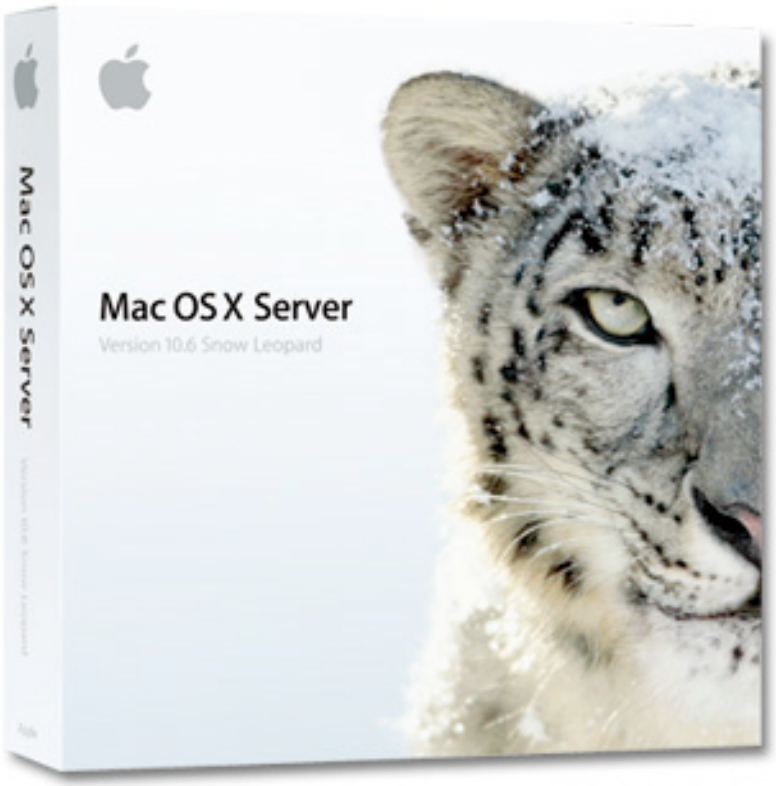
Apple Certified Technical Coordinator ACTC v10.6



NOTEBOOK

Hosting Mail Services 39

Apple Certified Technical Coordinator v10.6

Disclaimer

This notebook is intended for personal use only, it is a collection of questions and answers regarding the subjects concerning the ACTC certification v10.6.

It has never been authorized by Apple or Editors of the Apple Training Series books and is not intended to substitute any official Apple resource suggested to obtain the ACTC certification.

The following content is an unofficial (my personal) guide to acquire knowledge to pass the certification exam Snow 201, it may be inaccurate and may contain mistakes, it is just the result of my studies and was intended to help myself in memorizing the main concepts learned reading the official books part of the Apple Training Series.

Marco Massari Calderone

marco at marcomc dot com

Installing and Configuring Mac OS X Server

Identify the minimum hardware requirements for installing Mac OS X Server

1. A Desktop Mac with Intel processor
2. 2GB of RAM
3. 10GB of free space on the Hard Drive

List the computer specific details that you will need From a Mac computer in order to perform a remote installation of Mac OS X Server on the computer

1. NIC's MAC Address to identify the target server
2. Computer's serial number to authenticate (8 first digits, case-sensitive)
3. Optionally, the current IP address assigned by a local DHCP service (as during the installation the same IP could be reassigned to the same server so will be easier to identify it)

List the volume formats which can be used for a Mac OS X Server boot volume

1. JHFS+ (Journaled)
2. JHFSX (Journaled, Case-Sensitive)

It's possible to use the non-Journaled HFS+ and HFSX, but they're not recommended

Describe how installing Mac OS X Server on a multiple-partition drive simplifies the task of keeping operating system files separate from server data

Keeping the system files separate from the serve data (user accounts, service data), saving them in a different partition allows easier maintenance as the administrator can safely reinstall the system without erasing data.

It also prevents user and service files and data to fill up the boot volume.

If the data is saved in a different drive on a different BUS we will have an increased speed in writing and accessing data.

List the possible passwords to use to access a remote Mac computer with Server Assistant when configuring a new installation on Mac OS X Server

1. Newly installed systems: first eight characters of the target server's serial number
2. Intel Xserve with no serial number (after the main logic board has been replaced): '`System S`'
3. Computer with no serial number (after the main logic board has been replaced): '`12345678`'
4. Configuring an upgraded server: the root's password

Describe how to install the Mac OS X Server administration software on a Mac OS X client computer

1. Install the package 'Server Administration Software.mpkg' from the Mac OS X Server Install Disc
2. Download the Server Admin Tools from Apple's website

Describe how to install Mac OS X Server on a head-less computer

1. Install Server Admin Tools in a Mac OS X client
2. Collect the information to identify and authenticate on the target server
3. Boot the target server with Mac OS X Server Install Disc
4. Launch Server Assistant application on the client computer
5. Find the server on the list of found server by Server Assistant or connect to the server specifying its IP address
6. Start the installation process from Server Assistant

Identify the packages that are installed by Server Assistant when Easy Install is selected

The default installation include the following packages:

1. Essential system software
2. Essential server software
3. Server administration software
4. Language translations (can be excluded in a customized installation)
5. Printer support (can be excluded in a customized installation)
6. `X11` (can be excluded in a customized installation)
7. Rosetta (can be excluded in a customized installation)

Describe four procedures for installing Mac OS X Server on a headless Xserve that has no optical drive

1. Connect an external optical drive via USB or Firewire
2. Use the optical drive on a computer in Target Disk Mode attached by FireWire cable
3. Start the server in Target Disk Mode and use another computer to install the software on the server system's mounted volume
4. Use another server with NetBoot service enabled to perform a network installation with a NetInstall image

Describe how to use the Installer Log file from a Mac with Mac OS X Server newly installed to verify that the installation was successful

Choose to view the Installer Log during the installation from the Window menu

Given an Installer Log file for a failed Mac OS X Server installation, identify the point of failure

- Choose the option 'Show All Logs and use the Filter field to search keywords such as 'fail', 'error', ' unable' and 'warning' that may indicate an unsuccessful installation

Or

- Choose the option 'Show Errors Only'

Compare and contrast effects of selecting each of the three Users and Groups options in Server Assistant including how they effect the state of Open Directory service

Create Users and Groups	Import Users and Groups	Configure Manually
• The server is configured as Open Directory Master (without interaction) • Users and Groups information will be stored and shared with client computers	• Open directory service is configured to connect to an Open Directory or Active Directory server where user and group records are stored	• Configures DNS service • You decide wether and how to configure Open Directory service
DEFAULT SERVICES ENABLED	DEFAULT SERVICES ENABLED	NO SERVICES ENABLED
Files and Printers Sharing	Files and Printers Sharing	X
Web and Application Hosting	Web and Application Hosting	X
Mail Services	Mail Services	X
Directory Services and Authorization	Directory Services and Authorization	X
Calendaring and Collaboration	X	X
Instant Messaging	X	X

Describe the security implications of having the root account enabled on a Mac OS X Server computer

1. The `root` account has unrestricted access to all resources via both command line (CLI) and Finder
2. The `root` account has by default the same password as the local administrator so anyone who knows the Administrator password can potentially gain the same unrestricted access

Describe the relationship between the password for the root account and the password for the initial administrator account on a Mac OS X Server computer

1. The password for root is the same as the password for the initial local administrator
2. The two passwords ARE NOT synchronized

Explain the purpose of the primary DNS name assigned using Server Assistant on a Mac OS X Server computer

1. It's a unique name for the server (FQDN)
2. Some services on Mac OS X either require a FQDN or will work better I one is available
3. If Server Assistant doesn't detect the DNS name you specify here from a DNS service it will automatically configure the DNS service on your Mac OS X Server

Explain the purpose of the primary DNS name assigned using Server Assistant on a MAc OS X Server computer

1. The Computer Name is used by clients who use the AFP protocol to access sheer points
2. The Computer Name is shown in the shared section of the Finder sidebar

Explain the purpose of the local hostname on a Mac OS X Server computer

The local hostname is used to identify the server in the local network and it's used by the Bonjour advertising protocol

Describe the importance of configuring server and client computers to use a common network Time Server so that the time-dependent services, such as Kerberos, function correctly

1. Server services are time-dependent and tolerate only a small time gap between the client and server system time
2. Configuring a common Time Server for the client and the server helps to remove issues related to time configuration

