



# The Mac OS X Server Essentials v10.5 Exam Skills Assessment Guide

## To Register

This exam is offered at Apple Authorized Training Centers and Prometric Testing Centers worldwide. For information on exam registration, please visit [training.apple.com/certification](http://training.apple.com/certification).

To learn more about Apple training offerings that can help you prepare for certification, please visit [training.apple.com](http://training.apple.com).

The Mac OS X Server Essentials v10.5 Exam (Prometric exam no. 9L0-509) is a computer-based test offered at Apple Authorized Training Centers and Prometric Testing Centers.

The exam is one of two required exams in the Apple Certified Technical Coordinator (ACTC) 10.5 certification track. You must pass this exam and the Mac OS X Support Essentials v10.5 Exam to become an ACTC.

You may take up to two hours to complete the exam, which consists of 90 multiple-choice questions that are based on the objectives listed in this guide.

The score required to pass is 69 percent. Eight demographic questions are presented but are not scored.

To prepare for the exam, read through the objectives in this guide to determine which areas you need to review. The primary reference source for this exam is the book: *Apple Training Series: Mac OS X Server Essentials, Second Edition* (Peachpit 2008).

You will not have access to any resources or references during the exam. Please note that the exam is based on Mac OS X and Mac OS X Server version 10.5.1, which was the most current version available at the time of publication. All references to Mac OS X, Mac OS X v10.5, Mac OS X Server, and Mac OS X Server v10.5 refer to version 10.5.1.

The number of test questions drawn from each knowledge area is indicated below. Please note that although this guide divides the objectives into ten knowledge areas, questions are presented randomly during the exam. Also note that UNIX commands and processes are shown in `monospace font` in the exam.

## Installation & Configuration

This topic has 11 items, drawn from the following objectives:

- Identify variables that should be documented when designing a server's configuration.
- Identify the minimum hardware requirements for Mac OS X Server v10.5 installation.
- Describe how to verify that a computer meets the minimum hardware requirements to install Mac OS X Server v10.5.

- Identify computer configuration details that should be documented prior to performing a remote installation of Mac OS X Server v10.5, including the computer's hardware serial number and its Ethernet hardware address.
- Describe how to:
  - Use the Mac OS X Server v10.5 Install DVD to install Mac OS X Server v10.5 on the local computer.
  - Use Server Assistant to install Mac OS X Server v10.5 on a remote computer.
  - Install Mac OS X Server v10.5 on an Xserve that has no video display and no optical drive, including these methods: connecting an external FireWire optical drive, booting the Xserve in target disk mode, and using a NetBoot server.
  - Use the Installer log to verify successful Mac OS X Server v10.5 installations and to identify causes of failed installations.
  - Install the Mac OS X Server v10.5 administration tools on a Mac OS X client computer.
- Describe benefits of installing Mac OS X Server v10.5 on a hard disk with multiple partitions, including keeping the operating system files separate from data.
- Describe benefits of configuring a RAID set for a server, including improved performance and redundancy.
- Differentiate between RAID 0 and RAID 1.
- Identify the packages installed in an Easy Install of Mac OS X Server v10.5.
- List, compare, and contrast the volume formats on which Mac OS X Server v10.5 can be installed.
- Identify the tools used to configure Mac OS X Server v10.5 with a serial number.
- Describe how to configure a network interface on a Mac OS X Server v10.5 computer.
- List the directory server roles available to a Mac OS X Server v10.5 computer during its initial configuration.
- Describe how to:
  - Create the initial administrator account on a Mac OS X Server v10.5 computer.
  - Configure a local hostname on a Mac OS X Server v10.5 computer.
  - Save setup configuration data for a Mac OS X Server v10.5 computer to a text file for later reference.
  - Create a configuration file that will allow a Mac OS X Server v10.5 computer to auto-configure itself with the included settings when the file is copied to the server.
  - Save setup configuration data for a Mac OS X Server v10.5 computer as a record in a directory server that will allow other Mac OS X Server v10.5 computers to use the record to auto-configure themselves.
- Compare and contrast the three types of server configuration: Standard, Workgroup, and Advanced, including the utilities used for each configuration, how each configuration uses directory services, and the purpose of each configuration.
- Describe how to connect to a newly configured, remote Mac OS X Server v10.5 computer.
- Outline the relationship between the root account password and the password for the initial administrator account on a Mac OS X Server v10.5 computer.

