OS X Server Essentials 10.9
Exam Preparation Guide

January 2014
Contents

About This Guide .................................................................3
Becoming an Apple Certified Technical Coordinator ...............3
Exam Details ........................................................................4
Recommended Exam Preparation ............................................5
Part One: Configuring and Monitoring OS X Server .................6
Part Two: Configuring Accounts .............................................13
Part Three: Managing Devices with Configuration Profiles .........18
Part Four: Providing File Services ..........................................20
Part Five: Implementing Deployment Solutions ......................24
Part Six: Providing Network Services ....................................29
Part Seven: Using Collaborative Services ..............................33
About This Guide

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

- Learn about Apple Certification
- Find out how to take the exam
- Locate resources to help you prepare for the 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 (ACSP)
- Apple Certified Technical Coordinator (ACTC)

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 10.9 Exam and OS X Server Essentials 10.9 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.

For more information on all OS X certifications, visit training.apple.com/certification/osxmac.

What are the benefits of Apple Certification?

Besides differentiating you as a skilled user and support professional for OS X Server, ACTC certification allows you to leverage the power of the Apple brand. When you achieve a certification, you receive an email detailing how you’ll receive your Apple certificate, along with instructions on how to order a framed version. 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 on the Apple Certified Professionals Registry.
- Review your certification progress
- Download your certification logo 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 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 10.9 Exam is a computer-based test offered at Apple Authorized Training Centers (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 to find out if a session can be scheduled. **Note: All AATCs offer all OS X and pro apps exams, even if they don’t offer the corresponding course.**

The OS X Server Essentials 10.9 Exam details are as follows:

- Exam number: 9L0-521
- Approximately 80 technical questions
- Five unscored demographic questions
- The exam uses a random pool of multiple-choice, true/false, and interactive-media questions
- Passing score: 75 percent (scores are not rounded; you must earn a score of 75 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 Server (version 3.1)
- 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 have additional questions about exams, visit training.apple.com/certification/faq.
Recommended Exam Preparation

The following exam preparation strategies are recommended:

- Gain experience with OS X Server.
- Learn from experts: Mavericks 201: OS X Server Essentials 10.9.
- Study the Apple Pro Training Series book, OS X Server Essentials by Arek Dreyer and Ben Greisler.
- Review the objectives and questions in this guide.

Gain experience with OS X Server

Nothing can substitute for time spent learning the technology. 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 and 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 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, you can get an electronic version on the iBookstore. Some books are also available in other languages. Click here for details.

Review the objectives and 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 lesson. Although this guide divides the objectives into lessons 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 lessons.
Part One: Configuring and Monitoring OS X Server

After completing Part One, “Configuring and Monitoring OS X Server” in OS X Server Essentials, you should be able to do the following tasks. Thirteen items from Part One are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- State the minimum system requirements for installing OS X Server.
- Explain the purpose of the primary DNS name assigned using Server Assistant on an OS X Server computer.
- Explain the purpose of the local host name on an OS X Server computer.
- Verify that the computer meets the minimum requirements to install 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 on an OS X Server computer.
- Install the OS X Server application so that the computer can provide OS X Server services.
- Explain the purpose and function of DNS.
- Define the following terms as they apply to the DNS service: DNS server, records, zone files, primary zone, secondary zone, zone transfer, forward zone.
- State two reasons why you’d need to use System Preferences instead of Server app to enable remote management or screen sharing for a computer running OS X Server.
- Configure OS X Server so that it can be managed by the Server app running on remote computers.
- Configure the computer so that it can be remotely managed from another computer through screen sharing or Remote Desktop.
- Define the term “certificate” as it applies to computer security.
- Determine whether the computer trusts the certificate authority that issued the certificate.
- Explain the purpose of a certificate.
- Explain the purposes of the following certificate types: Root, Chain.
- Explain how trust of a certificate is granted.
- Describe the function of the Certificate Authority (CA) as it applies to the Public Key Infrastructure (PKI).
- List the services capable of using certificates in OS X Server.
- Create a self-signed certificate.
- Install a certificate granted by a trusted authority.
- Display the built-in certificate(s).
- Create a certificate signing request (CSR).
- List at least four system conditions that can trigger an alert notification by OS X Server.
- Briefly describe what each service provides when enabled.
- Explain what condition is triggered by each alert type.
- Observe a screen shared from an OS X Server computer.
- Update the server computer with available software updates provided by Apple's Software Update service.
- Connect to the server so that you can monitor and configure it.
- Configure the OS X Server so that any system alerts are sent to the given email addresses.
- Configure the OS X Server so that the recipients are notified of any system alerts via push notifications.
- Determine the amount of free disk space on the server.
- Display a graph showing the amount of CPU utilization that has occurred on the server over the past hour, day, and week.
- Display a graph indicating the amount of network traffic that has occurred on the server over the past hour, day, and week.
- Describe what files are backed up with the default configuration of Time Machine on a computer with OS X Server.

