



OS X Server Essentials 10.7

Exam Preparation Guide



Updated February 2012

Contents

About This Guide	3
Becoming an Apple Certified Technical Coordinator	3
Exam Details	4
Recommended Exam Preparation.....	4
Chapter One: Installing and Configuring OS X Server.....	6
Chapter Two: Authenticating and Authorizing Accounts	9
Chapter Three: Using Open Directory	12
Chapter Four: Managing Accounts.....	15
Chapter Five: Implementing Deployment Solutions.....	17
Chapter Six: Providing File Services.....	20
Chapter Seven: Managing Web Services	24
Chapter Eight: Using Collaborative Services	25

About This Guide

This guide provides all the information you need to prepare to earn the Apple Certified Technical Coordinator certification. From this guide you can:

- Learn about Apple Certification
- Find out how to take an exam
- Locate resources to help you prepare for an exam
- Review the range of objectives that the exam may cover
- Get a feel for the type of questions that appear on the exam

Becoming an Apple Certified Technical Coordinator

The Apple Training and Certification program is designed to keep you at the forefront of Apple technology. Certification creates a benchmark to demonstrate your proficiency in specific Apple technologies and gives you a competitive edge in today's evolving job market.

Apple offers three OS X certifications: Apple Certified Associate: Mac Integration, Apple Certified Support Professional, and Apple Certified Technical Coordinator. For more information on all OS X certifications, visit training.apple.com/certification/macosex.

Apple Certified Technical Coordinator (ACTC) certification verifies a foundation in OS X and OS X Server core functionality and an ability to configure key services and perform basic troubleshooting. ACTC certification is intended for OS X technical coordinators and entry-level system administrators who maintain small-to-medium networks of computers using OS X Server.

Students earn ACTC certification by passing the OS X Support Essentials 10.7 Exam and the OS X Server Essentials 10.7 Exam. Both exams are administered only at [Apple Authorized Training Centers](#) (AATCs). Certification exams don't require class attendance, and all AATCs offer all exams, even if they don't offer the corresponding course.

Many Apple Certification exams are available in multiple languages. For details, visit training.apple.com/certification/localized.

What are the benefits of Apple Certification?

Besides differentiating you as a skilled user and support professional for OS X Lion Server, becoming an Apple Certified Technical Coordinator allows you to leverage the power of the Apple brand. When you pass a certification exam, you receive an email with a PDF copy of your Apple certificate, along with instructions on how to order a printed or a printed and framed certificate. The email includes LinkedIn, Facebook, and Twitter icons to make it easy for you to share your certification news with your networks on these sites.

You also receive a login for the [Apple Certification Records System](#), where you can:

- Update your profile information and opt in to display your Apple Certification(s) on the [Apple Certified Professionals Registry](#)
- Review your certification progress
- Download your certification logo(s) to use on business cards, resumes, websites, and more
- Provide access to employers to verify your certifications

Exam Details

The Apple Pro Training Series book *OS X Lion Server Essentials* by Arek Dreyer and Ben Greisler prepares you to take the certification exam to earn Apple Certified Technical Coordinator certification.

The OS X Server Essentials 10.7 exam is a computer-based test offered at AATCs. To find the closest AATC, visit training.apple.com/locations.

Many AATCs schedule certification exam sessions at training.apple.com/schedule. If you don't see a session scheduled at your nearest AATC, contact the AATC and it may be able to schedule a session. **Please note that all AATCs offer all Mac OS X and pro apps exams, even if they don't offer the corresponding course.**

The OS X Server Essentials 10.7 exam details:

- Exam number: 9L0-515
- Number of test questions: approximately 80 technical, 5 demographic (unscored)
- The exam uses a random pool of multiple-choice, fill-in-the-blank, and interactive-media questions
- Passing score: 72 percent (scores are *not* rounded; you must earn a score of 72 percent or higher to pass the exam)
- Details on exam scoring are at training.apple.com/certification/faq
- Exam duration: Two hours
- The exam is based on features and functionality present in OS X Lion Server (version 10.7.3)
- Some exams are also available in other languages; for details, visit training.apple.com/certification/localized

The exam timer doesn't start until you view the first technical question. You may not access any resources or references during the exam.

If you still have questions, visit training.apple.com/certification/faq for more information.

Recommended Exam Preparation

We recommend the following exam preparation strategies:

- Gain experience with OS X Server.
- Learn from experts: [Lion 201: OS X Server Essentials 10.7](#).
- Study the Apple Pro Training Series book *OS X Lion Server Essentials* by Arek Dreyer and Ben Greisler.
- Review the optional study materials.
- Review the objectives and sample questions in this guide.

Gain experience with OS X Server

Nothing can substitute for time spent learning the technology firsthand. After you read the book and/or take the class, spend time increasing your familiarity with OS X Server on your own to ensure your success on the certification exam.

Learn from experts

Apple Authorized Training Centers (AATCs) offer classes where you can learn hands on with the technology and benefit from the expertise of Apple Certified Trainers and your peers. Visit the [Apple Training & Certification](#) website to find course offerings at nearby AATCs.