List the Directory Server roles that can be chosen during the initial configuration of Mac OS X Server

1. Create Users and Groups: Directory Server is configured as Open Directory Master for users and groups and other directory services
2. Import Users and Groups: Open Directory service is configured to connect to an exiting Open Directory or Active Directory to access users and groups records
3. Configure Manually: let you choose to connect to and existing OD or AD o access users and groups; let you choose wether activating a Open Directory Master

Compare and Contrast how the two directory usage roles provide directory data

Stand Alone server	Connect to a Directory System
• Stores users and groups data in the Local Directory Domain • Other computers cannot access the Local Directory • When a client requests a service and try to authenticate the server verify if the credentials are present in the Local Directory • For the configuration you must choose the Manage Users and Groups and deny to generate and Open directory Master	• Users and groups information will be taken from another Directory server or from itself if it's an Open directory Master • Will share the server services with other computers on the network that are connected to the Directory System • You must bind other servers in order to join the directory System

Describe how to use Server Assistant on a Mac OS X Server computer to configure the server to use a local data store for directory data

In the Services pane of Server Assistant choose which services to activate then choose to save data on a local volume (a separate volume respect the System Volume)

Describe how to use Server Assistant to save setup configuration data for a Mac OS X Server computer to a text file so that it can be referenced at a later time

1. In the Review pane of Server Assistant click Details
2. Choose to Save Setup Profile to generate a text file (XML format) that you can use later for the automatic configuration of a server

Describe how to use Server Assistant to save the setup configuration data for a Mac OS X Server as a record in a Directory server so that another Mac OS X Server computer can recognize the record to configure itself

1. When choosing to Save Setup Profile in a text file (also in encrypted format) you can save it in a directory named '`Auto Server Setup`' (including spaces)
2. Place this folder in any volume (except the System Volume) that can be attached to the server during the installation (USB, FireWire, AFP Shares)
3. After the installation of the system the server will search for this folder in any attached volume and if it will be found the system will start configuring itself automatically

Explain the benefits of encrypting a Mac OS X Server configuration file

A Setup configuration file may contain the server activation code and administrator/root password so encrypting it is a good security choice especially if it's not possible to guarantee that the file will not be accessed by others than the System Administrator

Describe the two main purposes of the Server Admin utility

1. Service configuration: you can view information about a service (logs, graphs,start,stop,restart) and manage its settings.
   Before Server Admin can show you the service, you need to enable the service through the Services pane of the server Settings
2. Share Point: you can enable File Sharing via FTP, AFP, SMB, NFS protocols and manage how users can access them via SACL lists

Describe how to configure Server Admin so that specific services offered by a Mac OS X Server are added to the list of those that you can monitor and configure

1. Select the server from the SERVERS list
2. Click the 'Settings' button
3. Click the 'Services' pane button
4. Enable the services you want to manage checking the box by the service names present in the list
5. The enable services will appear under the server name in form of a list

Describe the role of the Server Status widget, including where it runs and which services it can monitor

1. It permits the administrator to monitor several aspects of the server
2. It runs in the Dashboard and can be installed in the server itself or in any other computer connected to the same network
3. It can monitor:
   - Various services and their status
   - Network load
   - Disk usage
4. It is installed with the Server Admin Tools

Describe how to configure the Server Status widget so that it can be used for high level monitoring of a Mac OS X Server computer

You can run multiple instances of the widget configured to monitor the same server. In each instance you can select a different information to be shown as main picture.

State which notifications can be configured in the main settings pane of the Server Admin to trigger an email notification when the condition has been met

1. A disk has less then 'x'% of disk space available
2. New software updates are available for the server
3. A certificate is expired or is about to expire

Describe how to use Server Admin to export configuration settings from specified services from a Mac OS X Server computer, so that they can be imported into a different Mac OS X Server computer

1. You can export configuration settings for specified services choosing `Server > Export > Service Settings`
2. Click the box next to name of the services you want to save the configuration for
3. Choose any destination to save the single configuration file generated

Describe how o use Server Admin to import into a Mac OS X Server computer a list of configuration settings exported from another server

1. Choose `Server > Import > Service Settings`
2. Browse the filesystem to the Configuration Settings file saved previously

Authenticating and Authorizing Accounts

List at least three examples of user authentication on a Mac OS X client computer such as logging in on a client computer, connecting to a file server, authenticating as an admin user for configuration purposes and providing a username and password for a secured website

1. Authenticating in a Local system
2. Authenticating in a Directory Service (by the use of Kerberos)
3. Authenticating on a File Server:
    - Via Kerberos with Single Sign-On if part of a directory service
    - Via Local credentials if is a Stand Alone server
4. Connection to a server with Admin credentials via Server Admin, Server Preferences or Screen Sharing
5. Connect to a website secured via realm

Explain the main purpose of Workgroup Manager in Mac OS X Server

Its main purpose is to create and configure user accounts on Mac OS X Server, both Local and Network accounts

List the four types of Mac OS X Server accounts that can be created and managed by Workgroup Manager

1. User account
2. Group account, collections of users and groups
3. Computer account, permit to define specific configuration for a computer
4. Computer Group account, collection of computers and computer groups

Explain the purpose of the User ID for a User account on a Mac OS X Server computer

The UID is a numerical value that the system uses to differentiate one user from another. Each name is associated with a UID.

Define the term "groups' as it applies to user accounts or a computer

A group account is a collection of accounts

Describe how to use Workgroup Manager to assign specified users to a group account stored on a Mac OS X Server computer

1. Select Group from the list
2. Click the add '+' button in the member list, to show the Users List
3. Drag & Drop one or more user names into the Member List and Save

Describe how to use Workgroup Manager to assign specified groups to a user account stored on a Mac OSX Server Computer

1. Select a User name
2. Click the 'Group' pane button
3. Click the add '+' button by the 'Other Groups' list to show the Groups drawer
4. Drag & Drop one or more Group names into the 'Other Groups' list and Save

Describe how to use Workgroup Manager to export user, group, computer group accounts so that they can be imported into a different Mac OS X Server computer

1. Select the accounts you want to export
2. Choose `Server > Export` from the menu
3. Select the destination folder for the generated file

User passwords are NEVER exported

Explain why it's a best practice to use groups instead of individual user accounts to manage permissions in Mac OS X server

1. A good practice in managing accounts is to keep granularity creating a hierarchical structure of groups that reflects your organization structure
2. In the process you are encouraged to create small groups (in some cases, nested) to assign specific permissions to small numbers of people instead of assigning permissions directly to user accounts
3. This approach makes the longtime management easier as anytime new users are generated it will be necessary to assign them to the proper group to acquire the correct permissions without need to set all the permissions to that user. The same when a user changes department it will be moved to a new group account to obtain new permissions and discharge the old ones

Explain how Unique IDs (UIDs) and Group IDs (GIDs) are used to relate permissions for files and folders to users and groups on a Mac OS X Server computer

1. According to the POSIX standards every file and folder is associated with a UID and GID. If the UID of a user matches the UID associated with an item then the user is identified as the owner.
2. In case a user's primary GID or other groups he's member of, are matching the GID associated with an item then the Group Permissions will be applied

Explain how Guest access and Everyone permissions to files on a Mac OS X Server computer can expose shared items to undesirable access

By default folders and files have the Everyone permissions set to 'read-only', in case the system has the Guest access enabled any computer that can reach the server will be permitted to read those files

Describe how to use Server Admin to modify the POSIX permissions for files and folders on a Mac OS X Server computer to restrict user access to them

1. Select the Server name from the SERVERS list
2. Click the 'File Sharing' button
3. Select the volume
4. Click the 'Browse' button and select the desired folder or file
5. Go to the POSIX section of the 'Permissions' table
6. Click the permissions pop-up menu to select the desired permissions

Explain how POSIX permissions can limit your options when setting up folder and file permission structures that involve multiple users and groups

1. POSIX permissions let you define just 3 levels of control:
   - On the owner
   - On the group
   - Everybody else
2. You need to workaround limitations in the permissions system rather than using it to naturally express your organization's structure

Define the term "Access Control Lists" (ACLs) as it applies to Mac OS X Server v10.6

1. They are lists of Access Control Entries that define multiple permissions to multiple users and groups
2. They add flexibility (with 17 possible options) to the permissions management