**Lesson One review questions**
Lesson One doesn't include any review questions.

**Lesson Two review questions**
After completing Lesson Two, you should be able to answer the following questions.

1. What are the minimum RAM and disk requirements for installing OS X Server?
2. What tool do you use to perform an installation and initial configuration of OS X Server?
3. If you're installing OS X Server on a Mac, what is one configuration step you should take before installing?
4. What are two kinds of names associated with your server, and what are they used for?
5. How can you install the Server app on an administrator computer?
6. Give two examples of services that appear with your server's computer name.
7. What kind of name is new-test-server.local?
8. What kind of name is server17.pretendco.com?
Answers

1. The minimum RAM and disk requirements for OS X Server are:
   - 2GB of RAM (more for high-demand servers running multiple services)
   - 10GB of available disk space

2. You use the Server app to perform an installation and initial configuration of OS X Server.

3. Configure your Mac with OS X to use a manually assigned IPv4 address.

4. You can use the Server app to configure these two names:
   - Computer name—This is what appears in the Finder sidebar for other Macs if your server offers file sharing services.
   - Host name—Computers and devices can access services offered by your server by using your server’s DNS host name, even if they’re not on its local network, as long as the host name corresponds with an IPv4 address that’s reachable and not blocked by firewalls.

5. Use the Mac App Store to download OS X Server. If you purchased a computer with OS X Server preinstalled, copy the Server app from that server to your administrator computer.

6. Your server’s computer name appears in the Finder sidebar window if the File Sharing or Screen Sharing services are enabled. It may also appear in AirDrop, Apple Remote Desktop, and in Xcode preferences when adding a new server for the Xcode service.

7. new-test-server.local is an example of a local host name.

8. server17.pretendco.com is an example of a host name.

Lesson Three review questions

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

1. What is the purpose of DNS?

2. If no DNS server is defined when configuring OS X Server, how will the server provide DNS for itself?

3. If you’re using an external DNS server to provide DNS for your server, what should you do prior to configuring the server?

4. When is it OK to leave the automatically configured DNS server running with no modification?

5. When might you want to use a manually configured DNS service on your OS X Server?
Answers

1. To convert host names into IP addresses and IP addresses to host names.

2. A basic DNS server is configured automatically and turned on.

3. You should check that the DNS server has the proper forward and reverse DNS information configured for your server's host name and IPv4 address.

4. When it's a very simple network with one server, and all the computers and devices are on the same network.

5. When you want to have records for multiple computers and devices.

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

1. Using an administrator computer with the Server app installed, how do you use the Server app to administer a remote server?

2. What option do you need to select in order to allow another Mac to administer your server, and where is its checkbox?

3. What tools does the Tools menu give you quick access to open?

4. Do you have to install extra software to take control of your server's keyboard and mouse?

5. If you use the Server app to choose a different service data volume to a volume mounted at /Volumes/Data, what folder will contain the service data?

6. Do you need to stop all services before using the Server app to change your service data volume?

7. Can you remotely install OS X Server on a brand new Mac computer that comes with OS X Server without first configuring OS X on that computer?

8. How do you display the list of advanced services in the Server app sidebar?

Answers

1. Open the Server app, choose Manage > Connect to Server, select your remote server from the list (or select Other, and then provide its host name or address), and provide credentials for a local administrator.

2. Select your server in the Server app sidebar (in the Server section), click the Settings tab, and then select the option "Allow remote administration using Server."
3. The Tools menu gives you access to these applications:
   • Directory Utility
   • Screen Sharing
   • System Image Utility
   • Xsan Admin

4. No, on your server computer, you open the Server app and select your server in the Server app sidebar (in the Server section). Click the Settings tab, select the checkbox “Enable screen sharing and remote management,” and then on your administrator computer use Screen Sharing to take control of your server computer’s keyboard.

5. In this case, your service data will be stored in /Volumes/Data/Library/Server.

6. No, the Server app automatically stops the appropriate services before moving their data to the new service data volume.

7. No, you need to configure OS X before installing and configuring OS X Server.

8. Hover the pointer over the word Advanced in the Server app sidebar, then click Show.

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

1. What is the difference between a root CA and an intermediate CA?

2. What is the problem with just using a self-signed SSL certificate?

3. What tool do you use to create a new self-signed SSL certificate and a CSR?

4. What tool do you use to create a secure archive of your certificate and private key?

5. Can different services use different certificates, or do all the services on your server need to use the same certificate?

Answers

1. 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 and intermediate CAs that OS X trusts.

2. Computers and devices accessing services that use a self-signed SSL certificate will see a message that the SSL certificate is not trusted. It is a security risk to teach users to just trust any SSL certificate that causes a warning.
3. Use the Server app to create a new self-signed SSL certificate and a CSR.

4. Use Keychain Access on the server to create a secure archive of your certificate and private key. Be sure to choose “Personal Information Exchange (.p12)” in the File Format menu of the Save dialog.