Study the Apple Pro Training Series book

Apple Pro Training Series books are the basis for the related Apple Certification exams. The book for this exam is *Apple Pro Training Series: OS X Lion Server Essentials*. You can purchase the book at [peachpit.com](#) ([click here](#) for a 30 percent discount code). [Creative Edge](#), an on-demand digital library, offers subscription access to the Apple Training and Apple Pro Training Series, as well as thousands of other reference videos and books. If you use an iPad, an electronic version is available on the iBookstore. Some books are also available in other languages. [Click here](#) for details.

Review the optional study materials

The following resources may also help you prepare for your certification exam, as well as expand your general knowledge:

- Review the Upgrading and Migrating Guide and the Lion Server: Advanced Administration Guide at <http://images.apple.com/macosx/server/resources/documentation.html>
- Launch the Help documentation from the Help menu in OS X Lion Server.
- Designed for iPad and iPhone, the [Test Yourself app](#) lets students review and assess their knowledge of the material in the OS X Server Essentials 10.7 Exam. Peachpit should make the app available in 2012.
- For information on the Apple Training Program, visit training.apple.com/.

Review the objectives and review questions

Even if you're self-taught or have taken courses that don't use the Apple Pro Training Series curriculum, you can still prepare for the certification

exam by making sure that you can complete all the tasks and answer all the review questions in the following sections.

The exam objectives describe the knowledge domains assessed by the exam. The review questions summarize what you should have learned in each chapter. Please note that although this guide divides the objectives into chapters or knowledge areas, questions are presented randomly during the exam.

The number of test questions drawn from each knowledge area is indicated for each of the following chapters.

Chapter One: Installing and Configuring OS X Server

Upon completion of Chapter One, “Installing and Configuring OS X Server” in *OS X Lion Server Essentials*, you should be able to complete the following tasks. Fourteen items from this chapter are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Verify that a Mac meets the minimum requirements to install OS X Server
- Install the OS X Server administration software on an OS X client computer so that it can remotely monitor or configure an OS X Server computer
- State the minimum system requirements for installing OS X Server
- Describe how installing OS X Server on a multiple-partition drive simplifies the task of keeping operating system files separate from server data
- Explain the purpose of the computer name assigned using Server Assistant
- Explain the purpose of the primary DNS name assigned using Server Assistant
- Explain the purpose of the local host name
- List the steps that should be done before installing the OS X Server software
- Install the OS X Server app so that computer becomes an OS X Server computer
- Use Server Admin, the network address of an OS X Server computer, and the name and password of an administrator account on the server to connect to the server so that you can monitor and configure it
- Use Server Admin and details about required minimum free space available to configure the server to send a message to one or more email addresses when a disk drive connected to the server has less than the specified percentage of available free space
- Configure Server Admin so that specified services are added to the list of those that you can monitor and configure

- Use the Server app to determine the amount of free disk space on the server
- Use the Server app to display a graph showing the amount of CPU utilization on the server over the past hour, day, and week
- Use Server Admin to display a graph indicating the amount of network traffic on the server over the past hour, day, and week
- Configure the Server Status widget so that it can be used for high-level monitoring of an OS X Server computer
- Use the Server app on an OS X client computer to observe a screen shared from an OS X Server computer
- Use a list of services that can be monitored and configured by Server Admin to briefly describe what each service provides when enabled
- Use the Server app to configure the server to send a message to one or more email addresses when an Apple-provided software update is available
- Use the Server app to update the server with updates provided by Apple's Software Update service
- State which notifications can be configured in the main Settings pane of Server Admin to trigger an email notification when a specific condition has been met
- State how to configure an administrator email address in Server app to receive alert emails
- Use the Server app to create a self-signed certificate
- Use the Server app to install a certificate granted by a trusted authority
- Explain the purpose of a certificate
- Explain the purposes of root and chain the following types of certificates: root, chain
- Display the built-in certificate(s)
- Create a certificate signing request (CSR)
- Define the term "certificate" as it applies to computer security
- Determine whether a computer trusts the Certificate Authority that issued a certificate
- Explain how trust of a certificate is granted
- Describe the function of the CA as it applies to the Public Key Infrastructure (PKI)
- List the services capable of using certificates

Chapter One review questions

After completing Chapter One, you should be able to answer the following questions.

1. What are the minimum hardware requirements for installing OS X Lion Server?

2. What tool do you use to configure Lion Server if you have an unconfigured Lion Server?
3. If you're installing Lion Server on a Mac with Lion, what's one configuration step you should take first?
4. What are three kinds of names associated with your Lion Server, and what are they used for?
5. How can you install the Server app on an administrator computer?
6. What are three ways to keep Lion Server up to date with software?
7. What three applications can you use to display graphs of performance characteristics of your Lion Server?
8. What's the difference between a root certificate authority (CA) and an intermediate CA?
9. What's the problem with just using a self-signed SSL certificate?