Define "Access Control Entry" as it applies to ACLs in Mac OS X Server

1. An ACE is a single entries of a Access Control List and they define a permission of a single account
2. The ACEs order matter, if it's a 'deny' or 'allow' it doesn't matter

Explain the order in which Mac OS X interprets ACEs and POSIX permission settings to determine the effective permissions of a file

The system first evaluate the ACEs, it matching ACEs are not found then it will applies POSIX permissions

Explain how GUIDs associate ACLs to users and groups

1. A GUID is a unique identifier for users and groups represented by a 128 bit number
2. ACLs guarantee unique identification by referring to GUIDs

Describe how filesystem ACLs in Mac OS X Server map to filesystem ACLs in Windows servers

ACLs are supported via SMB protocol

Define "inheritance" as it applies to filesystem ACLs in Mac OS X Server
ACL inheritance lets you determine how permissions pass from a folder to its descendants

Describe Service Access Control Lists (SACLs)
Service ACLs enable you to define who has access to specific services

Explain why a user account may be given administrative capabilities for a subset of the services provided by a Mac OS X Server computer

1. Depending on the organization structure there may be situations where it's necessary to grant administrative privileges to a group of users
2. In most cases those administrative privileges are limited to allow only to monitor services

Using Open Directory

Describe the function of directory services in a networked computing environment
Directory services provide a central repository for information about the computers, applications and users in an organization

List three advantages provided to users and system administrators by networked directory services, including providing a common user experience, providing easy access to networked resources such as printers and servers and allowing users to log in on different computers using a single account

1. User's Home folders can be located on another server and be mounted automatically on any computer the user logs in to
2. You can enforce policies such as password expiration and minimum length
3. You can manage user preferences
4. Provide authentication to Windows users
5. An OD server my work as aWindows PDC or BDC via Samba 3

Explain two 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

1. Providing common authentication information to multiple servers give the opportunity to the network user to access, through a bound client, services provided by different servers on the network using its credentials, without the need of specific credentials for each service
2. Having multiple client computers bound to the Directory System the user is given the capability to log in with any computer and as the OD stores its common configuration data it will be able to transparently load them to activate automounts (such as Home folder), access the designates network printers, load its personalized working environment

Describe the structure and components of Open Directory on a Mac OS X client computer

1. The structure of Open Directory on Mac OS X clients is similar to the one of Mac OS X Servers: the OD service act as intermediary between system and applications
2. Mac OS X clients are NOT enabled to provide sharing directories but they are limited to use a local directory that can manage only local users and services

List and describe the four Open Directory service roles as configured by Server Admin on a Mac OS X Server computer

1. Stand Alone: does not provide directory information to other computers or get directory information from an existing Directory System. The local directory cannot be shared
2. Open Directory Master: can provide directory information and authentication information to other systems
3. Server Connected to a Directory System: can setup the server to provide services that require user accounts and authentication but use accounts that are setup on another server
4. Open Directory Replica: a server host a replicated version of a directory. The replica is synchronized with the OD Master periodically.

Describe how to use Server Admin to configure a Mac OS X Server as an Open Directory Master so that multiple computers on the network can access directory data provided by the Mac OS X Server computer

Assuming that the server is configured as Stand Alone server:

1. Select the server name from the SERVERS list and expand the services list
2. Select the Open Directory service
3. Click the 'Settings' button
4. Click the 'Change' button by the 'Role' description
5. Choose 'Setup an Open Directory Master' and click continue to start the guided procedure

Describe how to use Directory Utility and the address of a Mac OS X Server computer configured as an open Directory Master to configure a Mac OS X client computer to connect to the Mac OS X Server computer for authentication and directory data

1. Enable the LDAPv3 service
2. Click the configuration button (pencil button)
3. Select the location and disclose the Options
4. Click the 'New' button
5. Digit the IP address or FQDN name of the OD Master server
6. Specify your computer ID, the OD Administrator short name and its password in the 'New LDAP connection' window, then click OK to save.

State how many replicas can be connected to a single Mac OS X Server computer and how many total replicas can be part of a single OD network

1. One Master can have 32 replicas
2. Each replica can have 32 replicas
3. So the total amount of replicas will be $32 + (32 * 32) = 1056$ replicas

Describe how to use Server Admin and Mac OS X Server configured as an Open directory Master to determine if any replica computer are connect to the Open Directory Master server

1. Select the Open Directory service
2. Click the 'Settings' button
3. Click the 'General' pane button
4. Click the 'Replica Tree' pane button to visualize the OD Master address and the master replicas

Describe how to use Server Admin connected to a Mac OS X Server computer to display Open Directory service-related log files

1. Select the Open Directory service
2. Click the 'Logs' button
3. Select which log to visualize from the pop-up menu at the bottom of the form

Describe how to user Server Admin to archive the Open Directory data on a Mac OS X Server to a disk image file so that the data can be restored later

1. Select the Open Directory service
2. Click the 'Archive' button
3. Click the 'Choose' button next to 'Archive in' field
4. Choose an external location for the archive, click the 'choose' button
5. Choose an archive name and password, click OK

State what data is archived when the Open directory Archive function is used with Mac OS X Server

1. LDAP database
2. Password Server database
3. Kerberos Key Distribution Center (KDC)
4. Local database and passwords
5. Local KDC
6. Hostname and directory service fils

State which utilities are used to configure the Open Directory service in Mac OS X Server and the primary purpose of each

1. Server Admin: gives full control over OD management and setup
2. Server Preferences: setup Mac OS X Server to be OD Master. Designed to manage only network accounts
3. Server Assistant: configure an OD Master automatically during the initial setup

Describe five methods a Mac OS X Server can use to provide authentication

1. Hash files: `NTLMv1, NTLMv2, MS-CAHP2;` hash files are stored where only the root user has access
2. Crypt passwords: stored in the user accounts; for backward compatibility purpose only
3. Kerberos: Single Sign-On authentication system
4. Password Server: password database for the applications that do not support kerberos
5. Shadow password: stored in a location accessible by the root only; for local-only users

Describe how to use Workgroup Manager to disable a specified user account so that it can no longer be used for authentication purposes, without deleting it

1. Select the account name
2. Click the 'Basic' pane button
3. Uncheck the 'access account' box

Describe how to use Workgroup Manager to configure user accounts on Mac OS X Server so that when a user changes its password, the password conforms to a set of password policies

1. Select the account name
2. Click the 'Advanced' pane button
3. Click the 'Options' button to show the password policy settings

Describe how Kerberos provides both identification and authentication services

Single Sign-On system is implemented through KDC system

Describe the following terms as they apply to Kerberos

1. Ticket: refers to Kerberos Tickets that give you access to directory services
2. Kerberos Distribution Center: is the service responsible for mediating between the user and the service
3. Ticket Granting Ticket: is a Ticket-to-Get-Tickets. It's generated by the KDC, if decrypted gives you access to service tickets
4. Service Ticket: the service ticket is given by the KDC to the user, the user will spend the ticket with a specified service. The service and the KDC do not need to communicate.

List four possible reasons a client computer might not be able to use Kerberos authentication to access a service

1. DNS configuration issue: DNS server may resolve address incorrectly and the Kerberos ticket won't be usable
2. Mismatch in time settings between the client and the server computers: Kerberos authentication is based on encrypted time stamps, by default difference of more then 5 minutes are not tolerated
3. Kerberos authentication disabled for a service
4. A user account not configured properly

Given the `ktutil` utility on a Mac OS X client computer, display the Kerberos tickets that have been granted to the computer

1. `$sudo ktutil`
2. `ktutil: read_kt /etc/Kirby.keytab`
3. `ktutil: list`

Describe how to troubleshoot a situation where a client computer is unable to use Kerberos to authenticate and access Kerberized services provided by a Mac OS X Server

1. Ensure that the DNS service you use is resolving addresses correctly
2. Make sure that the clocks for all computers are synchronized
3. Make sure that Kerberos authentication is enabled for the service in question
4. Refer to the `password-service` and `password-error` logs
5. View the user's Kerberos Tickets with Ticket Viewer application or `klist` CLI command

Given a user account stored on a Mac OS X Server computer, determine the appropriate password type for the account to use

1. Local user: shadow password, because supports multiple traditional authentication methods
2. Directory user: Open Directory Password Server/Kerberos

Crypt Password should be used just to provide backward compatibility with OS X 10.1 or earlier