5. Each service can use a different certificate, or you can use the same certificate for all services.

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

1. What is the purpose of alerts?
2. What are the two ways alerts can be delivered?
3. If you wish to use push alerts, what is the first step you need to take?
4. If an alert details offers to update services, what is the correct action?
5. Which volumes are shown in the Storage tab in the Server app?

Answers
1. Alerts provide a system of warning of various conditions.
2. Email, and alerts pushed to the Server app.
3. Configure the Apple Push Notification service for the server you’re using.
4. Understand the alert and rectify the situation before making any configuration changes, as they may be unneeded.
5. All that are visible and mounted on the server.

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

1. Why use Time Machine to back up OS X Server?
2. What files are not backed up by Time Machine that might be important in a server to a system administrator?
3. What kind of backup targets can be used for Time Machine?
4. If you don’t want to drop the oldest backups, what should you do?
5. What are three ways of recovering data from a Time Machine backup?
Answers

1. Time Machine provides a simple backup system that’s capable of backing up OS X Server and restoring its services.

2. /Library/Logs/.

3. Locally connected volumes and AFP file shares.

4. Don’t let the backup target volumes fill up, or the oldest backups will be dropped.

5. From the Time Machine graphical interface, directly from the backup volume, and via Restore from Time Machine Backup in the Recovery volume.
Part Two: Configuring Accounts

After completing Part Two, “Configuring Accounts” in *OS X Server Essentials*, you should be able to do the following tasks. Nine items from Part Two are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Describe five methods an OS X Server can use to provide authentication including hash files, crypt passwords, password server, Kerberos, and LDAP.
- Define the following term locales as it applies to OS X Server.
- Define the following terms as they apply to Kerberos: ticket, Kerberos Distribution Center, Ticket Granting Ticket, Service Ticket.
- List four possible 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 configured correctly.
- 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 types of password policies can be applied to a user account in OS X Server.
- State one method for displaying that status of Kerberos tickets on an OS X client computer.
- State which utilities are used to configure the Open Directory service in OS X Server and the primary purpose of each.
- Contrast the following methods for storing authentication information: crypt, shadow, Open Directory.
- State what data is archived when the Open Directory Archive function is used with OS X Server.
- 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.
- List and describe the four Open Directory service roles on an OS X Server computer: Open Directory master, standalone server, connected to a directory system, and Open Directory replica.
- Describe how Kerberos provides both identification and authentication services.
- Create user accounts on the server so that they can be accessed by client computers that are bound to the OS X Server computer.
- Troubleshoot a situation where the client computer is unable to use Kerberos to authenticate and access the services provided by the server.
- Disable a user account so that it can no longer be used for authentication purposes, without deleting it.
• Configure the password policies of the user accounts so that they become disabled on the specified date.

• Configure the password policies of the user accounts so that they become disabled after the specified number of failed attempts.

• Configure the user accounts so that when users change their password, the password conforms to the organization’s password policies.

• Define the terms “authentication” and “authorization” as they apply to computers and servers.

• State what characters can be used to create a short name for a user account on an OS X Server computer.

• Explain the additional functionality a user account gains when the “administer this server” option is selected for the account in Server app.

• 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 admin user for configuration purposes, and providing a username and password for a secured website.

• Explain the purpose of the user ID for a user account on an OS X Server computer.

• Describe three examples of authorization on an OS X client computer.

• Define the term “groups” as it applies to user accounts on a computer.

• Assign users to a group account stored on the server.

• Assign groups to a user account.

• Assign groups to a group, so that all of the users of the multiple groups can be granted the same permissions on the server.

• Import accounts into the server so that the accounts can be used for authentication and authorization purposes on the server.

• Create a user account so that the user can authenticate before accessing services provided by an OS X Server computer.

• Enable a user account on an OS X Server computer to have administrative capabilities on the server.

• Create a group account on an OS X Server computer.

• Describe service access control lists (ACLs).

• Configure the service ACLs on the server so that only the listed users and groups can access the listed services.

• Configure the service ACLs on the server so that only the listed users can access any services on the server.

Lesson Eight review questions
After completing Lesson Eight, 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 OS X Server?

3. Which applications can you use to configure OS X Server local user and group settings?

4. What tool can you use to import and export user accounts?

5. Which two formats of files can you use to import users with the Server app?

6. If you decide to manually manage access to services, what are some services included in the list?

7. When you select the checkbox to grant authorization for a user to access File Sharing services, what file sharing protocols does this enable for the user?

8. When you click the Manage Service Access button, does this prevent users that you create in the future from being able to access your OS X Server services?

Answers

1. Authentication is the process by which the system requires you to provide information before you can access a specific account. An example is entering a name and password while connecting to the 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 successfully authenticated.

2. User accounts provide basic access to a computer or server, whereas administrator accounts allow a person to administer the computer. On OS X Server, an administrator account is typically used for changing settings on the server computer itself, usually through the Server app.