- Explain the security risks posed by enabling the root account on a Mac OS X Server v10.5 computer.
- Describe how to configure a Mac OS X Server v10.5 computer's name so that its services can be uniquely identified on the network.
- Describe the import of configuring server and client computers to use a common network time server, so that time-based services such as Kerberos function properly.
- Describe how to configure the date and time on a Mac OS X Server v10.5 computer.
- Explain the purpose of:
  - The primary DNS name assigned to a Mac OS X Server v10.5 computer
  - The local hostname assigned to a Mac OS X Server v10.5 computer
  - The computer name assigned to a Mac OS X Server v10.5 computer
- Compare and contrast how the two directory usage roles, standalone and connected to a directory server, provide directory data.
- Describe how to configure a Mac OS X Server v10.5 computer to use the server's local data store for directory data.
- Outline the benefits of encrypting Mac OS X Server v10.5 computer configuration files and records.
- Describe how to encrypt stored configuration files or configuration records.
- Describe how to observe a Mac OS X Server v10.5 computer remotely from a Mac OS X v10.5 client computer using screen sharing.
- Describe the services that a Mac OS X Server v10.5 computer can provide.
- Describe the Mac OS X Server v10.5 computer services that can be monitored using the Server Admin utility.
- Describe how to connect to a Mac OS X Server v10.5 computer from a Mac OS X v10.5 client computer using the server's network address, and the name and password of an administrator.
- Describe how to configure Server Admin to monitor specific services on a Mac OS X Server v10.5 computer.
- Describe the main purposes of Server Admin, including service configuration and share point maintenance.
- Explain how to configure a Mac OS X Server v10.5 computer to send an email message when a hard disk connected to the server has less than a specified percentage of its space available.
- Describe the role of the Server Status widget, including where it runs and which services it can monitor.
- Describe how to configure the Server Status widget to perform high-level monitoring of a Mac OS X Server v10.5 computer.
- Describe how to use the Server Status widget to:
  - Determine the percentage of free disk space on the server.
  - Determine the server network load over a specified time period.
  - Determine the server CPU utilization over a specified time period.
- Describe how to use Server Admin to:
  - Display a graph showing server CPU utilization over a specified time period.

- Determine the percentage of free disk space on the server.
- Display a graph showing server network load over a specified time period.
- Update the server computer with available software updates provided by Apple's Software Update service.
- Configure the server to send an email when an Apple-provided software update is available.
- Export the configuration settings for specified services so that they can be imported into another Mac OS X Server v10.5 computer.
- Import configuration settings for specified services into a Mac OS X Server v10.5 computer.

### Providing DNS Service

This topic has 4 items, drawn from the following objectives:

- Describe how the Domain Name System (DNS) associates computer host names with IP addresses on a network.
- Outline the purposes of a DNS server, including translating between domain names and IP addresses, and acting as a cache and relay for translations provided by other DNS servers.
- Describe how a DNS server uses a hierarchy of DNS servers to resolve domain names that are not stored locally.
- Define the term "DNS zone"
- Explain the purpose of each of these records that can be added to a DNS zone: address, alias or canonical name, mail exchange, and pointer.
- Explain how to start and stop DNS service on a Mac OS X Server v10.5 computer.
- List the steps necessary to configure a new DNS service for an organization, including registering a domain name, creating DNS zones, adding DNS records to the zones, and starting the DNS service.
- Describe how to verify that DNS service is resolving domain names and IP addresses correctly.
- Define the three types of DNS zones: master, slave, and forward.
- Describe how to create a new zone on a Mac OS X Server v10.5 computer.
- Differentiate between a fully qualified domain name (FQDN) and a relative domain name.
- Describe how to:
  - Add a new machine record to a DNS zone.
  - Add a new alias record to a DNS zone.
  - Add mail exchange records to a DNS zone.
  - Configure a mail exchange record's priority.
- Explain the purpose of a priority value in a mail exchange record in a DNS zone.

### Authentication, Authorization, & Access Control

This topic has 10 items, drawn from the following objectives:

- Define "authentication" and "authorization" as they apply to computers and servers.

- Describe how to:
  - Create a user account so a user can authenticate before accessing Mac OS X Server v10.5 services.
  - Create a group account.
  - Assign users to a group account.
  - Enable a user account to have administrative abilities.
- Identify examples of user authentication, such as a user logging in on a client computer, a user connecting to a file server, an admin user authenticating in order to configure the server, and providing a user name and password for a secured website.
- Explain the primary purpose of the Workgroup Manager utility in Mac OS X Server v10.5.
- List the types of Mac OS X Server v10.5 accounts that can be created and managed by Workgroup Manager, including user, workgroup, computer, and computer group.
- Describe how to export accounts from one Mac OS X Server v10.5 computer, so they can be imported to another Mac OS X Server v10.5 computer.
- Describe how to import accounts from a text file or an XML file to a Mac OS X Server v10.5 computer to be used for authentication and authorization purposes.
- Explain the purpose of a user ID for a Mac OS X Server v10.5 user account.
- Define the terms “groups” and “workgroups” as they apply to Mac OS X Server v10.5 user accounts.
- Describe how to:
  - Assign groups to a Mac OS X Server v10.5 user account.
  - Assign groups to a single group, so that all users can be granted the same permissions as a group on the Mac OS X Server v10.5 computer.
- Describe how to modify POSIX permissions for files and folders to restrict user access to them.
- List examples of authorization on a Mac OS X v10.5 client computer.
- Define the term “access control lists” (ACLs).
- Describe how to create ACLs for files and folders on a Mac OS X Server v10.5 computer, and files shared by a Mac OS X Server v10.5 computer.
- Describe how Mac OS X Server v10.5 file system ACLs map to Windows file system ACLs.
- Explain how guest access, and Everyone permissions to files on a Mac OS X Server v10.5 computer can expose shared items to undesired access.
- Define the terms unique IDs (UIDs), group IDs (GIDs), and globally unique IDs (GUIDs).
- Explain how:
  - UIDs and GIDs help relate permissions for files and folders to users and groups on a Mac OS X Server v10.5 computer.
  - GUIDs associate ACLs to users and groups on a Mac OS X Server v10.5 computer.
  - POSIX permissions can limit options when setting up folder and file permissions structures that involve multiple users or groups.
- Define the terms file system ACL “inheritance,” access control entries (ACEs), and service ACLs (SACLs).
- Explain how Mac OS X v10.5 interprets ACEs to determine the permissions of a file or folder.