State which utilities are used to set password policies for Mac OS X Server user accounts; state which password policies can be applied to a user account in Mac OS X Server

1. Workgroup Manager to apply User Account Setting policies (per-user password policies)
2. Server Admin to apply Global Policies

Using File Services

List the file sharing protocols that can be used to share files from a share point on a Mac OS X Server computer

1. AFP
2. SMB
3. FTP
4. NFS

Describe the four basic steps to set up file services

1. Planning, determine your organization requirements:
   - How are users organized?
   - What is the logical structure to follow assigning users and groups?
2. Configuring accounts, through Workgroup Manager create a group structure that best matches the organization's needs
3. Configuring file service, through Server Admin configure the service settings such as:
   - Maximum number of clients
   - Guests access
   - Logging levels
4. Monitoring the service, monitor service usage and unexpected activity through the logs accessible by Server Admin

Explain two issues related to configure a share point to share files over two different protocols

1. Volume Format case-sensitive: the issue arise when client and server support different case-sensitivity
2. Filesystem permissions: there may be issues in the compatibility with ACL implementation between client and server

Describe how to use Server Admin to configure a folder on a Mac OS X Server to act as Share Point

1. Click the 'File Sharing' button
2. Double-click on the volume listed, to browse its content
3. Select the folder to share and click the 'Share' button
4. The Sharing Point will appear in the 'Sharing Point' list

Describe how to use Server Admin to configure a share point in a Mac OS X Server as a Time Machine repository for Mac OS X client computers

1. Once enable the folder to act as Sharing Point, click the 'Sharing Point' button
2. Select the new Sharing Point
3. Click the 'Share Point' pane button in the bottom of the window
4. Check the 'Enable as Time Machine backup Destination' box

Describe how to use Server Admin to enable Spotlight to search a Share Point on a Mac OS X Server

In the same way you enable the Share Point as a Time Machine Backup Destination you can check the 'Enable Spotlight Searching' box

State what tool is used to create and manage Share Point in Mac OS X Servers

Server Admin

Describe how to use Server Admin to configure an AFP share point on a Mac OS X Server computer so that client computers can access the files on the share point without having to provide a user name and password

In the 'Share Point' pane enable ' the 'Automount' option and click the 'Edit' button to configure the mountpoint protocol

Describe how to use Server Admin to configure a Mac OS X Server's AFP service greeting message to display once per user session

1. Select the 'AFP' service
2. Click the 'Settings' button
3. Click the 'General' pane button
4. Set the greeting message and check the 'Do not send same greeting twice to the same user' box

Explain the usefulness of an Administrator user's ability to masquerade as any registered user for the AFP service on a Mac OS X Server computer

This feature is useful in the why the Administrator has the ability to verify standard users accessibility to offered service

Describe how to use Server Admin to configure a Mac OS X Server computer's AFP service to allow an administrator to masquerade as any registered user

1. Select the 'AFP' service
2. Click the 'Settings' button
3. Click the 'Access' pane button
4. Click the 'Enable administrator to masquerade as any registered user' box

Describe how to use Server Admin to configure a Mac OS X Server AFP Service to limit the number of simultaneous guest connections to a specified number of users

In the 'Access' pane enable Guest access and check the option button by 'Guest Connections' and fill the apposite field with the number of maximum guest connections you want to grant

Describe how to use Server Admin to configure a Mac OS X Server's AFP service to disconnect idle users when a specified time limit is reached

1. Select the 'AFP' service
2. Click the 'Settings' button
3. Click the 'Idle Users' pane button to get the options or configure the idle users management

List the types of AFP activities that can be logged

1. Logging in
2. Logging out
3. Opening files
4. Creating files and folders
5. Deleting files and folders

List the two log files that provide AFP service specific info in Mac OS X Server

1. AppleFileServiceAccess.log
2. AppleFileServiceError.log

Describe how the different authentication method choices for the AFP service in Mac OS X Server effect how a user authenticate

1. Standard: will use the standard Shadow Password method, the user must enter username and password
2. Kerberos: will use Single Sign-On method credentials, so the user doesn't need to authenticate again as is already logged in
3. Any Method: will first try with Kerberos authentication, if it fails will try the standard method

Explain how an administrator can masquerade as a registered user in Mac OS X Server

This option permit to provide a standard username in the authentication form and out any administrator password, the administrator do not need to know or reset the user's password to test its permissions

Describe how a Windows client access a shared Server Message Block (SMB) volume that resides on a Mac OS X Server computer

Once computer name and workgroup name are configured for the Mac OS X Server it can be browsed just like any other Windows server on the network

Explain the difference between the specified permissions and inherited permissions models as they relate to assigning permissions to new files and folders on a SMB share point hosted by a Mac OS X Server computer

1. Inherit permissions from parent: this option means that the new item will have the same permissions as the folder that contains that item
2. Assign as follow: you can use the pop-up menu to specify "Read & Write", "Write Only", "Read Only" and "No Access" for owner, group and others

Define the terms `oplock` and `strict locking` as they apply to the SMB service in Mac OS X Server

1. Oplocks (Opportunistic Locks): client-side performance enhancement, the client caches the file locally in order to perform read and write operations locally and save network bandwidth
2. Strict Locking: the SMB client must request a lock for an entire file as opposed to only a portion of the file, SMB service will check for an existing file lock with every read and write request

List and describe the four roles provided by the Windows service on a Mac OS X Server computer

1. Standalone: provides file services, but does not provide any Windows Authentication Service
2. Domain Master: provides file services by authenticating the user against an external domain controller
3. Primary Domain Controller (PDC): provides file service and Windows Authentication Service
4. Backup Domain Controller (BDC): act as a replica of PDC (can be configured on a Mac OS X Open Directory Replica server)

Define WINS registration as it applies to Mac OS X Server

Register with WINS server allows you to become the client of an existing WINS server by specifying its IP address or name, WINS act as a DNS server for NetBIOS protocol clients

Describe how to use Server Admin to configure a share point on a Mac OS X Server computer so that a a client computer can access the share point via FTP without a username and password

1. Select the FTP Service
2. Click the 'Settings' button
3. Click the 'General' pane button
4. Click the 'Enable Anonymous access' box

Describe how an FTP client requests the Mac OS X Server FTP server to perform file conversions before sending the files

The client must request the items adding a specific file extension such as:

- .tar
- .gz
- .tar.gz
- .dmg
- .bin (for forked files)
- .bin.gz
- .bin.tar
- .bin.tar.gz

Describe how to use Server Admin to isolate and resolve FTP service issues

1. Make sure FTP service is on
2. Make sure user has correct access privileges to the shared volume
3. See if there's any problem with Directory service
4. Verify IP filters or SACLs
5. Use the FTP service log

Explain what passive FTP is and when it would be used

1. It is a client-side feature that causes the FTP server to open a connection to the computer on a dynamically determined port
2. It is commonly used to access an FTP server behind a firewall

Explain how Mac OS X Server uses user IDs for access control in NFS volumes

The server simply trust what the client tells him, so the user presented by the client is used to perform items handling on the server assigning the relative permissions.

This may expose the server to identity spoofing attacks.

Describe how to use Server Admin to configure an NFS share point on a Mac OS X Server so that any client who access the files as root, access them as Nobody (GUEST)

1. Select the NFS service
2. Click the 'Share Points' button
3. Select a share point
4. Click the 'Share Point' pane button
5. Click the 'Protocol options' button
6. Select the 'NFS' pane button
7. Select 'Root to Nobody' in the 'Mapping' pop-up menu

Describe how to use Server Admin to configure the security level for a NFS share point on a Mac OS X Server

You find the security pop-up menu beneath the mapping pop-up menu and it offers options such:

- Standard
- Any
- Kerberos v5
- Kerberos v5 with data integrity
- Kerberos v5 with data integrity and privacy

Describe how to determine the URL used by a client computer to access an NFS share point on a Mac OS X Server

1. `$: showmount -e nfs.server.name`
   Lists the names of the NFS exports available on nfs.server.name
2. The URL is created like this:
   `nfs://ifs.server.name/Share_Point_Absolute_Path`

Explain two benefits of providing automounts

1. Provide Network Home Folders:
   - The user will be able to access its own settings and items from any connected client
   - The Home folders can be placed on any server part of the Directory System so to distribute the network load
2. Sharing OS resources such as System Files and Applications:
   - It's possible to share applications stored on the server
   - Share fonts and files

