog, iChat (Jabber), VPN, DHCP, DNS, and NAT. For details, see the Mac OS X Server setup and administration guides described in the Preface.

By providing these services, Mac OS X Server can replace Windows NT servers in small workgroups. For example, you may be administering several Windows NT servers acquired over the years to support domain login and shared network folders. By today's standards, your older servers are probably rather slow and have small storage capacities. It's quite possible to migrate user accounts from multiple Windows NT domain controllers to one Mac OS X Server system. The same Mac OS X Server system could also host shared network folders for Windows users. If you prefer to isolate the user accounts on a dedicated Mac OS X Server system, the shared folders could reside on another Mac OS X Server system.

While serving users of Windows workstations, Mac OS X Server can also serve users of Mac OS X computers. A user account on the server can be used to log in from a Mac OS X computer as well as a Windows workstation. A user who logs in on both platforms can have the same home directory no matter where he or she logs in.

Note: "Log in" and "log on" mean the same thing. "Log on" is commonly used in the Windows environment and "log in" is commonly used in the Mac OS X environment.



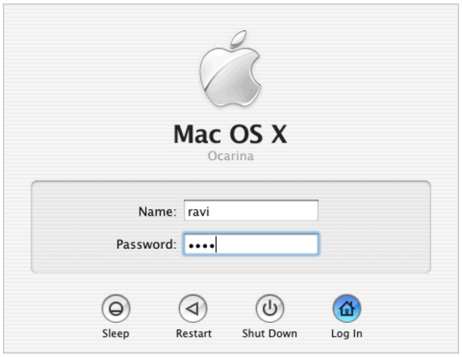
Log On to Windows

User name: ravi

Password: ••••

Log on to: LAB

□ Log on using dial-up connection



Name: ravi

Password: ••••

Users can log on to Windows and log in to Mac OS X using the same account

Planning Your Migration

Before you begin migrating accounts and services from a Windows NT server to Mac OS X Server, you should do some planning. You need to plan for:

- Migrating users, groups, and computers to a Mac OS X Server PDC
- Providing home directories and roaming user profiles
- Migrating Windows file service
- Providing Windows access to print service
- Configuring DNS

Migrating Users, Groups, and Computers to Mac OS X Server PDC

Mac OS X Server includes a command-line tool, `ntdomainmigration.sh`, that:

- Sets up Mac OS X Server as a PDC.
- Extracts user and group information and uses it to create Mac OS X Server user and group accounts.
- Extracts computer information and uses it to add Windows computers to the Mac OS X Server Windows Computers list, making them members of the Mac OS X Server PDC domain.

The migrated user and group accounts are stored in the server's LDAP directory together with the migrated computer records and other information. The PDC has access to this directory information because you migrate to a server that is already an Open Directory master, which hosts an LDAP directory. The LDAP directory will remain efficient with 200,000 records. Of course, a server hosting a directory domain of that size would need sufficient hard disk space to store all the records.

The PDC also uses the Open Directory master's Password Server to authenticate users when they log in to the Windows domain. The Password Server can validate passwords using the NTLMv2, NTLMv1, LAN Manager, and many other authentication methods. The Open Directory master can also have a Kerberos KDC. The PDC doesn't use Kerberos to authenticate users for Windows services, but mail and other services can be configured to use Kerberos to authenticate Windows workstation users who have accounts in the LDAP directory. For additional information on directory and authentication services, see the Open Directory administration guide.

If you want to provide failover and backup for the new PDC and you have additional Mac OS X Server systems, you can make one or more of them backup domain controllers (BDC). The PDC and BDCs have synchronized copies of directory and authentication data, and they share client requests for this data. If the PDC becomes unavailable, clients automatically fail over to a BDC until the PDC becomes available. See the Windows services administration guide for more information and instruction on setting up a BDC.

If you have Mac OS X Server systems that are neither PDC nor BDC, you can set them up to provide additional Windows services as members of the Mac OS X Server PDC domain. As a Windows domain member, Mac OS X Server's Windows services use the domain controller for user identification and authentication.

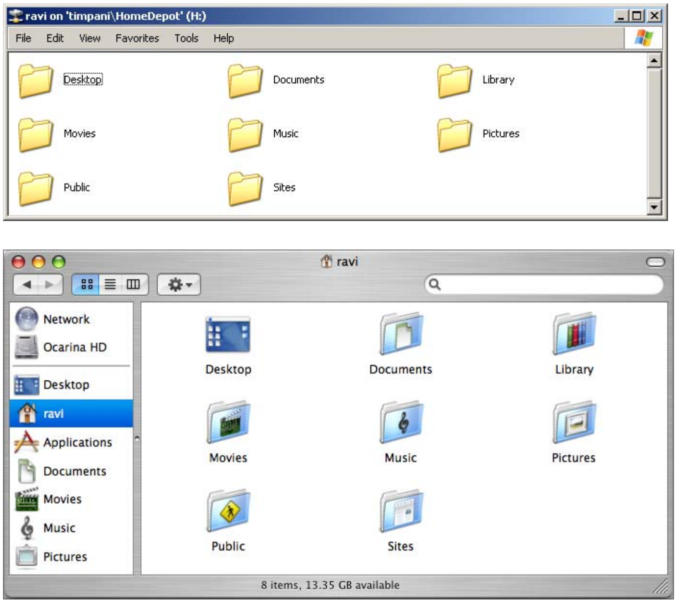
When setting up Mac OS X Server as a PDC, make sure your network doesn't have another PDC with the same domain name. The network can have multiple Open Directory masters, but only one PDC.

Providing Home Directories and Roaming User Profiles

Migrated users can continue using their existing home directories unless the home directories are located on the Windows NT server that you're taking out of service. If some users have home directories on the Windows NT server that's going out of service, you can migrate their home directories to Mac OS X Server. You can also migrate other users' home directories to Mac OS X Server.

Before you migrate home directories from the Windows NT server, the users will have to copy their files temporarily to another location such as their My Documents folders or a network folder. After you set up Mac OS X Server home directories for the users, the users can copy their files to their new home directories.

When a user with a Mac OS X Server home directory logs in to the Mac OS X Server PDC's Windows domain, Windows automatically maps the home directory to a network drive. If the same user logs in to a Mac OS X client computer, Mac OS X automatically mounts the same home directory. The user has the same network home directory whether logging in to a Windows computer or a Mac OS X computer.



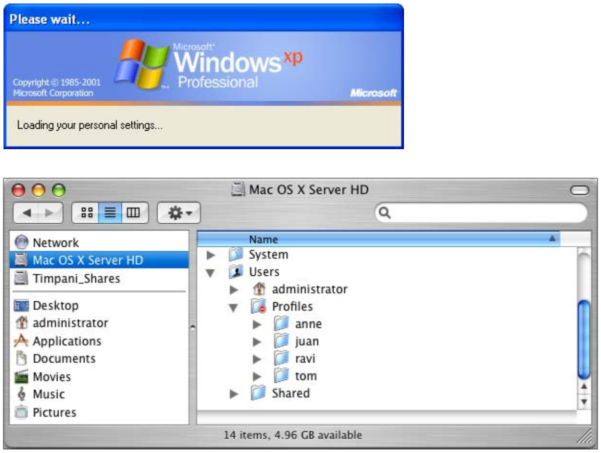
Users can access the same home directory from Windows and Mac OS X

A Mac OS X Server home directory is located in a share point, which is a folder, hard disk, hard disk partition, or other volume that can be accessed over the network. A home directory share point can be on the same server as the PDC or a Mac OS X Server domain member. Settings in the user account specify the home directory location and the drive letter for the Windows mapped drive. You can manage share points and home directory settings with Workgroup Manager.

Mac OS X Server also stores a user profile for each Windows user who logs in and out of the PDC. These are roaming profiles; each user has the same profile when he or she logs in to the PDC from any Windows workstation on the network. A user profile stores a Windows user's preference settings (screen saver, colors, backgrounds, event sounds, web cookies, and so on), favorites, My Documents folder, and more in a share point on a Mac OS X Server system.

Normally the PDC server stores users' roaming profile data, but you can have another Mac OS X Server system store the user profile data for any users. If you have only one Mac OS X Server system, it can be the PDC and host home directories and roaming user profiles.