Answers

1. The minimum requirements are:
 - Mac with an Intel Core 2 Duo, Core i3, Core i5, Core i7, or Xeon processor
 - 2 GB of RAM (more for high-demand servers running multiple services)
 - 10 GB of available disk space
2. You use the Server app to configure an unconfigured Lion Server.
3. You should configure your Mac with Lion to use a manually assigned IPv4 address.
4. You can use the Server app to configure these three names:
 - Computer Name: What appears in the Finder sidebar if your server offers file-sharing services.
 - Bonjour name: Appended with .local and is used for services discovery.
 - DNS host name: Computers and devices can access services offered by your Lion Server by using its DNS host name, even if they're not on its local network, as long as the host name corresponds with an IPv4 address that is reachable and not blocked by firewalls.
5. You can use the Mac App Store to download the Server app to an administrator computer, or just copy the Server app to an administrator computer.
6. You can:
 - Log in to your Lion Server, and from the Apple menu, choose Software Update

- Use the Alerts section of the Server app to install available software updates
 - Click Server Updates in the toolbar of Server Admin, select the update(s) to install, and then click Install
7. The Server app, Server Admin, and the Server Status widget all display graphs.
 8. An intermediate CA's public key certificate is signed by another CA. A root CA's public key certificate is signed by itself. Note that there is a set of root CAs that Lion and Lion Server trust.
 9. Computers and devices that access services that use a self-signed SSL certificate will see a message that the SSL certificate is not trusted. It's a security risk to teach users to just trust any SSL certificate that causes a warning.

Chapter Two: Authenticating and Authorizing Accounts

Upon completion of Chapter Two, "Authenticating and Authorizing Accounts" in *OS X Lion Server Essentials*, you should be able to complete the following tasks. Nine items from this chapter are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Use Server app to create a user account so that the user can authenticate before accessing services provided by an OS X Server computer
- Use Server app to enable a user account to have administrative capabilities on the server
- Use Server app to create a group account
- Use Server app to assign users to a group account stored on the server
- Use Server app to assign groups to a user account
- Use Server app to assign groups to one group so that all the users can be granted the same permissions, as a group, on the server
- Use Workgroup Manager to export user, group, computer, and computer group accounts so that they can be imported into a different OS X Server computer
- Use Workgroup Manager and a text file with user account data exported from a source other than an OS X Server computer to import the accounts so that they can be used for authentication and authorization on the server
- Use Workgroup Manager and a text file with accounts exported from another OS X Server computer to import the accounts into the server so they can be used for authentication and authorization on the server

- Define the terms “authentication” and “authorization” as they apply to computers and servers
- List at least three examples of user authentication on an OS X client computer, such as logging in on a client computer, connecting to a file server, authenticating as an administrator for configuration purposes, and providing a user name and password for a secured website
- Explain the main purpose of Workgroup Manager
- List the four types of OS X Server accounts that can be created and managed by Workgroup Manager, including user, group, computer, and computer group
- Explain the purpose of the user ID for a user account
- Define the term “groups” as it applies to user accounts on a computer
- Describe three examples of authorization on an OS X client computer
- Explain the purpose of aliases in the Server app
- Use Server Admin and a list of services to configure service access control lists (service ACLs) on the server so that only specified users and groups can access the listed services
- Use Server Admin to configure the service ACLs on the server so that only specified users can access any services on the server
- Use Server Admin to configure the server to allow specified users to monitor all the services provided by the server
- Use Server Admin to configure the server to allow specified users to administer all the services provided by the server
- Use Server Admin to configure the server to allow specified users to monitor only specified services
- Use Server Admin to configure the server to allow specified users to administer only specified services
- Describe service ACLs
- Explain why a user account may be given administrative capabilities for a subset of the services provided by an OS X Server computer
- Use the Server app to enable the VPN service on the server to allow remote users to connect to the internal network
- Explain the purpose of VPN and how it differs from a firewall in providing access to an internal network
- State what protocol is used by the VPN service on an OS X server computer to provide access
- Use the Server app and an OS X Server computer configured to provide VPN service to configure the shared secret for the VPN service on the server
- Use the Server app to configure the address range that’s used to assign addresses to users connecting to the network over the VPN service

Chapter Two review questions

After completing Chapter Two, you should be able to answer the following questions.

1. Describe the difference between authentication and authorization, and give an example of each.
2. What is the difference between user and administrator accounts on Lion Server?
3. Which applications can you use to configure Lion Server local user and group settings?
4. What tool can you use to import and export user accounts?
5. Which two file formats can you use to import users with Workgroup Manager?
6. Can you export user passwords with Workgroup Manager?
7. What tool can you use to authorize a nonadministrative user to administer or monitor specific services on Lion Server?
8. What's the difference between service ACLs and limited administrator settings?
9. What's an easy way to help your users running Lion to quickly configure their computers to use your server's VPN service?

Answers

1. Authentication is the process by which the system requires you to provide information before it allows you to access a specific account. An example is entering a name and password while connecting to a Lion Server's Apple Filing Protocol service. Authorization refers to the process by which permissions are used to regulate a user's access to specific resources, such as files and shared folders, once the user has been authenticated.
2. User accounts provide basic access to a computer or server, whereas administrator accounts allow a person to administer the computer. On Lion Server, an administrator account is typically used for changing settings on the server computer itself, usually through the Server app, Server Admin, or Workgroup Manager.
3. You can use the Users & Groups preferences, the Server app, and Workgroup Manager to create and configure local users and groups.
4. You can use Workgroup Manager to import and export user accounts. Additionally, you can use the Server app to import network users after you authenticate as a directory administrator.
5. You can use Workgroup Manager to import a character-delimited text file with user information, but you need to use Workgroup Manager to define the characteristics of the

information contained in the file. You can also import a text file that has a header line at the beginning of the file that defines its contents, such as a file exported from another OS X Server computer.