List the file sharing protocols that can be used to serve Home folders hosted by Mac OS X Server

1. NFS
2. AFP
3. SMB (only for Windows Clients)

Given a need for an automount share point and Server Admin, select the appropriate type of automount

1. NFS for UNIX clients
2. AFP for Mac clients

Explain how to configure a disk quota for a user account

1. Run the workgroup Manager and select the OD directory
2. Click the 'Accounts' button
3. Select the username from the list
4. Click the 'Home' pane button
5. Define the quota available for the user in the 'Disk Quota' field

Hosting Mail Services

Explain three reasons for hosting a Mail server

1. Limited network bandwidth: better use of network bandwidth, especially if large attachments are handled, as all the mail is kept in your server
2. Increased security: confidential data is stored in your premises and there's minor risk for it to fall into the wrong hands and also email password do not transit in internet
3. Enhanced control: you can setup all the options needed by your organization while external mail services may not offer all the options you need

Define the terms POP, IMAP and SMTP as they apply to mail service

1. POP (Post Office Protocol) is a common retrieval protocol used in mail servers where disk space and network connections are at a premium; makes quick connections and do not support server-side folders
2. IMAP (Internet Message Access Protocol) is another retrieval protocol, it allows the storage of emails and email folders on the server; mail clients will often remain connected for the duration of the user session resulting in a quicker notification of new messages resulting in a large bandwidth consumption
3. SMTP (Simple Mail Transfer Protocol) is responsible for delivering a message from the sender's email server to the recipient's email server

Explain how a message travels from a source client computer through multiple mail servers and is received by a destination client computer

1. The client computer send the message to its mail server via SMTP
2. The sender's mail server identify the recipient's mail server consulting MX entries in the DNS servers and send the message to it; the message may travel through many servers that will tag the message with the name of the server and the time it was processed
3. The recipient computer retrieves the message from its mail server via POP or IMAP or other protocols

Explain how when handling outgoing email a mail server identifies the network address of the destination mail server

1. The outgoing mail server first look up the address of the destination Mai eXchange (MX) server using DNS
2. A given internet domain can have multiple MX servers to help balance the load and provide redundant services, each MX is assigned a priority; highest priority = lowest number

Describe how to use Workgroup Manager to enable a user account in Mac OS X Server to send and receive emails

1. Select the user name from the list
2. Click the 'Mail' pane button
3. Select the 'Enable' option to access and configure the mail account

Describe how to use Server Admin to configure the mail service on a Mac OS X Server computer so that users can access their mail accounts via a web browser

1. Once the mail service is up and running select the 'Web' service from the list
2. Click the 'Sites' button
3. Click the 'Web Service' pane button
4. Check the 'Mail' box to activate the Web Mail interface

Define the term 'cluster' as it applies to mail servers

1. It consists of multiple mail servers that share the mail store by the use of Xsan
2. This provides mission critical redundancy and high performance
3. Easy to maintain using Xsan tools and software

Describe how to use Server Admin to configure the mail service on a Mac OS X Server computer to participate in a Mail Cluster

1. Select the 'Mail' service
2. Click the 'Settings' button
3. Click the 'Advanced' pane button
4. Click the 'Clustering' pane button
5. Click the 'Change' button by 'Mail Clustering' status description to get the available options

Define the terms 'Open Relay' and 'spam' as they apply to mail servers

1. Spam is unsolicited junk mail
2. Open Relay are servers that allow anyone to send messages through them (suitable for spammers)

Describe how to use Server Admin to configure the mail service on a Mac OS X Server computer to enable the authentication methods for POP, IMAP and SMTP to increase the server's security

1. Select the 'Mail' service
2. Click the 'Settings' button
3. Click the 'Advanced' pane button
4. Click the 'Security' pane button to get the available authentication options

Describe how to use Server Admin to configure the mail service on a Mac OS X Server to only relay emails from trusted mail servers

1. Select the 'Mail' service
2. Click the 'Settings' button
3. Click the 'Relay' pane button
4. Check the 'Accept SMTP relays only from these hosts and networks' box
5. Specify networks, addresses, hostnames if the trusted mail servers

Describe how to use Server Admin to verify that the mail service on a Mac OS X Server computer is not acting as an Open Relay

Use third party Open Relay Tests like www.abuse.net/relay.html

Define the term 'blacklist service' as it applies to mail servers

It's a service that publishes and updates lists of known open-relay servers that may origin spamming activities

Describe how to use Server Admin to configure the mail service on a Mac OS X Server computer to reduce the amount of incoming spam sent to local users

1. Go to the 'Relay' pane of the 'Settings' for 'Mail' service
2. Check the 'Refuse all messages from these hosts and networks' box and specify the known spam servers
3. Check the 'Use the junk mail rejection servers (real-time blacklist)' box and specify the blacklist servers that contain open relay server lists

Describe how to use Server Admin to configure the mail service on a Mac OS X Server computer to scan incoming email for junk mail

1. Select the 'Mail' service
2. Click the 'Settings' button
3. Click the 'Filters' pane button to get the spam filtering options and virus filtering options

Describe how to use Workgroup Manager to configure the quota for a user account so that it does not use more than a specified amount of disk space to store email

1. Select the user name from the list
2. Click the 'Mail' pane button
3. Configure the 'Mail Quota'

Describe how to use Server Admin to configure the mail service on a Mac OS X Server computer so that a user is sent a warning message when the amount of incoming email for a user account on the server exceed a specified warning percentage

1. Select the 'Mail' service from the list
2. Click the 'Settings' button
3. Click the 'Quotas' pane button
4. Check the 'Enable Warning when usage exceed' box and define the percentage, you can also edit the Quota Warning Message

Describe how to use Server Admin, a Mac OS X Server computer and a list of email addresses to create a mailing list so that an email sent to a single email address is distributed to multiple users

1. Select the 'Mail' service
2. Click the 'Settings' button
3. Click the 'Mailing Lists' pane button
4. Check the 'Enable mailman mailing list' box
5. If it's the first time you configure a mailing list, define the Master password and Administrators, and the 'Mailman' mailing list will be created to track them
6. Create a new mailing list `mailing.list.name` an add users
7. From now on all the messages sent to mailing.list.name@your.domain will be sent in copy to all the mailing list members

Describe how to use Server Admin to set the appropriate log level for the SMTP, IMAP/POP and Junk Mail logs according to specified operating conditions such as normal, under spam attack, users unable to end or receive email

1. Select the 'Mail' service
2. Click the 'Settings' button
3. Click the 'Logging' pane button
4. Adjust the logging level accordingly to the operating conditions

Describe how to use SMTP or POP/IMAP log files, Server Admin and a Mac OS X Server computer to identify messages that can help diagnose why a user is a unable to send or receive email using the server

1. In Server Admin select the 'Mail' service of your Mac OS X Server
2. Click the 'Logs' button
3. Select the log file name related to the service to troubleshoot, from the pop-up menu
4. Research for specific strings like 'error' or email addresses you are trying to use to send or retrieve
5. The logs will be able to identify if email address are mistyped or if the user is over quota, if the user is having problems retrieving its emails you'll recognize failed authentication attempts in the logs

Describe two methods to limit the amount of disk space used by the Mail service in Mac OS X Server

1. Setting quotas: will control the total amount of disk space a give user can occupy with all its email that is stored on the server
2. Setting the maximum incoming message size prevents the possibility of running out of disk space as a result of a few huge messages coming into your server

Managing Web Services

State the standard web server on which the web service in Mac OS X Server is based

1. Apache 2.2.11

Describe how to use Server Admin and a Mac OS X Server computer to create a new website

1. Select the 'Web' service
2. Click the 'Sites' button
3. Click the 'add' ('+') button at the bottom left of the site list
4. Configure the parameters for the new created site

Describe how to use Server Admin to disable a website on a Mac OS X Server computer hosting web service so that the site is not accessible by other computers

1. Select the 'Web' service
2. Click the 'Sites' button
3. Select the site name you want to disable for other computers
4. Change the 'IP Address' pop-up menu to 'other' and specify the loopback address (127.0.0.1) so that the site is accessible only by the server itself

State the default location where a Mac OS X Server computer's main website files are stored

`/Library/WebServer/Documents`

Describe how to use Server Admin to configure the location of the data files for a website hosted on a Mac OS X Server computer