Windows loads user profile settings stored on Mac OS X Server


Please wait…

Loading your personal settings…

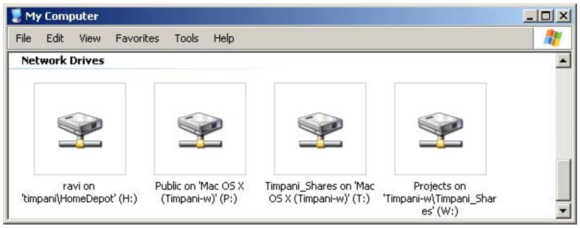
14 items, 4.96 GB available

Providing File Service

Whether you migrate users, groups, and computers to a Mac OS X Server PDC or not, you can set up Mac OS X Server to replace file service that Windows NT servers currently provide to Windows users. User accounts defined on Mac OS X Server can be used to authenticate access to shared network folders via the Windows standard protocol for file service, Server Message Block/Common Internet File System (SMB/CIFS or simply SMB). Windows users access shared folders on Mac OS X Server by using normal procedures such as mapping a network drive.

User accounts in the Mac OS X Server PDC (the server's LDAP directory) can be used to access the PDC server's shared folders, if any. The PDC user accounts can also be used to access shared folders on servers that are members of the Windows domain. In addition, user accounts defined in a server's local directory domain can be used to access shared folders on that server.

Shared folders reside in Mac OS X Server share points. Windows users can map network drives to share points on Mac OS X Server just like they map network drives to network folders on Windows NT servers.


My Computer
File
Edit
View
Favorites
Tools
Help
Network Drives
ravi on 'timpani\HomeDepot' (H:)
Public on 'Mac OS X (Timpani-w)' (P:)
Timpani_Shares on 'Mac OS X (Timpani-w)' (T:)
Projects on 'Timpani-w\Timpani_Shares' (W:)

Windows users can map network drives to Mac OS X Server share points

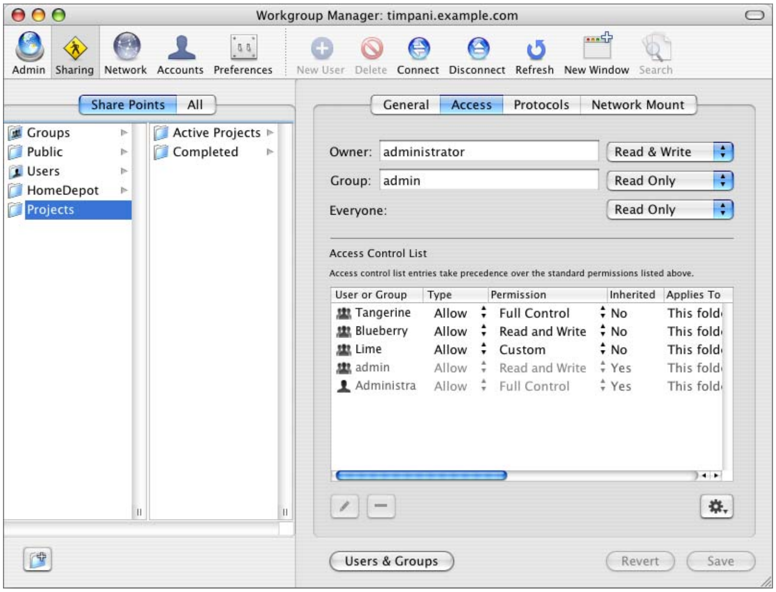
You can set up share points for the exclusive or nonexclusive use of Windows users. For example, you could set up a share point where Windows and Mac OS X users save shared graphics or word processing files that can be used on either platform. Conversely, you could set up a share point for SMB/CIFS access only, so that Windows users have a network location for files that can't be used on other platforms. The latter approach provides a single point of access for your Windows users and lets them take advantage of both opportunistic file locking (oplocks) and strict file locking.

In general, file locking prevents multiple clients from modifying the same information at the same time; a client locks the file or part of the file to gain exclusive access. Opportunistic locking grants exclusive access but also allows a client to cache its changes locally (on the client computer) for improved performance.

Important: Do not enable opportunistic locking, also known as *oplocks,* for a share point that's using any protocol other than SMB/CIFS.

You can control users' access to folders and files stored in Mac OS X Server share points by setting standard UNIX permissions (read, read and write, write, none) for owner, group, and everyone. For more flexible control, you can use access control lists (ACLs).

You can set standard UNIX permissions and an access control list (ACL) for a share point



Owner: administrator — Read & Write

Group: admin — Read Only

Everyone: — Read Only

Access Control List

Access control list entries take precedence over the standard permissions listed above.

User or Group	Type	Permission	Inherited	Applies To
Tangerine	Allow	Full Control	No	This fold
Blueberry	Allow	Read and Write	No	This fold
Lime	Allow	Custom	No	This fold
admin	Allow	Read and Write	Yes	This fold
Administra	Allow	Full Control	Yes	This fold

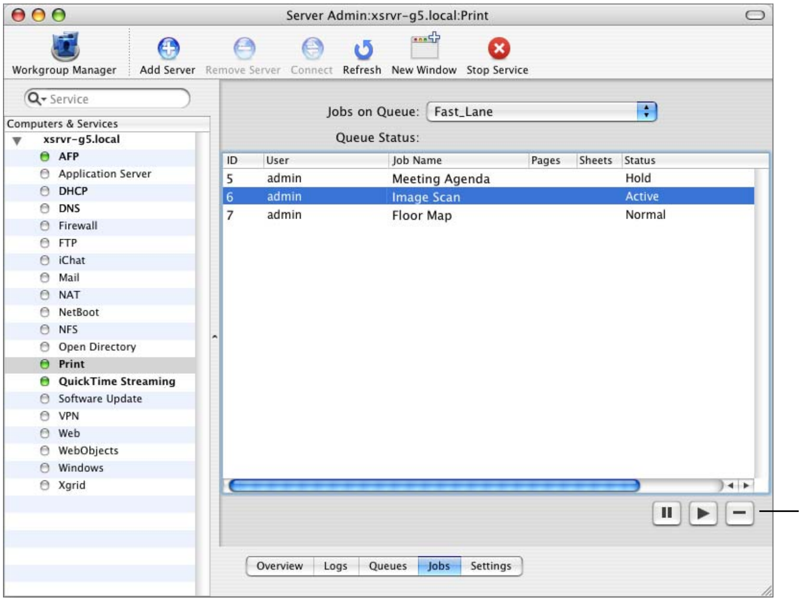
See the file services administration guide for additional information on share points and permissions.

Providing Print Service

Mac OS X Server print service helps you set up a managed printing environment on your network. You can share PostScript-compatible printers by setting up print queues for them on a server. When a user prints to a shared queue, the print job waits on the server until the printer is available or until established scheduling criteria are met.

For example, you can:

- Hold a job for printing at a later time
- Limit the number of pages individual users can print on specific printers
- Keep logs summarizing printer use



Jobs on Queue: Fast_Lane

Queue Status:

ID	User	Job Name	Pages	Sheets	Status
5	admin	Meeting Agenda			Hold
6	admin	Image Scan			Active
7	admin	Floor Map			Normal

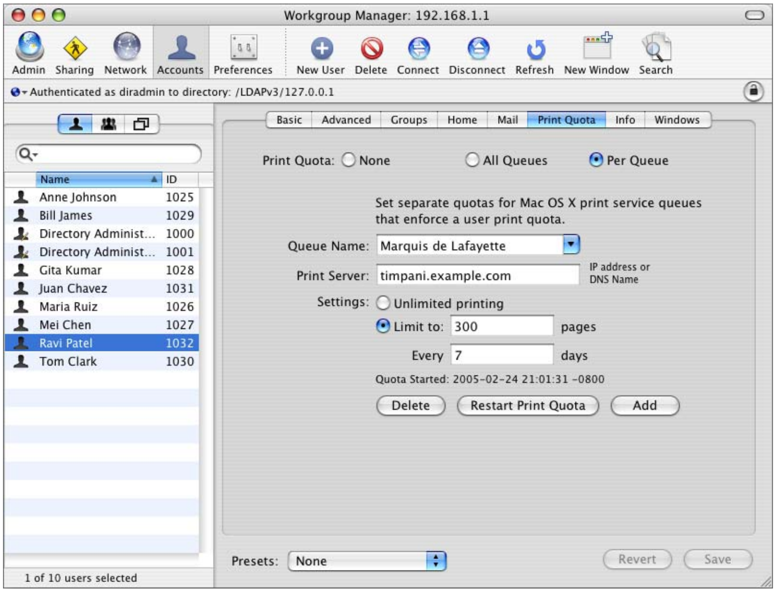
Manage print jobs for each print queue

Hold, start, or delete jobs

Mac OS X Server can make print queues available to Windows users via the standard Windows protocol for printer sharing, SMB/CIFS (abbreviated SMB). Printing to a Mac OS X Server print queue is like printing to any network printer in Windows. Installing a printer on a Windows computer requires computer administrator privileges. Users logged in using PDC user accounts can't install printers unless they're members of the local Administrators group (or the local Power Users group in Windows 2000).