- Describe the order in which Mac OS X v10.5 interprets ACEs and POSIX permission settings when determining the effective permissions for a file.
- Explain why it is a best practice to manage permissions at the workgroup level rather than at the user level in Mac OS X Server v10.5.
- Describe how to configure SACLs to restrict user access to some or all Mac OS X v10.5 Server services.
- Describe how to configure a Mac OS X Server v10.5 computer to allow a specified set of users to administer some or all of its services.
- Outline why a user might be given administrative abilities over a subset of Mac OS X Server v10.5 services.
- Describe how to configure a Mac OS X Server v10.5 computer to allow a specified set of users to monitor some or all of its services.

### Open Directory

This topic has 11 items, drawn from the following objectives:

- Describe the function of directory services in a networked computing environment.
- List, compare, and contrast the four Open Directory service roles available to a Mac OS X Server v10.5 computer, including: standalone, Open Directory master, connected to a directory server, and Open Directory replica.
- Define “Open Directory” as it relates to Mac OS X v10.5 client computers.
- Outline the Open Directory structure and components present on a Mac OS X v10.5 client computer.
- Describe how to configure DHCP service on a Mac OS X Server v10.5 computer to deliver LDAP configuration information to client computers so that the clients will automatically bind to the specified LDAP server.
- List advantages to users and administrators of networked directory services, including providing a common user experience, providing easier access to networked resources such as printers and servers, and allowing users to log in on different computers using a single account.
- List advantages of using a server to provide shared directory data, including providing common authentication information to multiple servers, and providing common configuration data, such as automounts and printers to multiple client computers.
- Describe how to configure a Mac OS X Server v10.5 computer:
  - To use directory data provided by another directory server so that users can access services on the Mac OS X Server v10.5 computer by authenticating with user accounts provided by the other directory server
  - As an Open Directory master, so that multiple computers on the network can access directory data provided by the Mac OS X Server v10.5 computer
  - As an Open Directory replica, so that the replica shares with client computers directory data provided by an Open Directory master
- Describe how to configure a Mac OS X v10.5 client computer to connect to a Mac OS X Server v10.5 computer configured as an Open Directory master for authentication and directory data.
- Outline how to create user accounts on a Mac OS X Server v10.5 computer configured as an Open Directory master, so that the user accounts can be accessed from client computers that are bound to the Open Directory master.

- Identify the maximum number of:
  - Open Directory replicas that can be connected to a Mac OS X Server v10.5 computer
  - Open Directory replicas that can be part of a single Open Directory network.
- Outline how to determine if any Open Directory replicas are connected to an Open Directory master.
- Explain how to display Open Directory service-related log files.
- Describe how to archive the Open Directory data on the server to a disk image file, so the data can be restored later.
- Describe how to restore Open Directory data from a disk image to a Mac OS X Server v10.5 computer.
- Identify and describe the Mac OS X Server v10.5 utilities used to configure Open Directory on a Mac OS X Server v10.5 computer.
- Identify the data that is archived by the Mac OS X Server v10.5 Open Directory Archive function.
- Describe how to configure user accounts so that when users change their passwords, the new passwords configure to organizational password policies.
- Describe how to configure password types for a user account on a Mac OS X Server v10.5 computer.
- Describe how to disable a user account without deleting it, so it can't be used for authentication.
- Identify and describe the five methods a Mac OS X Server v10.5 computer can use for authentication: hash files, crypt passwords, password server, Kerberos, and LDAP.
- Outline how Kerberos provides both authentication and identification services.
- Define these terms as they apply to Kerberos: ticket, Kerberos Distribution Center, ticket-granting ticket, service ticket.
- Contrast these methods for storing authentication information: crypt, shadow, and Open Directory.
- Identify reasons why a client computer might not be able to access a service using Kerberos authentication, including: DNS configuration issues, a mismatch in time settings between the client and server computers, Kerberos authentication for a service is disabled, a user account is not configured correctly.
- Describe how to display Kerberos tickets that have been granted to a computer.
- Explain how to troubleshoot a client computer's failure to access services when using Kerberos authentication.
- Describe how to configure user account password policies so that passwords are disabled after a specified number of failed authentication attempts.
- Describe how to configure user accounts so users cannot change their passwords.
- Explain how to determine the appropriate password type for an account.
- Identify the utilities used to set password policies for user accounts.
- Identify the types of password policies that can be applied to a user account in Mac OS X Server v10.5.
- Outline a method for displaying the status of Kerberos tickets on a Mac OS X v10.5 computer.