3. You can use the Users & Groups preferences and the Server app to create and configure local users and groups.

4. You can use the Server app to import user accounts. Additionally, as you’ll see in Lesson 10, you can use the Server app to import network users after you authenticate as a directory administrator.

5. You can use the Server app to import a character-delimited text file with user information, but you need a header line 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 the contents of the file.

6. Services include Calendar, Contacts, File Sharing, FTP, Mail, Messages, Profile Manager, Time Machine, and VPN.

7. Authorization to use File Sharing includes the AFP and SMB protocols.
8. No, even after you choose to manage service access manually, new users that you create with the Server app automatically get authorization to access services. Of course, you can edit a user and remove authorization for that user to access a service.

Lesson Nine review questions
After completing Lesson Nine, you should be able to answer the following questions.

1. What is 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 OS X Server play?
4. What criterion determines the Open Directory locale with which an OS X Open Directory client associates?
5. What log shows successful and failed attempts to authenticate against the password service?

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. OS X Server Open Directory roles include Open Directory master, standalone server, connected to a directory system, and Open Directory replica.
4. If a Mac has an IPv4 address that’s in the range of a subnet associated with an Open Directory locale, that Mac should use any of the Open Directory servers associated with that locale. Otherwise, it will use the default locale.
5. Password Service Server Log, located at /Library/Logs/PasswordService/ApplePasswordServer.Server.log, shows successful and failed attempts to authenticate.

Lesson Ten review questions
After completing Lesson Ten, you should be able to answer the following questions.

1. What tool can you use to check the ability to obtain a Kerberos ticket?
2. How do you import local network users from a text file with a properly formatted header line?

3. What are some reasons that a client computer might not be able to use Kerberos authentication to access a service?

4. In addition to authentication, what else can Kerberos provide?

5. How can you disable a local network user account so that it cannot be used to access services or log in on a bound Mac?

6. What are some examples of global password policies that you can apply to users that apply the next time they change their password?

7. What are some examples of global password policies that you can configure to disable login after certain events occur?

8. How does a user obtain a Kerberos service ticket?

Answers

1. Ticket Viewer is in /System/Library/CoreServices, and you can use it to confirm the ability to obtain a Kerberos ticket.

2. Choose Manage > Import Accounts from the File menu, select the text file, choose Local Network Accounts in the pop-up menu, provide directory administrator credentials, and click Import.

3. The client computer might not be bound to a directory service that provides Kerberos; the system time between the client computer and the server computer might be off by more than 5 minutes; there could be a DNS configuration issue; or the service might not be configured to use Kerberos.

4. Kerberos provides identification and authentication.

5. In the User pane of the Server app, double-click the user to edit the user, and deselect the checkbox “Allow user to log in.”

6. Some examples include that passwords must differ from account name; contain at least one letter; contain both uppercase and lowercase letters; contain at least one numeric character; contain a character that isn’t a letter or number; contain at least a given number of characters; or differ from the last given number of passwords used.

7. Some examples include that the login will be disabled on a specific date; after using it for a given number of times; after inactive for a given number of days; or after a user makes a given number of failed attempts.

8. Once a user has a ticket-granting ticket, OS X automatically attempts to obtain a service ticket when a user attempts to connect to a Kerberized service.
Part Three: Managing Devices with Configuration Profiles

After completing Part Three, “Managing Devices with Configuration Profiles” in OS X Server Essentials, you should be able to do the following tasks. Nine items from Part Three are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Define the following terms: configuration profile, enrollment profile, payload.
- Explain the benefit of signing a configuration profile.
- Describe the process for configuring the Profile Manager service on an OS X Server to manage devices.
- List two methods for delivering a profile to a user.
- Explain how to access the Profile Manager on a remote computer.
- Describe how to display a list of the profiles installed on an OS X computer.
- Explain how an OS X computer interprets two or more installed profiles that attempt to manage the same setting.
- Enable the Profile Manager service on the server.
- Configure the Profile Manager service to sign configuration profiles.
- Configure the Profile Manager service to manage devices.
- Open the Profile Manager on the remote computer.
- Remove a profile from an OS X computer.
- Explain how to install a profile on an iOS device such as an iPhone.

Lesson Eleven review questions

After completing Lesson Eleven, you should be able to answer the following questions.

1. What tool is used to create profiles?
2. Why should a configuration profile be signed?
3. What is a configuration profile? An enrollment profile?
4. What steps are involved with turning on the Profile Manager service?
5. What steps are involved with specifying that you want to sign your configuration profiles?
6. What three components comprise Profile Manager?

Answers

1. The Profile Manager web app is used to create profiles.
2. A configuration profile should be signed to validate the contents of the profile.
3. A configuration profile contains settings and preferences to manage the user experience in a controlled device. An enrollment profile allows the device that it's installed on to be remotely controlled, performing such tasks as remote wipe and lock, and installation of other configuration profiles.

4. You can just click the On/Off switch in the Server app Profile Manager pane to turn on the Profile Manager service, but to enable device management (also known as Mobile Device Management), click the Configure button next to Device Management, select a valid SSL certificate, and specify a verified Apple ID to obtain an Apple Push Notification service certificate.