To control the number of pages each user prints, you establish print quotas. A print quota sets how many pages a user can print during a specified time period. A user who reaches the print quota can't print again until the quota period ends. For each user, you set either a single quota that covers all print queues or individual quotas for each print queue.

Set a print quota for each user



Authenticated as diradmin to directory: /LDAPv3/127.0.0.1

Name	ID
Anne Johnson	1025
Bill James	1029
Directory Administ...	1000
Directory Administ...	1001
Gita Kumar	1028
Juan Chavez	1031
Maria Ruiz	1026
Mei Chen	1027
Ravi Patel	1032
Tom Clark	1030

1 of 10 users selected

Print Quota: ○ None ○ All Queues ● Per Queue

Set separate quotas for Mac OS X print service queues that enforce a user print quota.

Queue Name: Marquis de Lafayette

Print Server: timpani.example.com IP address or DNS Name

Settings: ○ Unlimited printing

● Limit to: 300 pages

Every 7 days

Quota Started: 2005-02-24 21:01:31 -0800

Presets: None

Configuring DNS

Some services of Mac OS X Server require or are easier to use with a properly configured DNS. In particular, Kerberos authentication requires a properly configured DNS. Although Mac OS X Server doesn't use Kerberos to authenticate Windows users for domain login, file service, or print service, Mac OS X Server can use Kerberos to authenticate Windows users for other services. In addition, Mac OS X Server can use Kerberos to authenticate Mac OS X users for login and file service. If you expect Mac OS X Server will provide services to Mac OS X users as well as Windows users, make sure your network's DNS is configured to resolve the server's name to its IP address and to resolve a reverse-lookup of the server's IP address to the server's name.

DNS can also be used as a fallback mechanism for name resolution by Windows workstations. Windows workstations initially try to discover the PDC via NetBIOS, so DNS is not required for Mac OS X Server to provide a PDC or other services to Windows users. However, Windows clients will fall back to DNS name resolution if they can't discover a server name via NetBIOS. So having DNS properly configured and enabled can be beneficial to Windows users.

Your DNS may be provided by Mac OS X Server or another server on your network. If you have an independent Internet service provider (ISP), it can also provide DNS. For information on configuring DNS in Mac OS X Server, see the network services administration guide.

Migrating Users, Groups, and Computers

2

Use the instructions in this chapter to transfer user and group accounts, computer records, and users' personal files from a Windows NT PDC to a Mac OS X Server PDC.

This chapter tells you what you can migrate, and then explains how.

Understanding What You Can Migrate

The instructions in "Step-by-Step Instructions" on page 22 describe how to reuse the following data from a Windows NT server with a Mac OS X Server PDC:

- User and group accounts
- Records for computers that are members of the NT domain
- Users' personal files from My Documents folders and home directory folders
- Roaming user profiles

To migrate user, group, and computer records, you must have a Mac OS X Server system that is or can be an Open Directory master.

Migrated users have the same home directory path after migration as before. During migration, each user's home directory path is copied to the Mac OS X Server user account. Users should be able to continue using their same home directories unless the home directories were on the Windows NT PDC server, which must be taken out of service after migration.

If some users have home directories on the Windows NT PDC server, they'll need to temporarily copy their home directory files to another location before you migrate their records to the Mac OS X Server PDC. These users can copy their home directory files to their My Documents folders if their client computers have sufficient disk space for all the copied files. Or the users can copy their files to a network folder that's not located on the PDC server.

You'll need to set up new home directories for these users on the Mac OS X Server PDC or a member server. After you migrate the users, they'll be able to copy files to their new home directories.

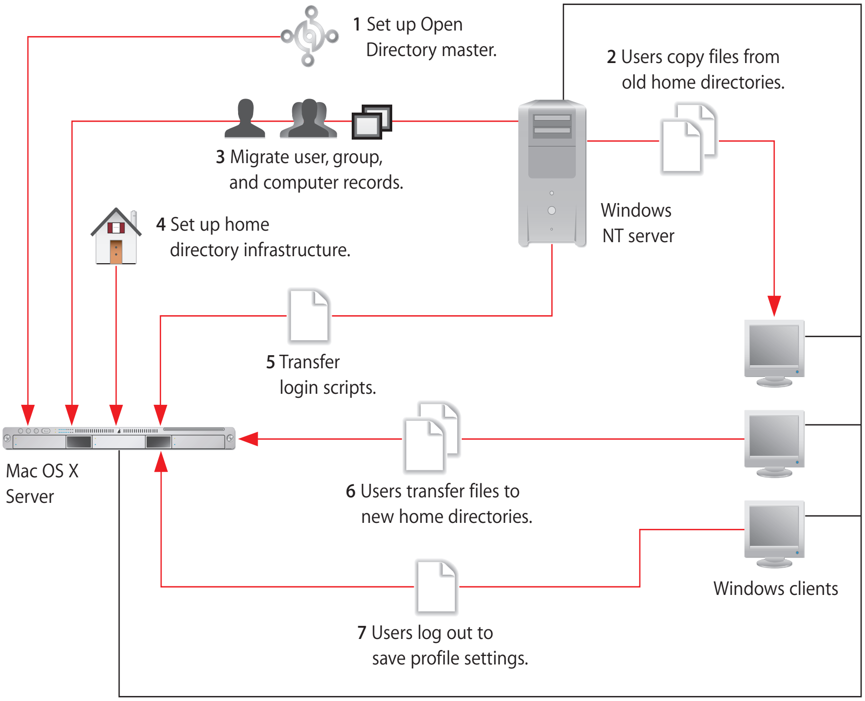
Tools You Can Use

To migrate users, groups, and computers, you use:

- Server Admin to make Mac OS X Server an Open Directory master and configure WINS service.
- The `ntdomainmigration.sh` command-line tool to set up Mac OS X Server as a PDC and migrate user, group, and computer information to it from the NT server.
- Workgroup Manager to edit migrated user and group accounts, set up network home directories, and configure roaming user profiles.
- Windows Explorer to copy users' files to their new home directories.

Step-by-Step Instructions

To migrate users, groups, and computers, follow the steps in this section. The following diagram summarizes the steps, and detailed instructions follow.


1 Set up Open Directory master.
2 Users copy files from old home directories.
3 Migrate user, group, and computer records.
Windows NT server
4 Set up home directory infrastructure.
5 Transfer login scripts.
Mac OS X Server
6 Users transfer files to new home directories.
Windows clients
7 Users log out to save profile settings.

Step 1: Set up an Open Directory master

You can set up an Open Directory master during the initial server setup that automatically follows installation of Mac OS X Server. If Mac OS X Server is already installed, you can use Server Admin to set up an Open Directory master.

When you set up an Open Directory master, Kerberos will start running only if the server is configured to use a DNS service that resolves the server's fully qualified DNS name and resolves a reverse-lookup of the server's IP address. Mac OS X Server doesn't use Kerberos authentication for Windows services, but can use Kerberos for other services. If you expect Mac OS X Server to provide services to Mac OS X users as well as Windows users, you should configure it so that Kerberos is running.

To make Mac OS X Server an Open Directory master:

1. If Mac OS X Server will use an existing DNS service, configure your network's DNS service to resolve the server's name and IP address and to resolve a reverse-lookup of the server's IP address to the server's name.

2. Install the Mac OS X Server v10.4 software if it isn't installed yet.

   See the getting started guide for installation instructions.

   If the Mac OS X Server software is already installed, skip this and the next step in this procedure, and go to step 4 on this page.

3. During the initial server setup that automatically follows installation, create an Open Directory master, but don't create a Windows primary domain controller (PDC) and don't set Windows file service to start automatically.

   - In the TCP/IP Settings pane, enter the IP addresses of one or more DNS servers that are configured to resolve the new server's name and IP address.

     If no DNS server is configured to resolve the new server's name and IP address, don't enter any DNS server address.

   - In the Directory Usage pane, choose Open Directory Master from the "Set directory usage to" pop-up menu. Do not select Enable Windows Primary Domain Controller. The server will become a PDC in Step 3, "Migrate users, groups, and computers to Mac OS X Server" on page 24.
   - In the Services pane, leave Windows file service turned off.