## File Services

This topic has 13 items, drawn from the following objectives:

- List the file sharing protocols that can be used to share files from a share point on a Mac OS X Server v10.5 computer.
- Identify issues related to sharing files using more than one protocol, including volume format case-sensitivity, and file system permissions.
- Describe how to configure:
  - A folder on a Mac OS X Server v10.5 computer as a share point
  - A share point on a Mac OS X Server v10.5 computer as a Time Machine repository for Mac OS X client computers
- Outline the four basic steps to setting up file services, including: planning, configuring accounts, configuring file service, and monitoring the service.
- Describe how to:
  - Create a new folder on a Mac OS X Server v10.5 computer
  - Enable Spotlight searching on a Mac OS X Server v10.5 computer share point
- Identify the utility used to create and manage share points in Mac OS X Server v10.5.
- Describe how to configure a Mac OS X Server v10.5 computer share point to allow client computers to access files using Apple Filing Protocol (AFP).
- Describe how to configure a Mac OS X Server v10.5 computer share point so client computers need not provide a user name and password to access files.
- Describe how to:
  - Display a graph showing AFP file service activity, including throughput and connections.
  - Edit the AFP service greeting message displayed when clients connect.
  - Select the authentication methods used when client computers attempt to connect to the server via AFP.
  - Configure the AFP service to log AFP user activity.
  - Display AFP error and access logs.
  - Configure the AFP service to log specific types of AFP activities, including: logging in, logging out, opening and creating files or folders, and deleting files or folders.
  - Configure the AFP service to disconnect idle users after a certain time limit.
  - Configure the share point name that AFP client computers see when browsing for a share point.
- Contrast standard POSIX behavior and inheritance with permissions assignment on an AFP share point that resides on a Mac OS X Server v10.5 computer.
- Outline how to select a default permissions model, POSIX or inherited, to use when new files and folders are created on an AFP share point on a Mac OS X Server v10.5 computer.
- Describe how to start and stop the AFP service on a Mac OS X Server v10.5 computer.
- Describe how to configure the AFP service on a Mac OS X Server v10.5 computer:
  - So that client computers can browse for AFP share points over Bonjour

- To display a greeting message once per user session
- To allow users to connect without providing a user name and password
- Explain why an administrator might want to masquerade as any registered user of the AFP service on a Mac OS X Server v10.5 computer.
- Describe how an administrator can masquerade as a registered user of the AFP service in Mac OS X Server v10.5.
- Describe how to configure the AFP service on a Mac OS X Server v10.5 computer to:
  - Allow an administrator to masquerade as any registered user.
  - Limit the number of simultaneous connections and simultaneous guest connections to a specific number.
  - Exempt guests, administrators, registered users, and users with open files from being disconnected automatically after being idle for a period of time.
  - Allow client computers to sleep for a specified time before being automatically disconnected from the server.
  - Log errors that occur with the service.
- List the types of AFP activities that can be logged.
- Identify the two Mac OS X Server v10.5 log files that provide info about the AFP service.
- Describe how the various authentication methods available for AFP service in Mac OS X Server v10.5 affect how a user authenticates.
- Describe how to start and stop Server Message Block (SMB) services on a Mac OS X Server v10.5 computer.
- Differentiate between the various permissions models available for SMB services on a Mac OS X Server v10.5 computer, including specified permissions and inherited permissions.
- Describe how a Windows client computer accesses a shared SMB volume that resides on a Mac OS X Server v10.5 computer.
- Explain how to configure a share point to allow client computers to access files using SMB.
- Explain how to configure the WINS registration for the SMB service on a Mac OS X Server v10.5 computer.
- Define the terms “oplocks” and “strict locking” as they apply to the SMB service in Mac OS X Server v10.5.
- Describe how to configure the SMB service in Mac OS X Server v10.5 to log SMB user activity.
- Describe how to enable oplocks or strict locking for an SMB share point on a Mac OS X Server v10.5 computer.
- Identify and describe the four roles provided by the Windows service on a Mac OS X Server v10.5 computer: Standalone, Domain Member, Primary Domain Controller, and Backup Domain Controller.
- Describe how to:
  - Configure an SMB share point on a Mac OS X Server v10.5 computer to allow user access without requiring a user name and password.