1. Click the 'File Sharing' button
2. Select a volume and browse the directories until the point where you want to put the website data file
3. Create the appropriate directories and files and assign them the permissions: at least give ability 'read' for the group '`_www`'
4. Select the 'Web' service from the list of services
5. Click the 'Sites' button
6. Create a new site
7. Specify the path of the newly create folder for the website data into the 'Web Folder' field
8. Save and restart the service

State which group on a Mc OS X Server computer must have read access to files that are to be saved by the web service

Group 'www'

Describe how to configure the permissions of a set of files on a Mac OS X Server computer hosting web service so that the files can be saved by the web service

1. Manage file permissions through the 'File Sharing' button of Server Admin
2. Ensure that the directory and files are at least 'read' for the group 'www'

List the three different methods for distinguishing between multiple websites hosted by Mac OS X Server computer so that the files can be saved by the web service

Using a unique combination of those 3 values you can save many different websites each with different data files:

- Host name (domain name)
- IP Address (which address or subnet is allowed to see the website)
- Port number (service port dedicated to the web site)

Describe how to use Server Admin to add an alias to a website hosted by a Mac OS X Server computer, so that the server responds to the new name

1. Select the 'Web' service
2. Click the 'Sites' button
3. Select ht website you want to add an alias for
4. Click the 'Aliases' pane button
5. Delete any '*' from the 'Web Server Aliases' field and add the domain name of the website and all its aliases
6. Save and restart the web service
7. Select the 'DNS' service
8. Click the 'Zones' button
9. Select the zone name your web service belongs to
10. Click the 'Add Record' button and select the 'Add Alias (CNAME) option
11. Specify the alias and the main domain name as 'Destination'; Save

Define the "realm" as it relates to a web server

They are essentially directories or locations that can only be accessed by certain users and groups

State the reason to enable the Folder listing option, for example, to provide a simple interface to a collection of files to be made available to users via the web service

A site that hosts files or applications for visitors to download may want its entire folder structure to be seen, which makes navigation of the site easier

Define the term "modules" as they apply to the web service in Mac OS X Server

They are pieces of code, extensions, that extend Apache functionalities

Describe how to use Server Admin to create realm so that access to a website running on a Mac OS X Server computer or to a portion of the site, is restricted to specified users

1. Select the 'Web' service
2. Click the 'Sites' button
3. Select the website you want to create realm for
4. Click the 'realm' pane button
5. Click the 'add' ('+') button to create a new realm
6. Specify the name, the authentication method and the portion of website you want to secure
7. On the right pane define the access permissions by users or groups

List the types of logs generated by the web service in Mac OS X Server

1. Access logs
2. Error logs

State the protocol used by WebDAV to share files

`http`

Describe how to use Server Admin to configure the permissions for a folder of files on a Mac OS X Server computer to allow for read/write access over WebDAV

You need to setup permissions in realm to permit WebDAV users to read and write items of the website

Given the address of a Mac OS X Server computer sharing files via WebDAV state the URL to access the files

`http://webdav.server.address`

Compare and contrast WebDAV with other common file sharing protocols such as AFP, SMB, FTP discussing security issues, format of the URL used to access and benefits of using each

	AFP	SMB	FTP	NFS	WebDAV (HTTP)
Native	Mac OS X	Windows	Multi platform	UNIX	Multi Platform
Security	Kerberos or Standard	Kerberos or NTLMv2	Kerberos or clear-text	Kerberos or NONE	Kerberos, digest, basic
Browseable	YES	YES	NO	YES	NO
Example URL	afp:// server.domain	smb:// server.domain	ftp:// server.domain	nfs:// server.domain	http:// server.domain

Using Collaborative Services

Define the term "wiki" as it applies to Mac OS X Server

A wiki is a collaborative web-based tool that allows users and groups to post information in a manner that promotes the logical progression of an idea, a project a theme or any other focal point within an organization

State three benefits of setting up a wiki server

1. Secrecy of information: a group of users can post, edit, review and discuss material of a "secret" project without interference from other groups
2. History of information: detailed history of information is kept and retrievable at any time
3. Possibility to define users and groups that are allowed to create wikis

Define the term "weblog" as it applies to Mac OS X Server

Also know as "Blog". It permits users and groups to catalog their experiences surrounding a project or a theme, organized in chronological format

Describe how to use Server Admin to enable the wiki and blog services for a website hosted on a Mac S X Server computer

1. Select the 'Web' service
2. Click the 'Sites' button
3. Select the website you want to enable wiki and blog for
4. Click the 'Web Services' pane button
5. Check the 'Wikis' and 'Blogs' boxes, then save

Describe how to use Server Admin to add specified group to a list of those that can create a wiki on a website hosted on a Mac OS X Server computer

1. Select the 'Web' service
2. Click the 'Settings' button
3. Click the 'Wiki' pane button
4. Add users and groups in the 'Wiki Creators' list

Describe how to use a Mac OS X Server computer hosting a wiki-enabled website and a client computer with a web browser to create a wiki hosted on the server

1. In the browser of the client computer enter the Mac OS X Server FQDN URL
2. Click the WIKIS link and authenticate with a realm enabled user with permissions to create wikis
3. In the 'wikis' page click 'Create a new wiki' to start a guided procedure in 3 steps creation :
    1. Name & Description
    2. Theme choice
    3. Permissions: public or private

List the reasons according to the Mac OS X Server documentation why you would want to provide shared calendar services using iCal service on a Mac OS X Server computer

1. Share Calendars
2. Schedule meetings
3. Coordinate events

Identify a reason why you would need to establish quotas for users of the iCal service on Mac OS X Server

To prevent users from attaching large files to every event they have

Describe how to use a Mac OS X Server computer that is hosting shared calendars and iCal on a Mac OS X client computer to configure iCal on the client computer so that it displays the share scheduling data provided by the iCal service

1. Open iCal on the client computer
2. Select `iCal > Preferences` from the menu
3. Click the 'Accounts' button
4. Click the 'add' ('+') button to create a new account
5. Select the 'CalDAV' as account type, fill username, password and address files of the account and server information of the server hosting the iCal service
6. Complete the configuration and save

Describe how to use a Mac OS X Server computer that is hosting shared calendars, and Directory services on a Mac OS X client to create new resources on the iCa; server that can be scheduled using iCal on the client computer

1. Open 'iCal Server Utility' on the Mac OS X Client computer
2. Click the 'add' ('+') button to create a new 'Location' or 'Resource'
3. Authenticate with a valid network account
4. Configure the new 'Location' or 'Resource' and save

Describe how to use Server Admin and Mac OS X Server computer with iCal service enabled to troubleshoot issues with the iCal Server

1. Increase the log level to 'Info'
2. Consult:
   - `/var/log/caldavd/error.log`
   - `/var/log/caldavd/access.log`

State which protocols are used by the iCal service in Mac OS X Server

1. CalDAV (Calendar Server Extensions for WebDAV)
2. HTTP to access files

State which protocol is used by the chat service in Mac OS X Server

1. Jabber: familiar name
2. XMPP (Extensible Messaging and Presence Protocol): official name

Explain the benefits of setting up a chat server

1. Automatically generated chat transcripts:
   - Users can review their chat logs of a conversation
   - root user can access all logged messages
2. Increase of security:
   - Chats kept within the organization (avoid the use of external servers), restriction to certain users and groups, private and controlled chats

Describe how to use Server Admin to modify the list of host domains that the chat service in Mac OS X Server will connect to

1. Select the 'iChat' service from the list
2. Click the 'Settings' button
3. Click the 'General' pane button
4. Specify the Host Domain you want iChat service to connect to

List the methods that can be used by the iChat service in Mac OS X Server to authenticate iChat clients

1. Standard: to only accept password authentication
2. Kerberos: to only accept Kerberos authentication
3. Any Method: to accept both password and Kerberos authentication

Describe how to determine the iChat server screen name for a specified user account on a Mac OS X Server computer

They are Jabber ID and use the general format `user-short-name@domain.name`

Describe how to add a service account to iChat on the client computer so that it can be used to chat with other iChat users via the iChat service on a Mac OS X Server computer

1. Open iChat on the Mac OS X client computer
2. Select `iChat > Preferences` from the menu
3. Click the 'Accounts' button
4. Click the 'add' ('+') button to add a new account
5. Select 'Jabber' from the 'Account Type' pop-up menu
6. Enter a valid account name and password
7. Click 'Continue' and then 'Done'