     You can turn on other services in this pane. If you don't turn on services now, you can turn them on later by using Server Admin.

4. If Mac OS X Server will provide its own DNS service, set it up and configure the server's Network preferences to use it.

   - For instructions on setting up the server's DNS service, see the network services administration guide.

- In the Network pane of System Preferences, make sure the server's IP address is the first address in the DNS Servers field for the primary network interface. For instructions, open System Preferences, choose Help > System Preferences Help, and search for "changing network settings."

5 Use Server Admin to confirm that the server is an Open Directory master and see whether Kerberos is running.

Open Server Admin, connect to the server, select Open Directory in the Computers & Services list, and click Overview.

- If Open Directory's Overview pane doesn't say the server is an Open Directory master, click Settings, click General, and choose Open Directory Master from the Role pop-up menu. For detailed instructions, see the Open Directory administration guide.
- If the Overview pane says Kerberos is stopped, you can start it now. Click Settings, click General, then click Kerberize. For detailed instructions on starting Kerberos after setting up an Open Directory master, see the Open Directory administration guide.

  Kerberos won't start if the server isn't configured to use a DNS server that resolves the server's fully qualified DNS name and resolves a reverse-lookup of the server's IP address.

6 Use Server Admin to make sure the authentication methods use by Windows services—NTLMv1, NTLMv2, and optionally LAN Manager—are enabled.

With Open Directory selected for the PDC server in Server Admin's Computers & Services list, click Policy, then click Security. Make sure "NTLMv1 and NTLMv2" is selected. Select other authentication methods needed by services and users of the server.

Step 2: Have users copy files from old home directories

Tell users who have home directories on the Windows NT server that's going out of service that they need to copy files from their home directories to their My Documents folders or a network folder that's staying in service. Later, these users will be able to copy their files to their new Mac OS X Server home directories.

Users who have home directories on Windows servers that are staying in service don't need to copy their home directory files anywhere. After you migrate these users to Mac OS X Server, they should still be able to access their home directories as before.

Step 3: Migrate users, groups, and computers to Mac OS X Server

Use the `ntdomainmigration.sh` command-line tool to migrate user, group, and computer information from the NT server. For migrated user and groups, the tool creates user accounts and group accounts in the LDAP directory of Mac OS X Server. For migrated computers, the tool creates computer records and adds them to the Windows Computers computer list in the LDAP directory. In addition, the tool sets up Mac OS X Server as a PDC and starts Windows services.

To use the `ntdomainmigration.sh` tool, you need to know the NT server's Windows domain, the name and password of an NT domain administrator, and the name and password of an LDAP directory administrator. If your network has an existing WINS server, you also need to know its IP address or DNS name.

When you run the `ntdomainmigration.sh` tool, it outputs information about migrated users, groups, computers. You can save this information if you want to keep a log of the migration.

To migrate users, groups, and computers, and make Mac OS X Server a PDC:

1 Configure Mac OS X Server to use your network's existing WINS server or to provide WINS service.

Open Server Admin, connect to the server, and select Windows in the Computers & Services list. Then click Settings, click Advanced, and do one of the following:

- If your network has an existing WINS server, select "Register with WINS server" and enter the IP address or DNS name of the WINS server.
- If your network doesn't have a WINS server, select "Enable WINS server."

You may not need to set up WINS service if Mac OS X Server is on the same subnet as the Windows NT server, but it does no harm.

2 Make sure that Windows service is stopped.

With Windows selected in Server Admin's Computers & Services list, click Overview. If the Overview pane reports Windows service is running, click Stop Service in the toolbar or choose Server > Stop Service.

3 Open Terminal, enter the following command (substituting as described in the following table), then press Return:

```
sudo /usr/sbin/ntdomainmigration.sh <ntdomain> <ntserver> <ntadmin>
   <diradmin>
```

For	Substitute
`<ntdomain>`	The NT server's Windows domain name
`<ntserver>`	The NT Server's NetBIOS name
`<ntadmin>`	The name of an NT domain user with administrator rights
`<diradmin>`	The name of an LDAP directory user account with directory administrator privileges

4 When prompted as follows, enter the root user's password, the password of the NT domain administrator you specified, then the password of the LDAP directory administrator you specified:

```
Password:
Enter NT Domain Administrator's password (<ntadmin>):
Enter LDAP Administrator's password (<diradmin>):
```

After the first prompt, you enter the root user's password. Usually it is the same as the the server administrator password entered during initial server setup.

In the second and third prompts, in place of `<ntadmin>` you see the NT domain administrator name you specified, and in place of `<diradmin>` you see the LDAP directory administrator name you specified.

5 After the `ntdomainmigration.sh` tool finishes, you can save a migration log by choosing File > Save Text As.

After you enter the three passwords, the `ntdomainmigration.sh` tool outputs information about the user, group, and computer records it migrates. When the tool finishes, it outputs "Successfully Migrated Domain." This is the information you can save as a migration log.

If errors occur during migration, the `ntdomainmigration.sh` tool writes them in the system log. To view the system log, open Server Admin, select the server in the Computers & Services list, click Logs, then choose System Log from the Show pop-up menu.

6 Optionally, use Workgroup Manger to edit the migrated user and group accounts.

You can now select migrated user or group accounts and edit account settings for the selected accounts. For example, you can:

- Select all the migrated user accounts and set password policy rules in the Advanced pane so that users are forced to change their passwords the next time they log in. Until migrated users reset their passwords, they work only with the NTLMv1, NTLMv2, and LAN Manager authentication methods that Windows services use. Migrated users' passwords must be reset to work with authentication methods that other services require.
- Add users to groups either in the Members pane for group accounts or in the Groups pane for user accounts.
- Select multiple user accounts and set up their email accounts in the Mail pane.
- Specify a share point for the selected users' network home directories, as described in the next step.

See the Open Directory administration guide for instructions on setting password policy and password security options. See the Windows services administration guide and the user management guide for other user and group task instructions.

7 Use Server Admin to start Windows service.

Open Server Admin, select Windows in the Computers & Services list, and click Overview. If Windows service is stopped, click Start Service in the toolbar or choose Server > Start Service.

8 Take the Windows NT PDC out of service.

Mac OS X Server is now the PDC for the Windows domain, and the domain shouldn't have two PDCs.

Step 4: Set up the home directory infrastructure

If some users had home directories on the Windows NT server that you took out of service, you need to set up Mac OS X Server home directories for them. If you wish, you can set up Mac OS X Server home directories for other migrated users as well. A user's home directory is mounted automatically when a user logs in with a Mac OS X Server user account. The home directory is mapped to a network drive, and you can specify the drive letter for each user.

There are two parts to setting up Mac OS X Server home directories for Windows users:

- Setting up one or more Mac OS X Server share points for home directories
- Specifying home directory settings—location and drive letter—for user accounts

The share point you set up for home directories can be the predefined /Users folder on the Mac OS X Server PDC. If you prefer to have user home directories on a different server or servers, you can create share points on other Mac OS X Server systems. A share point for a Windows home directory must be on a Windows domain member server or the PDC server and must be configured to use the SMB/CIFS protocol. See the Windows services administration guide for instructions on setting up a Mac OS X Server system as a Windows domain member.

If the share point will be used for both Windows and Mac OS X users' home directories, it must also use the AFP or NFS protocol and have a network mount record configured for home directories. For instructions on setting up Mac OS X home directories, see the chapter on home directories in the user management guide.

For an overview of share points, including a discussion of issues you may want to consider before creating them, see the share points chapter in the file services administration guide.

To set up a share point for Windows users' home directories:

1 Open Workgroup Manager and select an existing share point or set up a new share point for home directories.

- To use an existing share point, connect Workgroup Manager to the server on which the share point resides and click Sharing. Click Share Points and select the share point.
- To set up a new share point, connect Workgroup Manager to the server on which the share point resides and click Sharing. Click All and select the folder you want to serve as the home directory share point. If you want to create a new folder as a share point, click the New Folder button (folder icon with +), enter the folder name, and click OK. Next, select "Share this item and its contents" in the General pane and click Save.

  Note: Don't use a slash (/) in the name of a folder or volume you plan to share. Users trying to access the share point might have trouble seeing it.

2 With the home directory share point selected in Workgroup Manager, click Access, set the selected share point's access control list (ACL) permissions and standard UNIX privileges as desired, then click Save.