- Configure the share point name that SMB client computers will see when browsing for the SMB share point that resides on a Mac OS X Server v10.5 computer.
- Configure the Computer Name and Workgroup for the SMB service on the Mac OS X Server v10.5 computer.
- Configure the SMB service on a Mac OS X Server v10.5 computer to allow user access without requiring a user name and password.
- Configure the SMB service on a Mac OS X Server v10.5 computer to limit the number of simultaneous connections to a specific number.
- Select an authentication method to use when client computers try to connect to the SMB service on a Mac OS X Server v10.5 computer.
- Configure a Mac OS X Server v10.5 computer to act as a Workgroup Master Browser.
  - Display a graph that shows number of SMB connections over time.
- Define “Workgroup Master Browser” and “Domain Master Browser” as they apply to the SMB service in Mac OS X Server v10.5.
- Define “WINS registration” as it applies to the SMB service in Mac OS X Server v10.5.
- Describe how to:
  - Start and stop File Transfer Protocol (FTP) services on a Mac OS X Server v10.5 computer.
  - Troubleshoot FTP service issues.
  - Enable and disable anonymous access over FTP.
  - Configure the FTP service logs.
  - Create access control lists (ACLs) to control access to FTP services on the Mac OS X Server v10.5 computer.
  - Configure a share point on a Mac OS X Server v10.5 computer to allow client computers to access its files over FTP, with or without a user name and password.
  - Select the authentication methods used when client computers attempt to connect to the Mac OS X Server v10.5 computer via FTP.
  - Configure the share point name that client computers see when browsing for the share point.
- Describe how an FTP client requests the Mac OS X Server v10.5 FTP service to perform file conversions before sending files.
- Explain passive FTP and when it is useful.
- Explain how Mac OS X Server v10.5 uses user IDs for access control on NFS volumes.
- Describe how to configure a share point on a Mac OS X Server v10.5 computer:
  - So that it is accessible via NFS
  - To be accessible to any NFS client computer regardless of the client computer’s IP address
  - To be accessible to NFS client computers on a specified subnet of a network
  - To be accessible to NFS client computers with specific IP addresses
  - So clients access its files as Nobody (Guest)
  - So clients who access its files as root, access them as Nobody (Guest)

- So its files and folders are “Read only” to NFS client computers
- Configure the security level of an NFSshare point on a Mac OS X Server v10.5 computer.
- State the URL used by client computers to access an NFS share point on a Mac OS X Server v10.5 computer.
- Identify at least two benefits of providing automounts, including providing network home folders and sharing OS resources such as system files and applications.
- Describe how to configure a share point on a Mac OS X Server v10.5 computer to act as a shared Applications folder for Mac OS X client computers.
- Describe how to configure a share point on a Mac OS X Server v10.5 computer to host network home folders.
- List the file sharing protocols that can be used to serve home folders hosted by a Mac OS X Server v10.5 computer.
- Describe how to configure:
  - A disk quota on a home folder that is hosted on a Mac OS X Server v10.5 computer
  - A Mac OS X Server v10.5 user account to use a share point hosted on a Mac OS X Server v10.5 computer as a home folder
  - A share point on a Mac OS X Server v10.5 computer to act as a Library folder for Mac OS X client computers
- Outline how to select the file sharing protocol that is used when a share point is mounted.
- Describe how to configure the protocol used to serve home folders that are hosted on a share point on a Mac OS X Server v10.5 computer.
- Describe how to select the appropriate type of automount when an automount share point is needed.

## Mail Service

This topic has 7 items, drawn from the following objectives:

- Define the terms POP, IMAP, and SMTP as they apply to email service.
- Explain how an email server that is handling outgoing email identifies the network address of the destination mail server.
- Define the term “cluster” as it applies to mail servers.
- Identify reasons for hosting a mail server, including limited network bandwidth, increased security, and enhanced control.
- Describe how an email travels from a source client computer through multiple mail servers to a destination client computer.
- Describe the steps to enable a Mac OS X Server v10.5 user account to send and receive email.
- Describe how to configure a Mac OS X Server v10.5 user account to use a specified mail server to send and receive email.
- Explain reasons for selecting and how to select POP or IMAP for a Mac OS X Server v10.5 user account to receive email.
- Explain how to start and stop mail service on a Mac OS X Server v10.5 computer.

- Explain how to configure the domain name and host name for Mac OS X Server v10.5 mail service.
- Describe how to enable Mac OS X Server v10.5 mail service to allow client computers to use either the POP or IMAP protocol to receive email.
- Outline how to configure Mac OS X Server v10.5 mail service to specify a limit on the number of IMAP connections.
- Explain how to enable Mac OS X Server v10.5 mail service to use the SMTP protocol to receive email from client computers and from other mail servers.
- Describe how to configure Mac OS X Server v10.5 mail service to:
  - Relay outgoing email through a specified mail server.
  - Participate in a mail cluster.
  - Let users access their mail accounts via a web browser.
- Describe how to enable authentication methods for POP, IMAP, and SMTP protocols to increase a Mac OS X Server v10.5 computer's security.
- Define the terms "open relay," "spam," and "blacklist service" as they apply to mail service.
- Explain how to verify that a Mac OS X Server v10.5 mail service is not acting as an open relay.
- Outline how to configure Mac OS X Server v10.5 mail service to:
  - Only relay mail from trusted mail servers.
  - Reduce the amount of incoming spam for local users.
  - Refuse email from rogue mail servers.
  - Scan incoming email for junk mail.
  - Send or not send incoming email that has been identified as junk.
  - Scan incoming email for viruses.
  - Handle infected messages.
  - Update its virus database in a specified timeframe.
- Describe how to configure how aggressive the mail service is in scanning for junk mail.
- Explain how to set the appropriate log levels for SMTP, IMAP/POP, and Junk Mail, based on specific operating conditions, such as normal, under a spam attack, and users unable to send or receive email.
- Outline how to configure Mac OS X Server v10.5 mail service to:
  - Send a copy of all email, including undeliverable email to a specified email address.
  - Reject incoming email that is larger than a specified size.
  - Limit user accounts to a specified disk space usage, through mail quotas.
  - Disable incoming mail for a user account when its quota is reached.
  - Send a warning email when a certain percentage of a user account's mail quota is reached.
- Describe how to create a mail list so that emails sent to a single email address will be distributed to multiple users.