5. In the Server app Profile Manager pane, select the “Sign configuration profiles” option, and choose a valid code signing certificate. Then when you create profiles with the Profile Manager web app, they’re automatically signed.

6. The Profile Manager includes the Profile Manager web app, the user portal, and the optional device management (Mobile Device Management) service.

Lesson Twelve review questions
After completing Lesson Twelve, you should be able to answer the following questions.

1. At what levels can clients be managed?
2. Name at least three ways a profile can be delivered.
3. What service does push notification rely on?
4. How is a profile removed from an OS X computer? From an iOS device?
5. How can you view the contents of a profile?

Answers

1. Users, user groups, devices, and device groups.
2. User Portal, email, web page, or manual delivery. The mobile device management capabilities of Profile Manager can also push profiles to enrolled devices.
3. Apple Push Notification service (APNs).
4. In OS X 10.7 Lion and later, the profiles are managed in the Profiles preferences. On an iOS device, navigate to Settings/General/Profiles to view and remove installed profiles.
5. Any text editor. The text contained in the profile is either straight XML or XML with some binary data if signed.
Part Four: Providing File Services

After completing Part Four, “Providing File Services” in *OS X Server Essentials*, you should be able to do the following tasks. Twelve items from Part Four are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- List the file sharing protocols that can be enabled for a share point on an OS X server using the File Sharing service pane within the Server application.
- 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 locking.
- Given the address of an OS X Server computer sharing files via WebDAV, 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.
- State what tool is used to create and manage share points in an OS X Server.
- Describe how a Windows client accesses a shared Server Message Block (SMB) volume that resides on an OS X Server computer.
- Configure a share point to allow client computers to access the files using the Apple Filing Protocol (AFP).
- Configure a share point to allow client computers to access files using the SMB protocol.
- Configure a share point to share files using WebDAV so that iOS devices can access files stored on the share point.
- Create a new folder on a server so that the folder can be configured to act as a share point.
- Configure a folder on a server to act as a share point so that other computers on the network can access files stored within the folder.
- Configure the share point so that client computers can access the files on the share point without having to provide a user name and password.
- 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.
- Explain why it’s a best practice to use groups instead of individual user accounts to manage permissions in OS X Server.
• Explain how unique IDs (UIDs) and group IDs (GIDs) are used to relate permissions for files and folders to users and groups on an OS X Server computer.

• Explain how Guest access and the file permissions for Everyone 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 inheritance, access control entry (ACE), access control lists (ACLs), and globally unique ID (GUID) as they apply to OS X Server.

• Explain how access control entries are interpreted to determine the permissions of a file or folder.

• Create ACLs that control access to files and folders shared by the server.

• Modify the permissions on the share point to grant or restrict access to the share point for specified user accounts.

• Modify the POSIX permissions for files and folders to restrict user access to them.

Lesson Thirteen review questions
After completing Lesson Thirteen, you should be able to answer the following questions.

1. Name three file sharing protocols supported by the OS X Server File Sharing pane and their principal target clients.

2. What is one concern with using the FTP service?

3. How does OS X Server support browsing for Windows clients?

4. How do you enable guest access to a share point?

5. Where can you quickly view how many AFP and SMB connections there currently are to your server?

6. How can you configure a share point to be accessible to an app on an iOS device?

7. Where would you find information about AFP service errors?

8. How can you create a new share point?

9. What file sharing protocols are enabled by default for a share point you just created?

10. Do you need to start the Websites service in order to provide WebDAV service?

Answers

1. AFP for Macs with OS X earlier than Mavericks, SMB for OS X Mavericks and Windows clients, and WebDAV for iOS devices are three file sharing protocols supported by OS X Server.
2. Normally the network traffic is not encrypted for authenticating to the FTP service with user name and password.

3. OS X Server uses NetBIOS to advertise its presence to Windows clients; Windows users see the server in their Network Neighborhood or Network Places.

4. Edit a share point and select the “Allow guest users to access this share” checkbox.

5. The Connected Users tab displays the number of AFP and SMB connections; you may need to choose View > Refresh (or press Command-R) to refresh the number.

6. Edit a share point and select the “Share over WebDAV” checkbox.

7. The Logs pane of the Console app displays the AFP Error log, which displays the contents of the log file: /Library/Logs/AppleFileService/AppleFileServiceError.Log.

8. In the File Sharing list of share points, click Add (+) and either select an existing folder or create a new folder and select the new folder.

9. AFP and SMB are enabled by default for a new share point.

10. No, the Websites service doesn’t need to be running in order for you to offer File Sharing services via WebDAV (of course, the File Sharing service must be running).

Lesson Fourteen review questions

After completing Lesson Fourteen, you should be able to answer the following questions.