- To change the owner or group of the share point, type a name or drag a name from the Users & Groups drawer.
- To open the Users & Groups drawer, click Users & Groups.

  If you don't see a recently created user or group, click Refresh. To change the autorefresh interval, choose Workgroup Manager > Preferences.

- Use the pop-up menus next to the fields to change the permissions for Owner, Group, and Everyone.

  Everyone is any user who can log in to the file server: registered users and guests, alike.

- To add an entry to the ACL, drag a name from the Users & Groups drawer.
- To change an entry in the ACL, select it, click the Edit button (pencil shaped), and change permission settings.

  You can also change an entry's type and permission level by choosing from the pop-up menus in the Type and Permission columns of the ACL.

- To remove an entry from the ACL, select it and click the Delete button (–).
- To apply all ACL permissions or selected UNIX privileges of a share point to all files and folders it contains, select the share point or folder, choose Propagate Permissions from the Action menu, then select what you want to propagate and click OK.

  This overrides access privileges that other users may have set for the affected files and folders.

The usual UNIX privileges for a share point containing home directories are: Owner is the primary server administrator and has Read & Write permissions; Group is "admin" and has Read & Write permissions; and Everyone has Read Only permission. See the file services administration guide for more information on ACLs and UNIX privileges.

3 Click Protocols, configure settings for Windows and other protocols, then click Save.

- Choose Windows File Settings from the pop-up menu, make sure "Share this item using SMB" is selected, and configure the other settings as desired.

  Important: If Mac OS or UNIX users will also access the share point, make sure "Enable strict locking" is selected.

- Use the pop-up menu at the top of the Protocols pane to configure settings for other file sharing protocols.

See the Windows services administration guide for more information and detailed instructions on Windows file settings. See the file services administration guide for information and instructions on Apple file settings, FTP settings, and NFS export settings.

4 If the share point will be used for Mac OS X home directories as well as Windows home directories, set up the share point to mount automatically on client computers.

With the share point selected in Workgroup Manager, click Network Mount. Choose the PDC server's LDAP directory from the Where pop-up menu. Click the lock to the right of this pop-up menu and authenticate as an administrator of the LDAP directory. Select "Enable network mounting of this share point." Choose AFP or NFS from the Protocol pop-up menu. Select "Use For User Home Directories" and click Save.

To specify a location and drive letter for Windows users' home directories:

1 In Workgroup Manager, select the user accounts for which you want to set up a home directory.

To select user accounts, click the Accounts button, and then click the small globe icon below the toolbar and open the PDC's LDAP directory. To edit the home directory information, click the lock to authenticate as an LDAP directory domain administrator. Then select one or more users in the user list.

2 If you want to use the same network home directory for Windows as for Mac OS X, click Home and specify the share point to use.

In the share points list, select /Users or the share point you want to use, then click Create Home Now.

If the share point you want to use isn't listed, click the Add (+) button, and enter the URL of the share point and the path to the user's home directory in the share point.

If you want to specify the /Users share point but it isn't listed, click the Add (+) button, and enter the path to the user's home directory in the Home field. Enter the path as follows:

/Users/*usershortname*

For *usershortname*, substitute the first short name of the user account you're configuring.

3 Click Windows, enter the home directory location in the Path field, choose a drive letter from the Hard Drive pop-up menu, then click Save.

- Leave Path blank to use the same home directory for Windows login and Mac OS X login. You can also specify this home directory by entering a UNC path that doesn't include a share point:

  \\*servername**usershortname*

  For *servername,* substitute the NetBIOS name of the PDC server or a Windows domain member server where the share point is located.

  For *usershortname*, substitute the first short name of the user account you're configuring.

- To specify a different SMB/CIFS share point, enter a UNC path that includes the share point:

\\servername\sharename\usershortname

For *sharename*, substitute the name of the share point.

- The default drive letter is H. Windows uses the drive letter to identify the mounted home directory.

4 If the Path field isn't blank, make sure the specified share point contains a folder for the user's home directory.

The folder's name must match the user's first short name, and the user must have read and write permission for the folder.

If the Path field is blank, the home directory share point doesn't have to contain a home directory folder for the user. In this case, Mac OS X Server will automatically create a home directory folder in the share point specified in the Home pane.

Step 5: Transfer login scripts to Mac OS X Server

If users have login scripts on the Windows NT server, you can copy them to the Mac OS X Server PDC and configure user accounts to use them. You can copy the scripts across your network or use a removable disk such as a CD-R disc or USB drive. On the Mac OS X Server PDC, user login scripts reside in the /etc/netlogon/ folder.

To copy login scripts to the Mac OS X Server PDC over the network:

1 On a Windows computer from which you can access both the NT server and a Mac OS X Server share point where you can copy files, open the folder containing the scripts you want to copy.

2 Connect to the Mac OS X Server share point and map a network drive to the share point.

For detailed instructions on mapping a network drive, see the onscreen help in Windows.

3 Copy scripts to the mapped Mac OS X Server share point.

4 Log in to the Mac OS X Server PDC using the root user name and password, open the share point folder to which you copied scripts, and copy the scripts to the /etc/netlogon/ folder.

The root user name is "root" or "System Administrator" and the password is initially the same as the password given to the first administrator account when it was created.

If you're copying scripts in the Finder, you can open /etc/netlogon/ by choosing Go > Go to Folder, entering /etc/netlogon/, and clicking Go.

5 Log out, then log in using the name and password of a server administrator.

6 In Workgroup Manager, select each Windows PDC user account and make sure the location of the user's login script is correctly specified in the Windows pane.

The Login Script field should contain the relative path to a login script located in /etc/netlogon/. For example, if you've copied a script named setup.bat into /etc/netlogon/, the Login Script field should contain setup.bat.

Step 6: Users can transfer files to Mac OS X Server home directories

Users who backed up files from the old Windows NT server (in Step 2 on page 24) can now copy those files to the Mac OS X Server home directories you set up for them (in Step 4 on page 27). When each of these users logs in using a Mac OS X Server PDC user account, the user's home directory will be mapped to a network drive automatically. The user can then copy files from the My Documents folder and from network folders. After successfully copying these files to the home directory, the user can delete them from their previous locations.

Users should generally keep large files in their network home directories instead of their My Documents folders. The larger the My Documents folder is, the longer it takes to synchronize when logging in to and logging out of the domain. But users who need access to files while disconnected from the network shouldn't keep those files in their network home directories.

Step 7: Users log out to update their roaming profiles

Roaming profiles that were stored on the old Windows NT PDC server are migrated individually when migrated users log out of the Mac OS X Server PDC's Windows domain. Roaming profiles aren't migrated en masse from the old PDC to the new PDC.

The first time each user logs in to the new PDC, the Windows workstation won't be able to load the roaming profile from the old PDC because it's now out of service. In this case, Windows uses the local copy of the user profile stored on the Windows workstation. When the user logs out, Windows saves the profile settings and contents of the My Documents folder on the Mac OS X Server PDC server. From then on, Windows should be able to load the roaming profile when the user logs in to the Mac OS X Server PDC's Windows domain.

If you want to have roaming profiles stored on a server other than the Mac OS X Server PDC, you can specify the profile path for each user in the Windows pane of Workgroup Manager. See the Windows services administration guide for instructions.

Migrating Windows File Service

3

Use the instructions in this chapter if you need to transfer the contents of network folders on a Windows NT server to share points on Mac OS X Server systems.

You set up Mac OS X Server file service by designating folders on the server as share points and putting files for Windows users into the share point folders. You can set ACLs and standard UNIX privileges to control the kind of access users have to share points and folders. Then Windows users can map network drives to Mac OS X Server share points and access their contents.

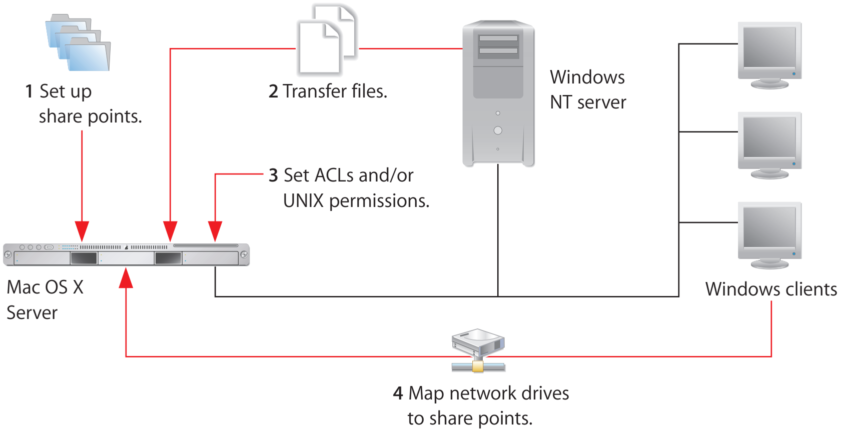
Tools You Can Use

To migrate file service, you use:

- Workgroup Manager to create share points and shared folders, and to set ACLs and UNIX privileges for them.
- Windows Explorer to copy shared files and map network drives to Mac OS X Server share points.