- Identify messages that can help diagnose why a user is unable to send or receive email using the mail service.
- Identify methods to limit the amount of disk space used by the Mac OS X Server v10.5 mail service, including setting mail quotas, and setting maximum incoming message sizes.
- Describe how to set a mail quota for a user account.

## Web Service

This topic has 6 items, drawn from the following objectives:

- Describe how to:
  - Start and stop the Mac OS X Server v10.5 web service.
  - Display a graph that charts the throughput or number of requests made for the web service.
  - Create a new website on a Mac OS X Server v10.5 computer.
  - Configure two or more websites on a Mac OS X Server v10.5 computer, so that each is uniquely accessible
  - Create a realm so that access to a website or portion of a website is restricted to specific users
- List various methods for distinguishing between multiple websites hosted by a Mac OS X Server v10.5 computer, including domain name, IP address, and port number, so that a single Mac OS X Server v10.5 can host multiple websites.
- Define the terms, “realm,” “alias,” and “module” as they relate to Mac OS X Server v10.5 web service.
- Describe how to:
  - Add an alias to a website so that the Mac OS X Server v10.5 responds to the new name.
  - Enable and disable a module for the Mac OS X Server v10.5 web service.
  - Configure the folder listing option.
- Explain how enabling the folder listing option for a Mac OS X Server v10.5 website can decrease the security of the website.
- Identify a reason to enable the folder listing option, such as, to provide a simple interface to a collection of files to be made available to users via the web service.
- Identify the default location of a Mac OS X Server v10.5 computer’s website files.
- Describe how to configure the location of the data files for a website hosted by the Mac OS X Server v10.5 web service.
- Explain how to enable log files for a website hosted by Mac OS X Server v10.5 web service.
- Identify the standard web server on which Mac OS X Server v10.5 web service is based.
- Identify the full default URL for the website of a user whose site files are in the user’s home folder, which is stored on the Mac OS X Server v10.5 computer hosting the web service.
- State the correct permissions settings for a set of files stored on a Mac OS X Server v10.5 computer, so the server’s web service can serve the files.

- Identify the Mac OS X Server v10.5 group that must have Read access to files that are to be served by the Mac OS X Server v10.5 web service.
- Explain how to enable and disable a site hosted by the Mac OS X Server v10.5 web service, so the site is accessible or not from other computers.
- Identify sites whose performance will be enhanced by enabling the performance cache in the Mac OS X Server v10.5 web service, such as sites serving static web pages.
- List the types of logs generated by the Mac OS X Server v10.5 web service
- Compare and contrast WebDAV with other common file sharing protocols such as AFP, FTP, SMB, including security issues, URL formats, and benefits.
- Describe how to:
  - Enable and disable WebDAV on a website hosted by a Mac OS X Server v10.5 computer.
  - Configure permissions for a folder on a Mac OS X Server v10.5 computer to allow Read/Write access to the folder over WebDAV.
- State the URL for accessing files on a Mac OS X Server v10.5, shared via WebDAV.
- Identify the protocol WebDAV uses to share files.

### Collaborative Services

This topic has 10 items, drawn from the following objectives:

- Define the terms “wiki” and “weblog” as they apply to Mac OS X Server v10.5.
- Describe how to:
  - Enable the wiki and blog services for a website hosted by a Mac OS X Server v10.5 computer.
  - Add groups that reside on the Mac OS X Server v10.5 computer to a list of those who can create a wiki on a website hosted by the server.
  - Enable web calendar capabilities for a website hosted by a Mac OS X Server v10.5 computer.
  - Create and modify a wiki on a Mac OS X Server v10.5 computer that is hosting a wiki-enabled website.
- State three benefits of setting up a wiki server.
- Describe how to:
  - Enable the iCal service on a Mac OS X Server v10.5 computer so that two or more Mac OS X client computers can access and share calendar data.
  - Configure where the calendar data repository for iCal services hosted on a Mac OS X Server v10.5 computer will reside.
  - Configure user quotas for storing data in the iCal server hosted on a Mac OS X Server v10.5 computer.
  - Configure the iCal server hosted on a Mac OS X Server v10.5 computer to use SSL.
  - Troubleshoot issues with the iCal server hosted on a Mac OS X Server v10.5 computer.
- Identify a reason why it is necessary to establish a quota for users of the iCal service hosted on a Mac OS X Server v10.5 computer.