1. When does an ACE for a folder’s ACL get propagated to items in the folder?

2. What permissions can you choose for an ACE in the File Sharing pane of the Server app?

3. What permissions can you specify for an ACE in the permissions dialog of the Storage pane of the Server app?

4. In the permissions dialog of the Storage pane in the Server app, what four rules for inheritance can you apply to an ACE?

5. How do you remove an inherited ACE?

6. What might it mean if you see a GUID rather than a user name in an ACL?

Answers

1. 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
1. Server app, choose Propagate Permissions from the Action (gear icon) pop-up menu, select the Access Control List checkbox, and click OK. Finally, if you use the File Sharing pane to modify a share point’s POSIX permissions or ACL, the ACL will be automatically propagated.

2. When you edit an ACE in the File Sharing pane of the Server app, you can choose Read & Write, Read, or Write.

3. When you edit an ACE in the Storage pane of the Server app, you can select checkboxes for 13 kinds of permissions. The categories include Administration, Read, and Write.

4. Apply to this folder; Apply to child folders; Apply to child files; and Apply to all descendants.

5. In the Storage pane of the Server app, navigate to the item that has an ACL, click the Action (gear icon) pop-up menu, choose Edit Permissions, click the Action (gear icon) pop-up menu, and choose Remove Inherited Entries.

6. If you see a GUID instead of a user name in an ACL, it could mean that you removed a user or a group from your server, and the ACE is displaying that user’s or group’s GUID because it cannot map the GUID to a user or a group.
Part Five: Implementing Deployment Solutions

After completing Part Five, “Implementing Deployment Solutions” in *OS X Server Essentials*, you should be able to do the following tasks. Ten items from Part Five are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Explain what configuration is needed on client devices in order to take advantage of a Caching server.
- Explain how the Caching service interacts with Apple’s servers in order to cache software downloaded by clients on the local network.
- State what types of software are cached by the Caching service in OS X server.
- Explain five problems that are solved by using a NetInstall server.
- State the minimum network requirements to support client computers booting using the NetInstall service in OS X Server.
- State the location on an OS X Server computer where a NetInstall image should be stored so that it can be used by the NetInstall service.
- Copy a network disk image to the correct location so that it can be used by the NetInstall service.
- State three methods that can be used to configure the client computer to boot using an image provided by a NetInstall server.
- State what keys should be pressed during startup to configure a Mac computer to boot from a NetInstall server.
- Define shadow files, NetBoot, NetInstall, and NetRestore as they apply to OS X Server.
- List the client computers that are booted using a network boot image hosted by OS X Server.
- List the initial steps a client computer goes through when it’s configured to boot using a NetInstall server.
- Identify, in a set of NetInstall log files, an issue that would prevent the service from serving images to clients properly.
- State the minimum system requirements for client computers booting using the NetInstall service in OS X Server.
- Describe the purpose of the filters in the NetInstall service.
- Locate the System Image Utility application on an OS X computer.
- Explain the differences between the three types of System Image Utility images: NetBoot, Network Install, and NetRestore.
- List the types of sources (install application, install media, and disk volumes) that can be used to create a NetBoot or NetInstall image.
- Compare and contrast the benefits of 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 OS X version for a NetBoot or NetInstall image source.
• Create a network boot image that can be used by the NetInstall service on an OS X Server computer so that other Mac computers can use the image as a boot volume.

• Configure the NetInstall service to set which volumes on the server will be used to store NetInstall data.

• Create a network boot image that can be used by the NetInstall service so that other Macs on the network can boot from the image to install software.

• Start and stop the NetInstall service.

• Enable a network boot image in the NetInstall service so that client computers can boot using it.

• Configure the OS X computer to boot using the NetInstall service by pressing a key sequence during startup.

• Configure an OS X computer to boot using a specified image.

• Configure the NetInstall service to allow or deny the specified client computers access to the NetInstall service.

• Configure which network boot image will be the default image used by the NetInstall service.

• Set what protocol will be used to serve a network boot image.

• Display the NetInstall log files so that they can be used for troubleshooting.

• Explain 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 in OS X Server, including how it can automatically download updates provided by Apple and share only select updates to clients.

• Configure the Software Update service to automatically download all software updates provided by Apple.

• Configure the Software Update service to automatically enable any updates that have been downloaded from Apple.

• Configure the Software Update service to automatically delete unused or legacy updates.

• Enable updates in the Software Update service so that they’re accessible by other computers on the network.

• List what Apple-provided updates are available to be downloaded.

• Configure a profile to enable the OS X computer to use the given OS X Server as the source for any software updates to be applied to the OS X computer.
Lesson Fifteen review questions

After completing Lesson Fifteen, 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 NetInstall 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 images?

Answers

1. Because NetBoot unifies and centralizes the system software that NetBoot clients use, software configuration and maintenance are reduced to a minimum. A single change to a NetBoot image propagates to all client computers on the next startup. NetBoot also decouples the system software from the computer, decreasing potential time invested in software troubleshooting.

2. A client can select a network disk image via the Startup pane within System Preferences; hold down the N key at startup to use the default NetInstall image; or use the Option key to enter the Startup Manager.