Describe how to use Server Admin and a Mac OS X Server computer that is hosting iChat service to display chat messages, if any, that have been stored on the server

You need root access to view the `jabbered_user_message.log`

Explain the purpose of the federation feature for the iChat service in Mac OS X Server

1. Allows two Mac OS X Servers running iChat services to join, it also allow any other XMPP chat service to join as well
2. An organization may have more then one Mac OS X Server using iChat service, it is possible to join them together allowing users and groups in both OD to communicate

Describe how to use Server Admin to enable the server-to-server federation feature for the iChat service

1. Select the 'iChat' service
2. Click the 'Settings' button
3. Check the 'Enable XMPP server-to-server federation' box
4. Configure the federation preferences

Describe how to use Serve Admin to display the iChat service log on a Mac OS X computer

In the 'iChat' service pane click the 'Logs' button and select 'iChat Service Log' from the pop-up menu (`/var/log/system.log`)

Describe how to use system log file for a Mac OS X Server computer to identify the users that are currently connected to the iChat service

Enter 'session started' in the search field to see all users, dates and times that sessions have begun

Explain how contact data is shared between Mac OS X client computers and the Address Book service on the Mac OS X Server

1. It uses CardDAV protocol (an extension of WebDAV)
2. It enables users to store contacts in the server and to access those contacts with multiple computers and devices

Describe how to configure the Address Book service so that users can store contact information on the server

1. Select the 'Address Book' service
2. Click the 'Settings' button
3. Configure the 'Data Store location' under the 'General' pane
4. Configure the 'Authentication Type' under the 'Authentication' pane

Explain how to configure a Mac OS X client computer to access shared contact information provided by the Address Book service on a Mac OS X Server computer

To access the shared contact information the is no need for any configuration: it's only required that the Mac OS X client computer is bound with the Directory service, so Directory Services item will appear in the Group Column of the Address Book application

Describe how to use a Mac OS X computer and a Mac OS X Server computer hosting the Address book service to configure the client computer to access contact information stored on the server

1. Open Address Book on the Mac OS X client computer
2. Select '`Address Book > Preferences`' from the menu
3. Click the 'Accounts' button
4. Click the 'add' ('+') button to add a new account
5. Select 'CardDAV' as account type
6. Fill the form with a network user's credentials

Implementing Deployment Solutions

Explain five problems that are solved by using NetBoot server

1. Rapidly update a large number of computers with newer system software:
   Computers may start up an installation without user interaction from the same Network Install Image, without need to load forma a DVD drive so there's no need to repeat the installation process for every single computer
2. Simply repurposing a number of computers with a different software including Operating System and applications:
   It's possible to prepare different NetBoot boot images containing different OS and software so that you can restart the computers every time with a different Network Boot Image, ideal for uses in schools so every classroom may have different system configuration
3. Emergency boot disk when a drive on a client computer has failed:
   Its a good practice to prepare a NetBoot boot image containing diagnostic and repair tools so that an administrator can boot a computer with this service boot image and perform troubleshooting operations on the hard drive of the computer or other diagnostics on the computer without the need of overwrite the computer's data
4. Quickly revert system such as kiosks to a known 'clean' state:
   So we are sure that users cannot compromise the computer installing unsolicited software, and also for privacy purpose all the caches and information shared by a user session are erased at the next restart
5. Quick and easy method for imaging computers with a variety of configurations:
   As it's possible to create Restore Images from configured and personalized existing systems, so to quickly restore a system to a working status in case of hard drive failure or system corruption

Define the term 'NetBoot' as it applies to Mac OS X Server

It's the service that permits client computers to start up using system software that they access from a server instead of the client's local hard drive

List the initial steps a client computer goes through when it is configured to boot using a NetBoot server

1. The client places a request for an IP address
2. After receiving the IP address it requests the startup software. The server delivers a boot ROM via TFTP protocol
3. It receives the Boot ROM and initiate to mount and load the images for NetBoot network disk image, served by http or NFS
4. After booting the NetBoot image, a new request for DHCP IP address is placed

Describe how to use a Mac OS X computer that has the Mac OS X Server administrator tools installed to locate the System Image Utility application

The System Image Utility is located on the `/Application/Server` folder

Explain how network home folders complement a NetBoot system by providing users a location to store personal data and preferences

1. When a client computer boot and load from a NetBoot image all the data that the user need to write to the computer drive is redirected to a shadow file in the server that is erased when the user session ends so that all data is lost forever
2. If we need to allow users to save their information and data it becames useful to assign them a network account with the Open Directory service and assign them a network shared home folder so that when they login in a NetBoot booted computer their network shared home folder is mounted automatically and their information are permanently stored on the network share

Explain the difference between the three types of System Image Utility Images

1. A Boot Image is a file that looks and acts like a mountable disk or volume
2. An Install Image is a special boot image that boot the client long enough to install software from the image after which the client can boot from its own hard drive
3. A Restore Image is the same as an Install Image with the difference that it's generated by a configured system volume instead of an Install DVD/CD

List the three types of sources that can be used to create a NetBoot Image or NetInstall Image

1. Mac OS X Install DVD, replicate the experience of starting from the install disc but without the need of having a DVD drive available
2. Mounted Volumes, image creation is much faster then when using discs. Installations made with images created in this way are faster respect using disc-created images
3. Disk Images (of a configured hard drive), you can use Disk Utility to create an image of an existing volume; when creating the image you have the option of adding additional software to the image and include updates

State the minimum Mac OS version for a NetBoot or NetInstall image source

System Image Utility can only build images of Mac OS X v10.6

Describe how to use the System Image Utility running on Mac OS X computer and an appropriate image source to create a NetBoot image that can be used by the NetBoot service on Mac OS X Server computer

1. Launch the System Image Utility from `/Applications/Server` folder
2. Mount an Installation or System volume image, or insert a Mac OS X 10.6 installation disc
3. When the mounted volume appear in the sources list select it and you will be given the options available to create a NetBoot Image

State the location on a Mac OS X Server computer where a NetBoot image should be stored so that it can be used by the NetBoot service

`/Library/NetBoot/NetBootSP`*n*

State the minimum network requirements to support client computers booting using the NetBoot service on a Mac OS X Server

Hardware requirement:

1. 100 Base-T Ethernet, up to 10 clients
2. 100 Base-T switched Ethernet, 10 to 50 clients
3. 1000 Base-T switched Ethernet, beyond 50 clients

Software requirement:

1. HTTP or NFS service
2. Optionally AFP and DHCP services

Describe how to use Server Admin to configure the NetBoot service to share NetBoot Images over a specified network port

1. Select the 'NetBoot' service
2. Click the 'Settings' button
3. Click the 'General' pane button
4. Enable the port you want the service to be active on, choose from the list of ports

State three methods that can be used to configure a client computer to boot using an image provided by a NetBoot server

1. Keep pressing the 'N' key in the keyboard when you switch on the Mac computer
2. Keep pressing the 'Option' (ALT) button when you switch on the Mac computer bad then choose the icon representing the available NetBoot Images
3. Open 'System Preferences', go to the 'Startup Disk' pane, choose the NetBoot Image and restart the computer

Describe how to use Server Admin to configure which image among multiple images hosted by a Mac OS X Server will be a default image used by the NetBoot service

In the 'Image' pane of 'NetBoot' service 'Settings', select the image you want to be the default option and click the 'default' option button

Define the term 'shadow files' as it applies to the NetBoot service in Mac OS X Server

Shadow files are used for NetBoot clients that don't use their local hard drive to write out data when booted

Describe how to use a set of NetBoot log files for a NetBoot service that is not serving images to client properly to identify the issue

Change the logging level and consult them via Server Admin

Describe how to use System Image Utility to configure a NetBoot image to change ByHost preferences after it has been installed

1. Mount a valid volume to create a NetBoot image
2. Open 'System Image Utility'
3. Click the 'Customize' button
4. Start creating a workflow from Image Customization
5. Add the action 'Apply System Configuration Settings'
6. Click 'Change ByHost preferences to match client after install'

State the minimum system requirement for client computers booting using the NetBoot service in Mac OS X Server

1. 512MB of RAM
2. Ethernet support
3. Latest updates for NetBoot System Disk Images

Describe the purpose of the filters in the NetBoot Service on a Mac OS X Server computer