- List three reasons stated in the Mac OS X Server v10.5 documentation for providing shared calendar services using the iCal service on a Mac OS X Server v10.5 computer.
- Describe how to configure iCal on a client Mac OS X computer to display shared scheduling data provided by the iCal service on a Mac OS X Server v10.5 computer.
- Explain how to create new resources on a Mac OS X Server v10.5 computer's iCal service that can be scheduled using iCal on a client Mac OS X computer.
- Identify the protocols used by the Mac OS X Server v10.5 iCal service.
- Describe how to:
  - Start and stop the iChat service on a Mac OS X Server v10.5 computer.
  - Configure the authentication method used by the iChat service on a Mac OS X Server v10.5 computer.
  - Choose the SSL certificate that the iChat service on a Mac OS X Server v10.5 computer will use to secure text, audio, and video chats.
  - Modify the list of host domains that the iChat service in Mac OS X Server v10.5 will connect to.
  - Troubleshoot issues with the iChat service on a Mac OS X Server v10.5 computer.
- Explain the purpose of the federation feature in the iChat service in Mac OS X Server v10.5.
- Explain the benefits of setting up a chat server, including automatically generated chat transcripts, and increased security.
- Identify the protocol used by the iChat service in Mac OS X Server v10.5, by both its familiar name, Jabber, and its official name, Extensible Messaging and Presence Protocol (XMPP).
- Describe how to:
  - Add a service account to iChat on a client computer, so that it can be used to chat with other iChat users via the iChat service on a Mac OS X Server v10.5 computer.
  - Identify the iChat server screen name for a user account.
  - Configure the iChat service on a Mac OS X Server v10.5 computer so that all chats are logged to a file on the server.
  - Specify the location where chat logs are stored on a Mac OS X Server v10.5 computer.
  - Discover how many users are connected to the iChat service on a Mac OS X Server v10.5 computer.
  - Discover which users are connected to the iChat service on a Mac OS X Server v10.5 computer.
  - Display chat messages that are stored on the Mac OS X Server v10.5 computer.
  - Display the iChat service log.
  - Enable the server-to-server federation feature for the iChat service on a Mac OS X Server v10.5 computer.
  - Configure the iChat service on a Mac OS X Server v10.5 computer to allow federation with any other or with a specific XMPP chat server.

- List methods that can be used by the iChat service in Mac OS X Server v10.5 to authenticate iChat clients.
- Describe how to enable or disable access to iChat services on a Mac OS X Server v10.5 computer for a specific user or group account.

## Deployment Solutions

This topic has 8 items, drawn from the following objectives:

- Describe how to start and stop NetBoot service on a Mac OS X Server v10.5 computer.
- List the initial steps that a client computer goes through when booting from a NetBoot server.
- Describe the function and location of the System Image Utility application on a Mac OS X Server v10.5 computer.
- Describe how to:
  - Configure NetBoot service on a Mac OS X Server v10.5 computer to allow or deny specific client computers access to the service.
  - Identify client computers that booted using a NetBoot system image hosted by a Mac OS X Server v10.5 computer.
  - Configure a specific NetBoot system image as the default image used by the NetBoot service.
  - Set the protocol used to serve a NetBoot system image.
- Explain how network home folders complement a NetBoot system by providing users a location to store personal data and preferences.
- Define the terms, “NetBoot” and “shadow files”, as they relate to Mac OS X Server v10.5.
- State three methods of configuring a client computer to boot using a system image provided by the NetBoot service in Mac OS X Server v10.5.
- Describe how to:
  - Configure a client computer to boot using NetBoot service when a key sequence is pressed during system startup.
  - Troubleshoot issues with the NetBoot service by reviewing NetBoot service log files.
  - Configure a NetBoot system image to change its ByHost preferences after it has been installed.
- Outline five scenarios where a NetBoot server is useful, including: having to quickly update a large installed base of computers with newer system software; quickly repurposing a number of computers with a different software, including operating systems and applications; needing an emergency boot disk when a hard drive on a client computer has failed; needing to quickly revert systems, such as kiosks, to a known “clean” state; and needing a quick and easy method for imaging computers with a variety of configurations.
- Differentiate between a NetInstall image and a NetBoot image.
- List the two types of sources, install media and disk volumes, that can be used to create a NetBoot or NetInstall image.
- State the minimum Mac OS version for a Mac OS X Server v10.5 NetBoot or NetInstall image source.