Step-by-Step Instructions

To migrate Windows file service, follow the steps in this section. The following diagram summarizes the steps, and detailed instructions follow.



Step 1: Set up SMB/CIFS share points in Mac OS X Server

You use Workgroup Manager to set up share points for folders and volumes (including disks, disk partitions, CDs, and DVDs) that you want Windows users to share.

- If you have set up a Mac OS X Server PDC, you may have set up share points for home directories and roaming user profiles or used the defaults. You can set up additional share points on Windows domain member servers or on the PDC itself.
- If you don't have a PDC, you can set up share points on a Mac OS X Server system configured for standalone Windows services.
- Share points that you set up on a standalone server, domain member server, or PDC server can be for the exclusive or nonexclusive use of Windows users.

For additional information on file locking and other Windows share point settings, see the chapter that covers share points in the Windows services administration guide. For an overview of share points, including a discussion of ACLs and standard UNIX privileges, see the file services administration guide.

To create an SMB/CIFS share point and control access to it:

1. Open Workgroup Manager, connect to the server that will host the share point, and click Sharing.
2. If you want to set ACL permissions for the new share point or folders in it, make sure ACLs are enabled for the volume on which the share point is located.

   To enable ACLs for a volume, click All, select the volume, select "Enable Access Control Lists on this volume," and click Save.
3. Click All and select the folder or volume you want to share.

If you want to create a folder to use as a share point, click the New Folder button (folder icon with +), enter the folder name, and click OK.

Note: Don't use a slash (/) in the name of a folder or volume you plan to share. Users trying to access the share point might have trouble seeing it.

4 Click General, then select "Share this item and its contents."

5 To control who has access to the share point, click Access and set ACL permissions, standard UNIX privileges, or both.

- To change the owner or group of the share point, type a name or drag a name from the Users & Groups drawer.
- To open the Users & Groups drawer, click Users & Groups.

  If you don't see a user or group you recently created, click Refresh. To change the autorefresh interval, choose Workgroup Manager > Preferences.

- Use the pop-up menus next to the fields to change the permissions for Owner, Group, and Everyone.

  Everyone is any user who can log in to the file server: registered users and guests, alike.

- To add an entry to the ACL, drag a name from the Users & Groups drawer.
- To change an entry in the ACL, select it, click the Edit button (pencil shaped), and change permission settings.

  You can also change an entry's type and permission level by choosing from the pop-up menus in the Type and Permission columns of the ACL.

- To remove an entry from the ACL, select it and click the Delete button (–).
- To apply all ACL permissions or selected UNIX privileges of a share point to all files and folders it contains, select the share point or folder, choose Propagate Permissions from the Action menu, then select what you want to propagate and click OK.

  This overrides access privileges that other users may have set for the affected files and folders.

If you want to assign permissions to a user or group account that doesn't exist, you can create the user or group account now in a new Workgroup Manager window. For instructions, see the user management guide.

6 Click Save, then click Protocols (on the right) and choose Windows File Settings from the pop-up menu.

7 Select "Share this item using SMB."

8 To allow unregistered users access to the share point, select "Allow SMB guest access."

For greater security, don't select this item.

9 To change the name that clients see when they browse for and connect to the share point using SMB/CIFS, type a new name in the "Custom SMB name" field.

Changing the custom name doesn't affect the name of the share point itself, only the name that SMB/CIFS clients see.

10 Select the type of locking for this share point.

- To allow clients to use opportunistic file locking, select "Enable oplocks."

  Important: Do not enable oplocks for a share point that's using any protocol other than SMB/CIFS. For more information on oplocks, see the Windows services administration guide.

- To have clients use standard locks on server files, select "Enable strict locking."

11 Choose a method for assigning default UNIX access permissions for new files and folders in the share point.

- To have new items adopt the permissions of the enclosing item, select "Inherit permissions from parent."
- To assign specific permissions, select "Assign as follows" and set the Owner, Group, and Everyone permissions using the pop-up menus.

12 To prevent AFP access to the new share point, choose Apple File Settings from the pop-up menu and deselect "Share this item using AFP."

13 To prevent FTP access to the new share point, choose FTP Settings from the pop-up menu and deselect "Share this item using FTP."

14 To prevent NFS access to the new share point, choose NFS Export Settings from the pop-up menu and deselect "Export this item and its contents to."

15 Click Save.

16 Make sure Windows service is running.

Open Server Admin, select Windows in the Computers & Services list, and click Overview. If Windows service is stopped, click Start Service in the toolbar or choose Server > Start Service.

Step 2: Transfer files from Windows NT to Mac OS X Server share points

After you set up Mac OS X Server share points, you can move files to them from network folders on the Windows server. Use any computer that can connect to both the Windows network folders and the Mac OS X Server share points. Windows users can also copy their own files to share points to which they have read/write access.

When connecting to each share point, use the name and password of a Mac OS X Server user account that has read/write access to the folders into which you're going to copy files.

Default permissions that you set up earlier for a share point (in Step 1, "Set up SMB/CIFS share points in Mac OS X Server") are assigned to folders you copy into the share point.

Step 3: Control access to copied files and folders

You may want to set ACLs on folders or change the UNIX privileges assigned by default to some files and folders that you copied from Windows NT network folders to Mac OS X Server share points. You can set ACLs or assign UNIX privileges to restrict access to folders owned by users. For example, you can give a user read and write access to a folder but give everyone else only write access, thereby creating a drop box.

You can also set ACLs to give certain groups more access to a folder. For example, you can give one group read and write access, another group read-only access, and everyone else no access. You can assign UNIX privileges to give one group more access than everyone else.

See the file services administration guide for additional information on ACLs and UNIX privileges.

To set ACL permissions or UNIX privileges on copied folders or files:

1. Open Workgroup Manager, connect to the server on which the copied folders or files are located, and click Sharing.

2. Make sure ACLs are enabled for the volume on which the copied folders or files are located.

   To enable ACLs for a volume, click All, select the volume, select "Enable Access Control Lists on this volume," and click Save.

3. Click Share Points, select the share point that contains a folder or file whose permissions you want to set, then navigate to and select the folder or file.

4. Change the standard UNIX access privileges as desired.

   - To change the owner or group of the shared item, type a name or drag a name from the Users & Groups drawer.

     To open the drawer, click Users & Groups. If you don't see a recently created user or group, click Refresh. To change the autorefresh interval, choose Workgroup Manager > Preferences.

   - Use the pop-up menus next to the fields to change the permissions for Owner, Group, and Everyone.

     Everyone is any user who can log in to the file server: registered users and guests, alike.

5. Change the ACL permissions as desired.

   Note: You can't explicitly configure ACL permissions for files. However, because files can inherit ACL permissions from their parent folder, you can set permissions for files by setting them for the parent folder and propagating them to descendant files.

   - To add an entry to the ACL, drag a name from the Users & Groups drawer.

- To change an entry in the ACL, select it, click the Edit button (pencil shaped), and change permission settings. You can also change an entry's type and permission level by choosing from the pop-up menus in the Type and Permission columns of the ACL.
- To remove an entry from the ACL, select it and click the Delete button (–).
- To remove a selected folder's inherited entries, choose "Remove inherited entries" from the Action menu.
- To make a selected folder's inherited entries explicit so you can edit them, choose "Make inherited entries explicit" from the Action menu.
- To apply ACL inheritance to a selected file, choose "Apply inheritance to selected file" from the Action menu.
- To remove a selected file's ACL, choose "Remove access control list" from the Action menu.

6 (Optional) To apply all ACL permissions or selected UNIX privileges of a share point or folder to all files and folders it contains, select the share point or folder, choose Propagate Permissions from the Action menu, then select what you want to propagate and click OK.

This overrides access privileges that other users may have set for the affected files and folders.