6. No. You can only import user passwords; you can't export user passwords when you export users with Workgroup Manager.
7. You can use Server Admin to give a nonadministrative user the ability to use Server Admin to administer or monitor specific services.
8. Service ACLs determine which users can use a given service, whereas limited administrator settings control which nonadministrative users can monitor or change a service with Server Admin.
9. Select VPN in the Server app sidebar, click Save Configuration Profile, and distribute the resulting .mobileconfig file to your users. When a user of a computer with Lion opens the .mobileconfig file, the Profiles preferences automatically open and prompt the user to install the configuration profile.

Chapter Three: Using Open Directory

Upon completion of Chapter Three, "Using Open Directory" in *OS X Lion Server Essentials*, you should be able to complete the following tasks. Nine items from this chapter are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Configure an OS X Server computer to use directory data provided by another directory server so that users can access services on the OS X Server computer by authenticating with user accounts provided by the other directory server
- Use Server Admin to configure the server as an Open Directory master so that multiple computers on the network can access directory data provided by the OS X Server computer
- Use Workgroup Manager and an OS X Server computer configured as an Open Directory master to create user accounts on the server that can be accessed by client computers bound to the OS X Server computer
- Use an OS X client computer and the address of an OS X Server computer configured as an Open Directory master to configure the OS X client computer to connect to the OS X Server computer for authentication and directory data
- Use Server Admin to configure the OS X Server computer to act as an Open Directory replica so that the replica server shares with client computers directory data as provided by the Open Directory master server
- Use Server Admin to determine whether any replica computers are connected to an Open Directory master server

- Use Server Admin to display the Open Directory service-related log files
- Describe the function of directory services in a networked computing environment
- List three advantages networked directory services provide to users and system administrators, 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 with a single account
- 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 auto-mounts and printers, to multiple client computers
- Define the term Open Directory as it applies to an OS X client computer
- Describe the structure and components of Open Directory on an OS X client computer
- List and describe the four Open Directory service roles as configured by Server Admin: Standalone, Open Directory master, Connected to, and Open Directory replica
- Compare and contrast the four Open Directory service roles as configured by Server Admin
- Use the pop-up menu in Workgroup Manager that lists the directory domains for the server to identify which item to choose to allow viewing and editing of records provided by the server to other computers bound to the server
- State how many replicas can be connected to a single OS X Server computer and how many total replicas can be part of a single Open Directory network
- State which utilities are used to configure the Open Directory service and the primary purpose of each
- State what data is archived when the Open Directory archive function is used
- Define the term “locale” as it applies to OS X Server
- Create a locale to specify to which server clients should connect so that directory usage may be balanced between a master and replica(s)
- Use the Workgroup Manager to configure the password type for a user account stored on an OS X Server computer
- Use Workgroup Manager to disable a user account so that it can't be used for authentication purposes—without deleting it
- Use Workgroup Manager to configure the password policies of user accounts so that they become disabled on a specified date
- Use Workgroup Manager to configure the password policies of user accounts so that they're disabled after a specified number of failed attempts

- Use Workgroup Manager to configure user accounts so that the users can't change their passwords
- Use Workgroup Manager to configure user accounts so that when users change their password it conforms to an organization's policies
- Use an OS X client computer and an OS X Server computer providing Kerberized services to troubleshoot a situation where the client computer is unable to use Kerberos to authenticate and access the services provided by the server
- Describe five methods an OS X Server computer can use to provide authentication, including hash files, crypt passwords, password server, Kerberos, and LDAP
- Contrast the following methods for storing authentication information: crypt, shadow, Open Directory
- Describe how Kerberos provides both identification and authentication services
- Define the following terms as they apply to Kerberos: ticket, Kerberos Distribution Center, Ticket Granting Ticket, and Service Ticket
- List four reasons a client computer might not be able to use Kerberos authentication to access a service, including a DNS configuration issue, a mismatch in time settings between the client and server computers, Kerberos authentication disabled for a service, and a user account not being configured correctly
- Determine the appropriate password type for a user account
- State which utilities are used to set password policies for user accounts
- State which types of password policies can be applied to a user account
- State one method for displaying the status of Kerberos tickets on an OS X client computer

Chapter Three review questions

After completing Chapter Three, you should be able to answer the following questions.

1. What's the main function of directory services?
2. What standard is used for data access with Open Directory? What version and level of support is provided for this standard?
3. In terms of Open Directory, what four roles can Lion Server play?
4. What are the two methods of applying password policies, and where are they located?
5. When you create an Open Directory archive, is the sparse image created on the server that hosts the Open Directory service or on the administrator computer from which you run Server Admin?

6. What criteria determines the Open Directory locale with which a Lion Open Directory client associates?
7. What log shows successful and failed attempts to authenticate against the password service?
8. What tool can you use to confirm forward and reverse DNS records?
9. What tool can you use to check the ability to obtain a Kerberos ticket?