Filters allow or deny the use of the service by MAC address, allow NetBoot clients to coexist with non-NetBoot clients and remove the risk to allowing non-NetBoot clients to access unlicensed applications or to accidentally perform a network installation

Managing Accounts

List six reasons one would use Mac OS X Server to manage user account preferences

1. Provide users with a consistent, controlled interface while allowing them to access their documents from any computer
2. Control permissions on mobile computers
3. Restrict certain resources for specific groups or individuals
4. Secure computer used in key areas such as administrative offices, classrooms or open labs
5. Customize the user experience using group folders
6. Customize Dock settings
7. Control access to software updates

Compare and contrast the characteristics of network user accounts and local user accounts in Mac OS X Server

Local User Account	Network User Account
• User account information stored on the computer • Home folder stored on the computer • User configuration on each computer has to be managed individually	• User account information stored in any Directory service • Home folder stored in any file server (part of the Directory) • User configuration managed centrally on the Directory by any of the bound computer by Workgroup Manager application

Identify which Mac OS X Server Utility is used to manage user account permissions and account preferences

Workgroup Manager

Describe how to use Workgroup Manager to enable the Inspector so that directory data in a Mac OS X Server can be examined

1. Choose '`Workgroup Manager > Preferences`' from the menu
2. Check the "Show 'All Records' tab and Inspector" box and click OK

Compare and contrast the four types of Mac OS X Server accounts

1. User: relate to a specific person, the short name and UID are unique identifiers
2. Group: represents a group of users , a group of groups or a mixture of both
3. Computer: represent a single computer, the Ethernet ID is the unique identifier
4. Computer Groups: represents a group of computers, a group of computer groups or a mixture of both

Describe how to use Server Admin to create a group folder on a Mac OS X Server that will be automatically accessible from the desktop of a Mac OS X computer client computer

1. Create an automount record for the Groups folder in the 'File Sharing' window
2. Then use Workgroup Manager to associate a new Group folder associated to a group. This doesn't generate the folder
3. Use the CLI command `CreateGroupFolder` to generate the configured folder

State the hierarchy of the four account types as that hierarchy applies to managed preferences on a Mac OS X Server computer

Managed users

override

Managed computers

override

Managed computers groups

override

Managed workgroups (user groups)

Describe how to use Workgroup Manager to create a new computer group account that contains specified computers

1. Click the 'Accounts' button
2. Click the 'Computer Groups' pane button in the accounts list
3. Click the 'New Computer Group' button and fill the required fields

Describe how the four time-based options for enforcing managed account preferences effect when a manage performance is enforced

1. Never: users can change settings as they wish
2. Once: the system manages the settings only at the first login of he account, after that the most recent user settings are loaded and the use is allowed to do any change
3. Always: a user cannot change a preference
4. Often: allows to change the preferences but resets to the original preferences at the next reboot as the user log in

Explain when a managed preference setting for one type of account is overridden by a different setting for the same preference on another type of account

That happens when the preference settings can have only one value

Explain when the settings for a common managed preference from different account types are combined

That happens when a preference can have multiple values and you set different values in different account levels

Describe how to use Workgroup Manager to state what the behavior will be on the client computer when a user log in who belong to a specified user account, group account, computer account, and computer group account with a common managed preference set

1. Click the managed preferences of the groups it's member of and the computer he's using, so mind the hierarchy level to understand which preferences are overridden and which are combined
2. From the CLI use:

```
$ mcxquery <options> -user <userName> -group <groupName> -computer <computerName>
```

State the location on a client computer where managed preferences are stored

`/Library/Managed Preferences`

Explain the purpose of a Guest Computer account in Workgroup Manager

It's useful to manage the settings of a guest computer or unknown computers that do not have managed preferences

Describe how to use Workgroup Manager to configure the managed preferences for an account so that any user that connect using the given account can open only specified widgets

1. Select the account name
2. Click the 'Preferences' button
3. Click the 'Applications' pane button
4. Click the 'Widgets' pane button
5. Select 'Always' for the 'Manage' options
6. Choose the widgets to be accessible for that account

Describe preference manifests as implemented in Mac OS X Server

Preference manifests are preference data in the manifest format so that Workgroup Manager is able to read and import into the accounts to managed

Describe how to use Workgroup Manager to import a preference manifest so that an application not listed in Workgroup Manager by default, can be managed

1. Select the account you want to manage the application for
2. Click the 'Preferences' button
3. Click the 'Details' pane button
4. Click the 'add' ('+') button to select the preference manifest file

List all managed preference settings that can be applied to a user account

1. Applications
2. Classic
3. Dock
4. Finder
5. Login
6. Media Access
7. Mobility
8. Network
9. Parental Control
10. Printing
11. Software update
12. System Preferences
13. Universal access

Explain the characteristics of a mobile user account in Mac OS X Server

1. It's a user account that resides in a shared domain but it's copied to the local computer
2. User can log in to a portable computer using the network account even when the computer is not connected to a network
3. Ability to do file synchronization with the server account
4. Files can be set through Workgroup Manager to be automatically copied from the user's network home folder
5. Option to se the Account Expiry
6. Capability of External Account provides the possibility to save user's data in an external attached device (also in MS-DOS FAT32 FileSystem) so the user can connect his external storage to any network computer without the need to copy data to the computer from the server
7. Permissions and ownerships are the same on the server and on the local computer client

Describe the top preference management problems in accordance to the Mac OS X Server User Management document and the techniques used to resolve them

1. Users don't see a list of Workgroups at login:
   - User might not be in a group
   - User might be in only one group
   - `Hold down the Option key during login to show the list of Workgroups`
   - The User's computer might not have its login preferences managed
   - `In the 'Access' pane of login preferences select 'Alway show workgroup dialog during login'`
2. Users can't open files
   - Commonly used applications may not be available in the managed preferences
   - `Open an alternative application first, then open the file from the application menu`
3. Users can't add printers to a printer list
   - In managed Printing Preferences select "Allow user to modify the printer list"
   - Or provide Administrator credential when adding/removing printers
4. Login items added by a user don't open
   - Select 'Always' as manage option, so existing items from the user's login list are removed and replaced with the items you list
   - Select 'User may add and remove additional items'
   - If frequency setting is 'Once', select 'Manage with user's items' too
5. Items placed in the Dock by a user are missing
   - Select 'Merge with user's Dock'
6. User's Dock has duplicate items
   - Items are duplicated if they are managed in more than one account type associated to the user
7. Users see a question mark in the Dock
   - The item added in the Dock is not present on the computer in use
8. Users see a message about an unexpected error
   - When Classic preferences are managed user cannot access those control panels:
     - Extension Manager
     - File Sharing
     - Software Update
   - This error occur also when a user tries to open an unproved application in the Classic environment or Mac OS X
9. You can't manage network views
   - Mac OS Server 10.5+ do not support managed network views
   - use a Mac OS X 10.4 version of Workgroup Manager

State two methods to have a group folder hosted by a Mac OS X Server computer to be automatically accessible from a desktop of a Mac OS X client computer

1. List the group folder in the Dock items of the group account
2. List the group folder in the Login items of the group account

Explain two reasons an organization would want to set up and internal Software Update server

1. Maintaining control over what updates users install:
   It's important to test the updates in non production computers before deploying them to user's computers
2. Reducing the amount of network bandwidth used, as all the updates are downloaded only onece from internet to the server

Describe how to use Server Admin to configure a Mac OS X to automatically delete unused or legacy updates

Check the 'Delete outdated software updated box in the 'Settings' of 'Software Update' service

Describe how to use Workgroup Manager to configure an account on a Mac OS X server computer to use the URL of a Mac OS X Server computer providing software updates to clients

1. Choose to 'Always' manage the 'Software Update' preferences of an account
2. Fill the address of the Software Updates server in the specific field

Describe the basic features of the Software Update service in Mac OS X Server

1. You can limit the bandwidth users can use to access the updates if you have many computer clients
2. You can change the location of the update packages to an external volume to avoid the system volume to be filled up
3. You can select which updates to make available
4. You can choose to copy all or only the new updates from Apple and to activate them automatically or not
5. You can choose to automatically delete outdated software updates

Describe how synchronized folders are implemented in Mac OS X Server

1. Preference files are managed separately from Home folders
2. You can choose to sync manually, in background, at login or logout
3. You can choose which files and folders to include or exclude from the synchronization