7 Click Save.

Step 4: Users can map networked drives to share points

Windows users can now connect to Mac OS X Server share points, which they see as network folders, and map network drives to these share points. For basic instructions on mapping a network drive, see the onscreen help in Windows.

The user's login name and password are used by default to authenticate the connection to a Mac OS X Server share point. If the user did not log in to Windows with the name and password of a Mac OS X Server user account, the user can click "Connect using a different user name" in the Map Network Drive dialog and enter the name and password of a Mac OS X Server user account.

You can add user accounts for Windows users who don't have them yet by using Workgroup Manager. See the Windows services administration guide for instructions.

Providing Windows Access to Print Service

4

Use the instructions in this chapter if you need to set up access to Mac OS X Server print queues from Windows workstations.

You set up print service for Windows users by setting up print queues to use the SMB/CIFS protocol. Then users can use the Add Printer wizard to install (connect to) the print queues as network printers on their Windows computers. Users will see these queues as printers.

Installing a print queue on a Windows computer requires a user account that's a member of the computer's Administrators group or Power Users group (Windows 2000). PDC user accounts aren't members of these local accounts by default.

If you want to limit the number of pages that some users print, you can set print quotas on their user accounts.

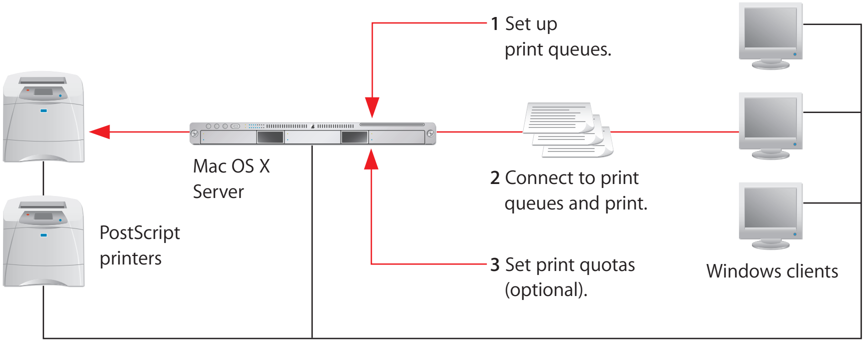
Tools You Can Use

To provide Windows access to print service, you can use:

- Server Admin to configure print queues for Windows access and print quota enforcement
- The Add Printer wizard on each Windows workstation to add print queues as printers
- Workgroup Manager to set print quotas for users (optional)

Step-by-Step Instructions

To give Windows users access to Mac OS X Server print queues, follow the steps in this section. The following diagram summarizes the steps, and detailed instructions follow it.



Step 1: Set Up SMB/CIFS print queues in Mac OS X Server

Use Server Admin to create queues on the server for your network PostScript printers, make the queues available to Windows users, and start print service on the server.

To set up a shared print queue for SMB/CIFS access:

1. In Server Admin, select Print in the Computers & Services list.

2. Click Settings, then click Queues.

   If you don't see the Queues button at the top of the Settings pane, you might already be looking at a queue's settings. Click the Back button (the left-pointing arrow in the upper right).

3. Select an existing queue that you want to make available to Windows users and click the Edit (pencil-shaped) button, or click the Add (+) button to create a new queue.

   In the dialog for creating a new queue for a printer, choose the printer's protocol from the pop-up menu at the top of the dialog, then specify the printer.

   - For an AppleTalk or Open Directory printer, select the printer in the list and click OK.
   - For an LPR printer, type the printer IP address or DNS name and click OK. (If you don't want to use the server's default print queue, deselect "Use default queue on server" and type a queue name.)

4. In the queue-editing pane, make sure the Sharing Name field complies with SMB/CIFS naming rules.

   For the SMB/CIFS protocol, Sharing Name must be 15 characters or fewer and must not contain characters other than A–Z, a–z, 0–9, and _ (underscore). Some Windows clients limit the name to 12 characters.

Sharing Name is the queue name, which users see as the name of a printer. Changing Sharing Name does not affect the printer's name on the server, which is shown above Sharing Name. You can edit the printer's name, kind (model), and location by using the Printer Setup Utility (in the /Applications/Utilities folder of Mac OS X Server).

To avoid conflicts, make sure Sharing Name is not the same as any SMB/CIFS share point name.

5 Select "SMB" and any other protocols used by client computers.

Windows computers can use SMB (that is, SMB/CIFS). Windows 2000 and Windows XP computers can use SMB or LPR.

Mac OS X and Mac OS 9 computers can use AppleTalk or LPR.

6 Select "Enforce quotas for this queue" if you want to enforce the print quotas you establish for users in Workgroup Manager.

7 Click Save, then click the Back button (in the upper right).

8 If print service is not running, click Start Service in the toolbar or choose File > Start Service.

9 Make sure Windows service is running.

Select Windows in the Computers & Services list and click Overview. If Windows service is stopped, click Start Service in the toolbar or choose Server > Start Service.

Step 2: Windows clients can connect to Mac OS X Server print queues

Windows users can now add connections to Mac OS X Server print queues by using the Add Printer wizard. On a Windows XP computer, adding a connection to a print queue requires logging in with a user account that's a member of the computer's Administrators group. On a Windows 2000 computer, adding a connection to a print queue requires logging in with a user account that's a member of the computer's Administrators group or Power Users group. PDC user accounts aren't members of these groups by default. For instructions on adding users to local group accounts, see the onscreen help on computer management in Windows. For basic instructions on connecting to network printers, see the onscreen help in Windows.

Step 3: Set print quotas and print quota enforcement (optional)

There are two parts to establishing print quotas:

- Specifying the quota and time period for each user using Workgroup Manager
- Setting print service to enforce quotas for individual queues using Server Admin

To set the print quota for one or more users:

1. In Workgroup Manager, select the user accounts for which you want to set up a home directory.

   To select user accounts, click the Accounts button, and then click the small globe icon below the toolbar and open the PDC's LDAP directory. To change print quota settings, click the lock to authenticate as an LDAP directory domain administrator. Then select one or more users in the user list.

2. Click Print Quota and select one of the Print Quota options.

   - To set one quota for all queues, select All Queues, then type the number of pages and the number of days after which the quota is reset.
   - To set a quota for a particular queue, select Per Queue, choose the queue from the pop-up list, and type the quota and quota period.

     If the queue is not in the list, click Add and change "untitled" to the queue name. Then choose the queue from the pop-up list, type the IP address or DNS name of the server hosting the queue, and type the user's page quota and quota period.

3. Click Save.

The quotas are not enforced until you turn on quota enforcement for specific queues in print service using Server Admin.

To enforce quotas for a print queue:

1. In Server Admin, select Print in the Computers & Services list.

2. Click Settings, then click Queues.

   If you don't see the Queues button at the top of the Settings pane, you might already be looking at a queue's settings. Click the Back button (the left-pointing arrow in the upper right).

3. Select a queue in the list and click the Edit (pencil-shaped) button.

4. Select "Enforce quotas for this queue."

5. Click Save, then click the Back button (in the upper right).

Glossary

access control list See **ACL**.

access privileges See **permissions**.

ACL Access Control List. A list maintained by a system that defines the rights of users and groups to access resources on the system.

Active Directory The directory and authentication service of Microsoft Windows 2000 Server and Windows Server 2003.

administrator A user with server or directory domain administration privileges. Administrators are always members of the predefined "admin" group.

administrator computer A Mac OS X computer onto which you've installed the server administration applications from the Mac OS X Server Admin CD.

AFP Apple Filing Protocol. A client/server protocol used by Apple file service on Macintosh-compatible computers to share files and network services. AFP uses TCP/IP and other protocols to communicate between computers on a network.

attribute A named data item containing a specific type of information and belonging to an entry (record or object) in a directory domain. The actual data that an attribute contains is its value.

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.

back up (verb) The act of creating a backup.

backup (noun) A collection of data that's stored for purposes of recovery in case the original copy of data is lost or becomes inaccessible.

BSD Berkeley System Distribution. A version of UNIX on which Mac OS X software is based.

character A synonym for byte.

chatting See **instant messaging**.

CIFS Common Internet File System. See **SMB/CIFS**.

client A computer (or a user of the computer) that requests data or services from another computer, or server.

code page Defines extensions to the character set for Microsoft Windows. The base character set, defined by the American Standard Code for Information Interchange (ASCII), maps letters of the Latin alphabet, numerals, punctuation, and control characters to the numbers 0 through 127. The code page maps additional characters, such as accented letters for a particular language and symbols, to the numbers 128 through 255.

command line The text you type at a shell prompt when using a command-line interface.

command-line interface A way of interfacing with the computer (for example, to run programs or modify file system permissions) by entering text commands at a shell prompt.

computer account See **computer list**.