Answers

1. Directory services provide a central repository for information about the computers, applications, and users in an organization.
2. Open Directory uses OpenLDAP and the Lightweight Directory Access Protocol (LDAP) standard to provide a common language for directory access. Open Directory uses LDAPv3 to provide read and write access to the directory data.
3. Lion Server can be an Open Directory master, a standalone server, connected to a directory system, and an Open Directory replica.
4. Per-user policies are defined in Workgroup Manager, and global policies are defined in Server Admin or the Server app.
5. The archive is created on the server that hosts the Open Directory service.
6. If a Lion computer's IPv4 address is in the range of a subnet associated with an Open Directory locale, that computer should use any of the Open Directory servers associated with that locale. Otherwise, it will use the default locale.
7. Password Service Server Log, located at /Library/Logs/PasswordService/ApplePasswordServer.Server.log, shows successful and failed attempts to authenticate.
8. You should use Network Utility to confirm forward and reverse DNS records before configuring as an Open Directory master or replica, or binding to another directory service.
9. Ticket Viewer is in /System/Library/CoreServices, and you can use it to confirm the ability to obtain a Kerberos ticket.

Chapter Four: Managing Accounts

Upon completion of Chapter Four, "Managing Accounts" in *OS X Lion Server Essentials*, you should be able to complete the following tasks. Ten items from this chapter are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Define the following terms: configuration profile, enrollment profile
- Enable the Profile Manager service on the server
- List two methods for delivering a profile to a user
- Use the Server app to configure the Profile Manager service to sign configuration profiles
- Explain the benefit of signing a configuration profile
- Use the Server app to configure the Profile Manager service to manage devices
- Describe the process for configuring the Profile Manager service to manage devices
- Explain how to access the Profile Manager on a remote computer
- Use a client computer with a web browser and an OS X Server computer hosting the Profile Manager service to open the Profile Manager on the client computer
- Remove an installed profile
- Explain how an OS X computer will interpret two or more installed profiles that attempt to manage the same setting
- Explain how to install a profile on an iOS device such as an iPhone
- Describe how to display a list of the installed profiles

Chapter Four review questions

After completing Chapter Four, you should be able to answer the following questions.

1. What tool is used to create profiles?
2. Name at least three ways a profile can be delivered.
3. Why should a configuration profile be signed?
4. How is a profile removed from an OS X computer? From an iOS device?
5. What is a configuration profile? An enrollment profile?
6. What steps are involved with turning on the Profile Manager service?
7. What steps are involved with specifying that you want to sign your configuration profiles?
8. What three components comprise Profile Manager?

Answers

1. The Profile Manager web app is used to create profiles.
2. User portal, email, web page, manual delivery, or a push to enrolled devices via the Mobile Device Management capabilities of Profile Manager.

3. A configuration profile should be signed to validate the contents of the profile.
4. In OS X Lion, the profiles are managed in the Profiles preference pane within System Preferences. On an iOS device, navigate to Settings > General > Profiles to view and remove installed profiles.
5. A configuration profile contains settings and preferences to manage the user experience in a controlled device. An enrollment profile allows the device to be remotely controlled, performing such tasks as remote wipe and lock, and installation of other configuration profiles.
6. You can click the On/Off switch in the Server app Profile Manager pane to turn on the Profile Manager service. To enable device management (also known as Mobile Device Management), click Configure next to Device Management, select a valid SSL certificate, and specify a verified Apple ID to obtain an Apple Push Notification service certificate.
7. In the Server app Profile Manager pane, select the checkbox labeled "Sign configuration profiles," then choose a valid code signing certificate. Then, when you create profiles with the Profile Manager web app, they're automatically signed.
8. The Profile Manager includes the Profile Manager web app, the user portal, and the optional device management (Mobile Device Management) service.

Chapter Five: Implementing Deployment Solutions

Upon completion of Chapter Five, "Implementing Deployment Solutions" in *OS X Lion Server Essentials*, you should be able to complete the following tasks. Nine items from this chapter are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Use System Image Utility and an appropriate image source to create a NetBoot image that can be used by the NetBoot service so that other Mac computers can use the image as a boot volume
- Use Server Admin to set which volumes on the server will be used to store NetBoot data
- Use System Image Utility and an appropriate image source to create a NetInstall image that can be used by the NetBoot service so that other Mac computers on the network can boot from the image to install software
- Use Server Admin to configure the NetBoot service to share NetBoot images over a specified network port
- Use Server Admin to start and stop the NetBoot service
- Use Server Admin to enable an image in the NetBoot service so that client computers can boot using it

- Use a NetBoot server to configure a client computer to boot using the NetBoot service by pressing a key sequence during startup
- Use System Preferences to configure an OS X client computer to boot using an image served by a NetBoot server
- Use Server Admin to configure the NetBoot service to allow or deny specified client computers access to the NetBoot service
- Use Server Admin to configure which image will be the default image used by the NetBoot service
- Use Server Admin to set what protocol will be used to serve the NetBoot image
- Use an OS X Server computer hosting NetBoot images to display the log files for the NetBoot service so that they can be used for troubleshooting
- Explain five problems that are solved by using a NetBoot server, including having to rapidly update a large number of computers with newer system software; quickly repurposing a number of computers with 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
- Define the term NetBoot as it applies to OS X Server
- List the initial steps a client computer goes through when it’s configured to boot using a NetBoot server
- Explain how network home folders complement a NetBoot system by providing users with a location to store personal data and preferences
- Locate the System Image Utility application
- Explain the differences between the three types of System Image Utility images: NetBoot, Network Install, and NetRestore
- List the types of sources, installation application, installation media and disk volumes that can be used to create a NetBoot or NetInstall image
- Compare and contrast the benefits of using each type of image source that can be used to create a NetBoot or NetInstall image, including the ability to create clean systems
- State the minimum Mac OS version for a NetBoot or NetInstall image source
- State the minimum network requirements to support client computers booting using the NetBoot service in OS X Server
- State the location where a NetBoot image should be stored so that it can be used by the NetBoot service
- Copy a NetBoot image to the correct location so that it can be used by the NetBoot service
- State three methods that can be used to configure the client computer to boot using an image provided by a NetBoot server