3. NetInstall makes use of DHCP, TFTP, NFS, and HTTP during the NetInstall client startup sequence. DHCP provides the IP address, TFTP delivers the boot ROM ("booter") file, and NFS or HTTP is used to deliver the network disk image.

4. Because the NetBoot boot image is read-only, anything that the client computer writes to the volume is cached in the shadow file. This allows a user to make changes to the boot volume, including setting preferences and storing files; however, when the computer is restarted, all changes are erased.

5. NetBoot allows multiple computers to boot into the same environment. NetInstall provides a convenient way to install operating systems and packages onto multiple computers. NetRestore provides a way to clone an existing image to multiple computers.

Lesson Sixteen review questions

After completing Lesson Sixteen, you should be able to answer the following questions.

1. What version of OS X is required for a Mac to use the Caching service via the Mac App Store? What version of iTunes is required for Macs and for PCs to use the Caching service?
What version of iOS is required for iOS devices to use the Caching service?

2. What additional configuration do you need to perform for eligible computers with OS X and for iOS devices to use the Caching service?

3. If your server has a public IPv4 address (as opposed to having a private IPv4 address behind NAT), and your clients have a private IPv4 address behind NAT, will your clients use your server’s Caching service?

4. What configuration is required if you have multiple servers with the Caching service turned on?

5. Can a Mac use the Software Update service and the Caching service simultaneously?

6. If you change the volume used for the Caching service, is the cached content moved to the new volume?

7. Will the Caching service fill up a volume with cached content?

8. How much available space do you need on a volume in order to specify to use it for the Caching service?

Answers

1. For the Mac App Store, OS X version 10.8.2 or later is required; as for iTunes for Macs and for PCs, iTunes version 11.0.2 or later is required. iOS devices with iOS 7 automatically use the Caching service if available.

2. No additional configuration is required for computers with OS X version 10.8.2 or later, or for iOS 7 devices.

3. No, your clients and your server must have private IPv4 addresses behind a NAT device that translates outgoing traffic (to the Internet) to use the same public IPv4 address.

4. You don’t need to perform any additional configuration; eligible clients will use the appropriate Caching server automatically.

5. No, a Mac can use either the Software Update service or the Caching service.

6. Yes, if you change the volume for the Caching service, the Server app automatically moves the cached content to the new volume.

7. No, the Caching service automatically removes the least recently downloaded item to make room for new content, after the volume has only 25GB available.

8. The Server app requires that a volume have 50GB available before you can use it for the Caching service.
Lesson Seventeen review questions

After completing Lesson Seventeen, you should be able to answer the following questions.

1. What are the advantages of using Software Update?
2. What are three logs available to monitor the service?
3. How can you configure a client to use the update service?
4. What is the default port used?
5. What level of management can Software Update be applied to in Profile Manager?

Answers

1. You can better administer updates to clients and prevent high-bandwidth usage from your clients all reaching out to the Apple update servers, keeping the traffic within your network.
3. Use the defaults command to modify the update plist or a configuration profile.
4. The default port is 8088. This is important as it needs to be defined in the catalog URL even though it isn’t shown in the configuration panes of the Server app.
5. Devices and device groups.
Part Six: Providing Network Services

After completing Part Six, “Providing Network Services” in OS X Server Essentials, you should be able to do the following tasks. Nine items from Part Six are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

• State where on an OS X Server computer, with the Time Machine service enabled, the user backup data is stored.
• Enable the Time Machine service in OS X Server.
• Configure the Time Machine service so that it uses the specified drive to store backup data.
• 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 to provide access.
• Enable the VPN service on the server to allow remote users to connect to the internal network.
• Configure the shared secret for the VPN service.
• Configure the address range that's used to assign addresses to users connecting to the network via the VPN service.
• State the standard web server on which the Websites service in OS X Server is based.
• List the three different methods for distinguishing between multiple 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 in OS X Server.
• Start and stop the Websites service on the OS X Server computer.
• Configure two or more websites on the server so that each is uniquely accessible.
• Create a new website so that other computers on the network can access the web files stored on the server.
• Delete a website hosted by OS X Server so that it's not accessible by other computers.
• Configure the location of the data files for a website hosted by OS X Server.
• Configure a website so that it requires a user to authenticate before the user can access the website.
• Configure the permissions of the files so that they can be served by the Websites service.
• Enable the DHCP service in OS X Server.
• Isolate and resolve DHCP issues with a DHCP client or with the DHCP service.
Lesson Eighteen review questions
After completing Lesson Eighteen, you should be able to answer the following questions.

1. What services must be running for Time Machine to provide a network backup target?
2. If you change the volume that Time Machine is backed up to, what will happen from the client side?
3. Why might you want to exclude certain folders from being backed up?
4. Can you recover what was in the Trash?

Answers
2. An entire backup will occur, rather than just the changes from the last backup.
3. You might exclude certain folders to preserve space or to avoid backing up unneeded material.
4. No, the contents in the Trash aren’t backed up.