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

cracker A malicious user who tries to gain unauthorized access to a computer system in order to disrupt computers and networks or steal information. Compare to hacker.

crypt password A type of password that's stored as a hash (using the standard UNIX encryption algorithm) directly in a user record.

default The automatic action performed by a program unless the user chooses otherwise.

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 services Services that provide system software and applications with uniform access to directory domains and other sources of information about users and resources.

DNS Domain Name System. A distributed database that maps IP addresses to domain names. A DNS server, also known as a name server, keeps a list of names and the IP addresses associated with each name.

DNS domain A unique name of a computer used in the Domain Name System to translate IP addresses and names. Also called a domain name.

DNS name A unique name of a computer used in the Domain Name System to translate IP addresses and names. Also called a domain name.

domain Part of the domain name of a computer on the Internet. It does not include the Top Level Domain designator (for example, .com, .net, .us, .uk). Domain name "www.example.com" consists of the subdomain or host name "www," the domain "example," and the top level domain "com."

drive letter A letter of the alphabet by which a disk or disk partition is identified in the Windows operating system.

encryption The process of obscuring data, making it unreadable without special knowledge. Usually done for secrecy and confidential communications.

file server A computer that serves files to clients. A file server may be a general-purpose computer that's capable of hosting additional applications or a computer capable only of serving files.

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

guest user A user who can log in to your server without a user name or password.

hacker An individual who enjoys programming, and explores ways to program new features and expand the capabilities of a computer system. See also **cracker**.

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.

instant messaging Live interactions in which two or more computer users exchange text messages, pictures, audio, or video in real time. Often called chatting because of its spontaneous, conversation-like qualities.

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.

KDC Kerberos Key Distribution Center. A trusted server that issues Kerberos tickets.

Kerberos A secure network authentication system. Kerberos uses tickets, which are issued for a specific user, service, and period of time. Once a user is authenticated, it's possible to access additional services without retyping a password (this is called single sign-on) for services that have been configured to take Kerberos tickets. Mac OS X Server uses Kerberos v5.

Kerberos Key Distribution Center See **KDC**.

Kerberos realm The authentication domain comprising the users and services that are registered with the same Kerberos server. The registered services and users trust the Kerberos server to verify each other's identities.

LDAP Lightweight Directory Access Protocol. A standard client-server protocol for accessing a directory domain.

local directory domain A directory of identification, authentication, authorization, and other administrative data that's accessible only on the computer where it resides. The local directory domain isn't accessible from other computers on the network.

log in (verb) The act of starting a session with a system (often by authenticating as a user with an account on the system) in order to obtain services or access files. Note that logging in is separate from connecting, which merely entails establishing a physical link with the system.

mount (verb) In general, to make a remote directory or volume available for access on a local system. In Xsan, to cause an Xsan volume to appear on a client's desktop, just like a local disk.

name server A server on a network that keeps a list of names and the IP addresses associated with each name. See also **DNS**, **WINS**.

nested group A group that is a member of another group. Nested groups enable administrators to manage groups of users at a global level (to influence all members of a group) and at a smaller level (to influence only certain members of a group).

NetBIOS Network Basic Input/Output System. A program that allows applications on different computers to communicate within a local area network.

NetInfo One of the Apple protocols for accessing a directory domain.

Network File System See **NFS**.

network interface Your computer's hardware connection to a network. This includes (but isn't limited to) Ethernet connections, AirPort cards, and FireWire connections.

NFS Network File System. A client/server protocol that uses Internet Protocol (IP) to allow remote users to access files as though they were local. NFS exports shared volumes to computers according to IP address, rather than user name and password.

Open Directory The Apple directory services architecture, which can access authoritative information about users and network resources from directory domains that use LDAP, NetInfo, or Active Directory protocols; BSD configuration files; and network services.

Open Directory master A server that provides LDAP directory service, Kerberos authentication service, and Open Directory Password Server.

Open Directory password A password that's stored in secure databases on the server and can be authenticated using Open Directory Password Server or Kerberos (if Kerberos is available).

Open Directory Password Server An authentication service that validates passwords using a variety of conventional authentication methods required by the different services of Mac OS X Server. The authentication methods include APOP, CRAM-MD5, DHX, LAN Manager, NTLMv1, NTLMv2, and WebDAV-Digest.

open source A term for the cooperative development of software by the Internet community. The basic principle is to involve as many people as possible in writing and debugging code by publishing the source code and encouraging the formation of a large community of developers who will submit modifications and enhancements.

oplocks See **opportunistic locking**.

opportunistic locking Also known as oplocks. A feature of Windows services that prevents users of shared files from changing the same file at the same time. Opportunistic locking locks the file or part of the file for exclusive use, but also caches the user's changes locally on the client computer for improved performance.

owner The owner of an item can change access permissions to the item. The owner may also change the group entry to any group in which the owner is a member. By default the owner has Read & Write permissions.

password An alphanumeric string used to authenticate the identity of a user or to authorize access to files or services.

password policy A set of rules that regulate the composition and validity of a user's password.

Password Server See **Open Directory Password Server**.

pathname The location of an item within a file system, represented as a series of names separated by slashes (/).

PDC Primary domain controller. In Windows networking, a domain controller that has been designated as the primary authentication server for its domain.

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

print queue An orderly waiting area where print jobs wait until a printer is available. The print service in Mac OS X Server uses print queues on the server to facilitate management.

privileges The right to access restricted areas of a system or perform certain tasks (such as management tasks) in the system.

protocol A set of rules that determines how data is sent back and forth between two applications.

replication The creation of duplicate copies of a directory domain in order to improve performance or ensure uninterrupted network services in the event of a system failure.

roaming user profiles The set of personal desktop and preference settings that a user makes, the Windows domain controller stores on a server, and Windows applies when the user logs in to the Windows domain from any workstation.

Samba Open source software that provides file, print, authentication, authorization, name resolution, and network service browsing to Windows clients using the SMB/CIFS protocol.

SASL Simple Authentication and Security Layer. An extensible authentication scheme that allows the Open Directory Password Server to support a variety of network user authentication methods required by the different services of Mac OS X Server.

security identifier See **SID**.

Server Message Block/Common Internet File System See **SMB/CIFS**.

shadow password A password that's stored in a secure file on the server and can be authenticated using a variety of conventional authentication methods required by the different services of Mac OS X Server. The authentication methods include APOP, CRAM-MD5, DHX, LAN Manager, NTLMv1, NTLMv2, and WebDAV-Digest.

share point A folder, hard disk (or hard disk partition), or CD that's accessible over the network. A share point is the point of access at the top level of a group of shared items. Share points can be shared using AFP, Windows SMB, NFS (an "export"), or FTP protocols.

SID Security Identifier. A unique value that identifies a user, group, or computer account in a Windows NT-compatible domain.

SMB/CIFS Server Message Block/Common Internet File System. A protocol that allows client computers to access files and network services. It can be used over TCP/IP, the Internet, and other network protocols. Windows services use SMB/CIFS to provide access to servers, printers, and other network resources.

standalone server A server that provides services on a network but doesn't get directory services from another server or provide directory services to other computers.

strict locking A feature of Windows services that prevents users of shared files from changing the same file at the same time. With strict locking, the Windows server checks whether a file is locked and enforces file locks, rather than relying on the client application to do so.

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.

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.

user profile The set of personal desktop and preference settings that Windows saves for a user and applies each time the user logs in.

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.

weblog A webpage that hosts chronologically ordered entries. It functions as an electronic journal or newsletter. Weblog service lets you create weblogs that are owned by individual users or by all members of a group.

Weblog service The Mac OS X Server service that lets users and groups securely create and use weblogs. Weblog service uses Open Directory authentication to verify the identity of weblog authors and readers. If accessed using a website that's SSL enabled, Weblog service uses SSL encryption to further safeguard access to weblogs.

Windows domain The Windows computers on a network that share a common directory of user, group, and computer accounts for authentication and authorization. An Open Directory master can provide the directory services for a Windows domain.

WINS Windows Internet Naming Service. A name resolution service used by Windows computers to match client names with IP addresses. A WINS server can be located on the local network or externally on the Internet.

workgroup A set of users for whom you define preferences and privileges as a group. Any preferences you define for a group are stored in the group account.

Index