- State what keys should be pressed during startup to configure a Mac to boot from a NetBoot server
- Define the term “shadow files” as it applies to the NetBoot service
- Use Server Admin to list the client computers that are booted using a NetBoot image hosted by the server
- Use Server Admin and the network address of a client computer connected to the NetBoot service to state the client computer’s connection information, including what image it used and when the client computer last booted
- Use a set of NetBoot log files for a NetBoot service that’s not serving images to clients properly to identify the issue
- State the minimum system requirements for client computers booting using the NetBoot service
- Describe the purpose of the filters in the NetBoot service
- Give two reasons an organization would want to set up an internal software update server, including maintaining control over what updates users install and reducing the amount of network bandwidth used
- Describe the basic features of the Software Update service, including how it can automatically download updates provided by Apple and share only select updates to clients
- Use Server Admin to configure the server to automatically download all software updates provided by Apple
- Use Server Admin to configure the server to download all new software updates provided by Apple
- Use Server Admin to configure the server to automatically enable any updates that have been downloaded from Apple
- Use Server Admin to configure the Software Update service to automatically delete unused or legacy updates
- Use Server Admin to configure the server to limit the amount of network bandwidth that can be used for distributing software updates
- Use Server Admin to enable updates downloaded to the Software Update service so that they’re accessible by other computers on the network
- Use Server Admin to list what Apple-provided updates are available
- Use Profile Manager to create a profile to configure an OS X computer to use an OS X Server computer as the source for any software updates for the OS X computer

Chapter Five review questions

After completing Chapter Five, you should be able to answer the following questions.

1. What are the advantages of using NetBoot?
2. What are three ways to configure the network startup disk?

3. Which network protocols are used during the NetBoot startup sequence? What components are delivered over each of these protocols?
4. What is a NetBoot shadow file?
5. What are the major differences between NetBoot, NetInstall, and NetRestore?

Answers

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

Chapter Six: Providing File Services

Upon completion of Chapter Six, “Providing File Services” in *OS X Lion Server Essentials*, you should be able to complete the following tasks. Eleven items from this chapter are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Use the Server app to modify the POSIX permissions for files and folders to restrict user access to them
- Use the Server app to create access control lists (ACLs) that control access to files and folders shared by the server
- Use the Server app to create ACLs for files and folders on the server

- Use server administrator software to isolate and resolve issues with file system ACLs on the server
- Explain why it's best to use groups instead of individual user accounts to manage permissions
- Explain how unique IDs (UIDs) and group IDs (GIDs) are used to relate permissions for files and folders to users and groups
- Explain how Guest access and permissions for Everyone for files can expose shared items to undesirable access
- Explain how POSIX permissions can limit your options when setting up folder and file permission structures that involve multiple users or groups
- Define the term "access control list" (ACL) as it applies to OS X Server
- Define "globally unique ID" (GUID) as it relates to user and group accounts
- Explain how Access Control Entries (ACEs) are interpreted to determine the permissions of a file or folder
- Explain the order of how OS X interprets access control entries and POSIX permission settings when determining the effective permissions of a file
- Explain how GUIDs associate ACLs to users and groups
- Describe how file system ACLs in OS X Server map to file system ACLs in Windows servers
- Define "inheritance" as it applies to file system ACLs
- Define "access control entry" (ACE) as it applies to ACLs
- Use the Server app to modify the permissions on a share point to grant or restrict access to user accounts
- Use the Server app to create a new folder on the server that can be configured to act as a share point
- Use the Server app to configure a folder on the server to act as a share point so that other computers on the network can access files stored within the folder
- List the file-sharing protocols that can be enabled for a share point using the File Sharing pane within the Server app
- Describe the four basic steps to set up file services, including planning, configuring accounts, configuring file service, and monitoring the service
- Explain two issues related to configuring a share point to share files over two different protocols, including volume format case-sensitivity and file system permissions
- State what tool is used to create and manage share points
- Use the Server app to configure a share point so that client computers can access the files using the Apple Filing Protocol (AFP)

- Use the Server app to configure a share point so that client computers can access the files on the share point without having to provide a user name and password
- Use the Server app to configure a share point so that client computers can access files using Server Message Block (SMB)
- Describe how a Windows client accesses a shared SMB volume that resides on an OS X Server computer
- Explain the difference between the specified permissions and inherited permissions models as they relate to assigning permissions to new files and folders on an SMB share point hosted by an OS X Server computer
- Use the address of an OS X Server computer sharing files over WebDAV to state the URL to access the files
- Compare and contrast WebDAV with other common file-sharing protocols such as AFP and SMB, discussing security issues, format of the URLs used to access, and benefits of using each
- Use the Server app and a share point on an OS X Server computer configured to provide network user data to configure the share point to be available to host home folders
- Use the Server app to configure a user account to use a network home folder hosted on a share point on the server
- Use the Server app and a folder on the server containing web files to create a website so that other computers on the network can access the web files
- Use the Server app to enable the Time Machine service on the server
- Use the Server app to configure the Time Machine service so that it uses a specified drive to store backup data
- State where the user backup data is stored when the Time Machine service is enabled

Chapter Six review questions

After completing Chapter Six, you should be able to answer the following questions.