- Compare and contrast the benefits of using various image sources for a NetBoot or NetInstall image, including the ability to create clean system.
- State the location where a NetBoot image should be stored on a Mac OS X Server v10.5 computer, so that it can be used by the NetBoot service.
- Describe how to:
  - Create a NetBoot or NetInstall image for use by the NetBoot service on a Mac OS X Server v10.5 computer.
  - Copy a NetBoot image to the location where it can be used by the NetBoot service on a Mac OS X Server v10.5 computer.
  - Enable a NetBoot image so that client computers can boot from it.
  - Configure a client computer to boot from a NetBoot image.
  - Configure NetBoot service to share images over a specific network port.
  - Specify volumes on a Mac OS X Server v10.5 computer used to store NetBoot data.
  - Identify client computers' connection information, including what image is booted from, and when it last booted.
- State the keys that should be pressed during system startup to configure the client computer to boot from a NetBoot image.
- Describe how to display the NetBoot service log files.
- Identify the minimum network requirements to support client computers booting using the NetBoot service in Mac OS X Server v10.5.
- Identify the minimum system requirements for client computers that will boot from the NetBoot service in Mac OS X Server v10.5.
- Describe the purpose of the filters in the Mac OS X Server v10.5 NetBoot service.

## Managing Accounts

This topic has 10 items, drawn from the following objectives:

- List reasons to use Mac OS X Server v10.5 to manage user account preferences, including providing consistent user experience between multiple computers, managing permissions on portable computers, restricting resources to select users or groups, increasing security, and providing a managed user experience.
- Identify the Mac OS X Server v10.5 utility used to manage user account permissions.
- Identify the Mac OS X Server v10.5 utility used to manage user account preferences.
- Compare and contrast the four type of Mac OS X Server v10.5 accounts: user, group, computer, and computer group.
- State locations on a client computer where managed preferences reside.
- Compare and contrast characteristics of network and local user accounts.
- Describe how the four time-based options for enforcing managed account preferences: Never, Once, Always, and Often, effect when a managed preference is enforced.
- Describe each of the three precedence rules for account preferences: inherit, override, and combine.
- Outline how preference manifests are implemented in Mac OS X Server v10.5.

- Outline common preference management problems according to the Mac OS X Server v10.5 User Management documentation, and techniques used to solve them.
- Describe how to:
  - Create a group folder on a Mac OS X Server v10.5 computer, that will be automatically accessible from the desktop of a client computer.
  - Import a preference manifest so that an application not listed by default in Workgroup Manager can still be managed.
  - Enable the Inspector on a Mac OS X Server v10.5 computer, so that directory data on the server can be examined.
  - Create a new computer account on the Mac OS X Server v10.5 computer, so that the computer can be managed.
  - Create a new computer group account containing specific computers.
- State the hierarchy of accounts on a Mac OS X Server v10.5 computer, as that hierarchy applies to managed preferences.
- Describe the behavior of a managed client computer when a managed user logs in and has an overlapping set of managed account preferences that apply at all four account levels.
- Explain the purpose of the Guest Computer account in Workgroup Manager.
- Describe how to configure managed preferences for an account so that any user who connects using the account can open only a specified set of applications or widgets.
- List all managed preference settings that can be applied to a user, group, computer, or computer group account.
- State two methods of hosting a group folder on a Mac OS X Server v10.5 computer so that it is automatically accessible from the desktop of a Mac OS X client computer.
- Describe how to configure a Mac OS X Server v10.5 computer to download all software updates provided by Apple.
- Explain two reasons an organization would want to set up an internal software update server, including maintaining control over the updates users install, and reducing the amount of network bandwidth used.
- Describe how to:
  - Configure a user account on a Mac OS X Server v10.5 computer to use an update server for software updates provided over the network.
  - Configure a Mac OS X Server v10.5 computer to download all new software updates provided by Apple.
  - Configure a Mac OS X Server v10.5 computer to automatically enable updates downloaded from Apple.
  - Configure the Mac OS X Server v10.5 computer to automatically delete any legacy or unused updates.
  - Configure the Mac OS X Server v10.5 computer to limit the network bandwidth used to distribute updates.
  - Enable updates so they are accessible to other computers on the network.
  - Identify updates provided by Apple that are available for download.

- Describe basic features of the Software Update service in Mac OS X Server v10.5, including its ability to automatically download updates provided by Apple, and to selectively distribute updates.
- Outline the characteristics of a mobile user account in Mac OS X Server v10.5.
- Describe how synchronized folders are implemented in Mac OS X Server v10.5.
- Describe how to:
  - Enable synchronized folders for a mobile user account in Mac OS X Server v10.5.
  - Configure a mobile user account to automatically be deleted from a Mac OS X client computer when a specified time period has elapsed.
  - Configure a Mac OS X Server v10.5 user account to use an external account.
  - Configure when a Mac OS X Server v10.5 user account's home folder on a client computer is synchronized with the same user's home folder stored on a server.

## For More Information

Please visit [www.apple.com/training](http://www.apple.com/training) for more information about all Apple training courses and certification programs.

© 2008 Apple Inc. All rights reserved. Apple, the Apple logo, Mac, and Mac OS are trademarks of Apple Inc., registered in the U.S. and other countries. Other product and company names mentioned herein may be trademarks of their respective companies. Mention of non-Apple products or services is for informational purposes only. Product specifications are subject to change without notice. May 2008