1. Name three file-sharing protocols supported by Lion Server and their principal target clients.
2. How does Lion Server support browsing for Windows clients?
3. When does an access control entry (ACE) for a folder's access control list (ACL) get propagated to items in the folder?
4. What two actions are necessary to provide a network home folder for a network user?
5. What permissions can you choose for an ACE in the File Sharing pane of the Server app?
6. What permissions can you specify for an ACE in the Storage pane of the Server app?

7. In the Storage pane of the Server app, what four rules for inheritance can you apply to an ACE?
8. How do you remove an inherited ACE?
9. What might it mean if you see a GUID rather than a user name in an ACL?
10. What URL should you use from an iOS device to save to a WebDAV-enabled share point hosted by the Lion Server at server17.pretendco.com, if the web service on the Lion Server uses an SSL certificate?
11. Do both the File Sharing and the Time Machine services need to be turned on to offer Time Machine services to your users?

Answers

1. AFP for Mac clients, SMB for Windows clients, and WebDAV for iOS devices are three file-sharing protocols supported by Lion Server.
2. Lion Server uses NetBIOS to advertise its presence to Windows clients; Windows users see Lion Server in their Network Neighborhood or Network Places.
3. An ACE of a folder's ACL is propagated to a new item that's created in that folder, or copied into that folder from another volume, if the inheritance options for the ACE apply. Also, an administrator can select a folder in the Storage pane of the Server app, choose Propagate Permissions from the Action pop-up menu, select the Access Control List checkbox, and click OK. Finally, if you use the File Sharing pane to modify an ACL that has been inherited, the changes will be propagated.
4. You need to first edit a share point and select the checkbox "Make available for home directories." Then you can edit a user, and select that share point in the Home Folder pop-up menu.
5. In the File Sharing pane of the Server app, when you edit an ACE, you can choose Read & Write, Read, or Write.
6. In the Storage pane of the Server app, when you edit an ACE, you can select checkboxes for 13 kinds of permissions. The categories include Administration, Read, and Write.
7. There are four inheritance rules: folder, child folders, child files, and all descendants.
8. In the Storage pane of the Server app, navigate to the item that has an ACL, click the Action pop-up menu, choose Edit Permissions, click the Action pop-up menu, and choose Remove Inherited Entries.
9. If you see a GUID instead of a user name, it could mean that you removed a user or a group from your Lion Server, and the ACE is displaying that user or group's GUID because it can't map the GUID to a user or a group.

10. In the iOS application that supports WebDAV, you would use the URL `https://server17.pretendco.com/webdav`. Depending on the application, you'll see a list of share points that support WebDAV.
11. Yes, both File Sharing and Time Machine need to be on to offer the Time Machine service to your users.

Chapter Seven: Managing Web Services

Upon completion of Chapter Seven, "Managing Web Services" in *OS X Lion Server Essentials*, you should be able to complete the following tasks. Four items from this chapter are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Use the Server app to configure a share point to share files using WebDAV so that iOS devices can access files stored on the share point
- Use the Server app and a website hosted on a OS X Server computer to disable the site so other computers can't access it
- Use the Server app to configure the location of the data files for a website hosted on an OS X Server computer
- Configure the permissions of files so that they can be served by the web service
- Use the Server app to start and stop the web service
- Use the Server app to configure two or more websites on the server so that each is uniquely accessible
- Use Server Admin and a website hosted by an OS X Server computer to add an alias to the website so that the server responds to the new name
- State the standard web server on which the web service in OS X Server is based
- List the three methods for distinguishing between websites hosted by an OS X Server computer, including domain name, IP address, and port number, so that multiple sites can be hosted on a single server
- List the types of logs generated by the web service
- Use the Server app and an OS X Server computer hosting a website to configure the website so that it requires a user to authenticate before accessing the website

Chapter Seven review questions

After completing Chapter Seven, you should be able to answer the following questions.

1. On what software is Lion Server's web service based?
2. Which permissions are necessary on a web folder to ensure that visitors to the site can access the pages?

3. What are access controls?
4. Where is the default location for the Apache log files?
5. What is the advantage of using SSL on a website?

Answers

1. Lion Server's web service is based on Apache, the open source web server software.
2. The everyone or www group must have read access to the web files.
3. Access controls are paths to folders that can be restricted based on group.
4. The default location for Apache log files is `/var/log/apache2/access_log` and `/var/log/apache2/error_log`.
5. SSL helps protect the traffic traveling to and from the website by encrypting the data.

Chapter Eight: Using Collaborative Services

Upon completion of Chapter Eight, "Using Collaborative Services" in *OS X Lion Server Essentials*, you should be able to complete the following tasks. Fourteen items from this chapter are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Use the Server app to enable the wiki service on the server
- Use the Server app and one or more groups of users on the server to add the groups to the list of those that can create a wiki
- Use the Server app to configure the server so that anyone can create a wiki
- Create a new wiki on the server
- Use a list of user accounts to modify the wiki permissions for the given users
- Define the term "wiki" as it applies to OS X Server
- State three benefits of setting up a wiki server
- Define the term "blog" as it applies to OS X Server
- Delete a wiki
- Configure a wiki to provide a blog
- Use the Server app to enable the iCal service so that two or more OS X client computers can access and share calendar data
- Configure iCal on an OS X client computer so that it displays shared scheduling data provided by the iCal service
- Create new resources on the iCal server that can be scheduled using iCal on an OS X client computer

- Use the Server app to troubleshoot issues with the iCal Server
- List three reasons why, according to the OS X Server documentation, you would want to provide shared calendar services using the iCal service on an OS X computer
- State which protocols are used by the iCal service in OS X Server
- Use the Server app to modify the list of host domains that the chat service in OS X Server will connect to
- Use the Server app to start and stop the iChat service on an OS X Server computer
- Add a service account to iChat on an OS X client computer so that it can be used to chat with other iChat users via the iChat service on an OS X Server computer
- Use the Server app to configure the iChat service so that all chat messages are logged to a file on the server
- Use the Server app to display chat messages that have been stored on the server
- Use the Server app to enable the server-to-server federation feature for the iChat service
- Use the Server app to configure the iChat service to allow federation with any other XMPP chat server
- Use the Server app to configure the iChat service to allow federation with just a specific XMPP server
- Use the Server app to display the iChat service log
- Use the Server app to troubleshoot issues with the iChat Server
- Use the Server app to enable or disable access to the iChat service for a given account
- State which protocol is used by the chat service in OS X Server, both the familiar name, Jabber, and the official name, Extensible Messaging and Presence Protocol (XMPP)
- Explain the benefits of setting up a chat server, including automatically generating chat transcripts and increasing security
- List the methods that can be used by the iChat service in OS X Server to authenticate iChat clients
- State the iChat server screen name for a user account
- Explain the purpose of the federation feature for the iChat service in OS X Server
- Use the Server app to identify how many users are connected to the iChat service
- Use the system log file to identify the users that are connected to the iChat service
- Use the Server app to configure the Address Book service so that users can store contact information on the server

- Use the Server app and an OS X Server computer hosting the Address Book service to configure the client computer to access contact information stored on the server
- Explain how contact data is shared between OS X client computers and the Address Book service
- Explain how to configure an OS X client computer to access shared contact information provided by the Address Book services
- Use the Server app to configure the Address Book service to provide contact information provided by a directory server
- Explain three reasons for hosting a mail server, including limited network bandwidth, increased security, and enhanced control
- Define the terms POP, IMAP, and SMTP as they apply to email service
- Explain how an email message travels from a source client computer through multiple mail servers and is received by a destination client computer
- Explain how a mail server identifies the network address of the destination mail server when handling outgoing email
- Use the Server app to configure a user account to be able to send email via the server
- Use the Server app to stop and start the Mail service
- Use the Server app to configure the domain name for the Mail service
- Use the Server app to configure the Mail service to relay all outgoing email through a specified mail server
- Use the Server app to configure the Mail service so that users can access their mail accounts through a web browser
- Use the Server app to configure the Mail service so that users can't store more than a specified amount of mail on the server
- Use the Server app to configure the Mail service to scan mail messages for viruses
- State what the Mail service uses to scan email messages for viruses
- Explain what service a blacklist server provides
- Explain what service the Mail service uses to analyze email messages to determine the likelihood of the message being junk mail
- Use the Server app to configure the Mail service to use a blacklist server to filter junk mail
- Use the Server app to configure the Mail service to filter for junk mail
- Use the Server app to configure how aggressively the Mail service filters for junk mail

Chapter Eight review questions

After completing Chapter Eight, you should be able to answer the following questions.

1. What protocol is used for the iChat service?

2. How would you limit access to iChat service on Lion Server?
3. What tools can an administrator use to specify which users can create wikis? How does a network user specify which users and groups can edit a wiki?
4. How would you enter the iChat name for the user Jet Dogg (short name: jet) on server17.pretendco.com?
5. What application do you use to create resources and locations for use in iCal events?
6. What open source protocol does the Address Book service use?
7. What is an open relay?
8. What is an MX record?
9. What is SMTP?
10. What are the main differences between POP and IMAP?
11. What method can be used to limit the amount of disk space used on a mail server?

Answers

1. The iChat service uses the Extensible Messaging and Presence Protocol (XMPP).
2. You can limit access through Service Access Control Lists, available per user in the Server app.
3. Administrators can use the Wiki Creators list in the Wiki service settings in the Server app. When creating a wiki with a web browser, a user can specify permissions for users and groups to access and edit the wiki.
4. The iChat name format for Jet Dogg on server17.pretendco.com is jet@server17.pretendco.com.
5. The Server app is used to create resources and locations for use in iCal events.
6. The Address Book service uses CardDAV.
7. An open relay is a mail server that allows anyone on the Internet to anonymously send email messages through it. It's the primary tool used by spammers on the Internet.
8. An MX record is a DNS record that indicates the priority and host name of a domain's email server.
9. Simple Mail Transfer Protocol defines how messages travel from one computer to another on the Internet.
10. IMAP keeps a copy of the email message and its state on the server, maintains a persistent connection between the client and server, allows folder access, and supports higher security authentication methods. POP typically stores the message

only until it's downloaded by the client and requires fewer server resources than IMAP.

- 11.** The method to control disk consumption by users is user quotas.