Lesson Nineteen review questions
After completing Lesson Nineteen, you should be able to answer the following questions.

1. What kind of users would benefit from using the VPN service?
2. What is an easy way to help your users running OS X to quickly configure their computers to use your server’s VPN service?
3. What two protocols does the OS X Server VPN service support?
4. What are the differences between the two supported VPN protocols?
5. If the shared secret becomes discovered, does this mean that anyone in the world can now use your server’s VPN service?
6. What do you need to do if you decide to change the shared secret?

Answers
1. Users who are away from your local network can use the VPN service to securely access resources available on your local network.
2. In the Server app sidebar, select VPN, click Save Configuration Profile, and distribute the resulting mobileconfig file to your users. When a user of a computer running OS X Lion or later opens the mobileconfig file, the Profiles preferences
automatically opens and prompts the user to install the configuration profile. You can also distribute the mobileconfig file to users of iOS devices.

3. L2TP and PPTP.
4. L2TP is more secure, but PPTP is compatible with older VPN client software.
5. Not necessarily; even if the shared secret becomes published, users still need to authenticate with a username and password to establish a VPN connection.
6. If you change the shared secret, all your VPN service users must change the shared secret in their VPN configurations. You can facilitate this change by saving a new configuration profile and distributing the new mobileconfig file to your users.

Lesson Twenty review questions
After completing Lesson Twenty, you should be able to answer the following questions.

1. If a host computer or device is on an active network with other clients receiving DHCP addresses, why might this specific computer or device not get an IPv4 address?
2. How can you determine whether a host has a routable IPv4 address or a link-local address?
3. What must you know before you can statically map an IPv4 address to a specific client?
4. Where would you find log entries related only to the DHCP service?

Answers

1. If other computers and devices on a given network are able to secure DHCP addresses, it’s likely that the server has run out of DHCP leases.
2. A link-local address must fall in the 169.254.x.x range, so checking the current IPv4 address of the client will provide the answer.
3. You must know the MAC address of the client; if the client already has a DHCP lease, simply create a static address from that client's entry in the Clients pane.
4. In the Server app's Logs pane (in the Service Log under the DHCP section).

Lesson Twenty-one review questions
After completing Lesson Twenty-one, you should be able to answer the following questions.

1. On what software is the OS X Server Websites 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. The Websites service is based on Apache, the open source web server software.

2. Everyone or the “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 the 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.
Part Seven: Using Collaborative Services

After completing Part Seven, “Using Collaborative Services” in OS X Server Essentials, you should be able to do the following tasks. Eighteen items from Part Seven are included in the pool of exam questions. Questions are drawn randomly from the following objectives:

- Define the terms “wiki” and “blog” as they apply to OS X Server.
- State three benefits of setting up a wiki server.
- Delete a wiki hosted by the Wiki service in OS X Server.
- Configure a wiki to provide a blog.
- Enable the Wiki service on the server.
- Add a given group to the list of those who can create a wiki on the server.
- Configure the server so that anyone can create a wiki on the server.
- Create a new wiki.
- Modify the permissions for the given list of wiki users.
- 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 the Mail 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 when handling outgoing email a mail server identifies the network address of the destination mail server.
- State what the Mail service on an OS X Server uses to scan mail messages for viruses.
- Explain what service the Mail service on an OS X Server uses to analyze mail messages to determine the likelihood of the message being junk mail.
- Explain what service a blacklist server provides.
- Stop and start the Mail service in OS X Server.
- Configure how aggressive the Mail service in OS X Server should be in filtering for junk mail.
- Configure a user account in OS X Server to be able to send email via the server.
- Configure the domain name for the Mail service.
- Configure the Mail service to relay all outgoing email through a specified mail server.
- Configure the Mail service so that users can’t store more than a specified amount of mail on the server.
- Configure the Mail service to scan mail messages for viruses.
- Configure the Mail service to use a blacklist server to filter junk mail.
• Configure the Mail service to filter for junk mail.
• List three reasons why you would want to provide shared calendar services using the Calendar service on an OS X computer.
• 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).
• State which protocols are used by the Calendar service in OS X Server.
• Explain the purpose of the federation feature for the Messages service in OS X Server.
• Explain the benefits of setting up a chat server, including automatically generating chat transcripts and increased security.
• State the Messages server screen name for a given user account.
• Configure the Messages service so that all chat messages are logged to a file on the server.
• Display chat messages, if any, that have been stored on the server.
• Enable the server-to-server federation feature for the Messages service.
• Configure the Messages service to allow federation with any other XMPP chat server.
• Configure the Messages service to allow federation with a specified XMPP chat server.
• Display the Messages service log.
• Enable the Calendar service so that two or more OS X client computers can access and share calendar data.
• Troubleshoot issues with the Messages service.
• Enable or disable access to the Messages service for a given user account.
• Configure Calendar on an OS X computer so that it displays the shared scheduling data provided by the Calendar service.
• Start and stop the Messages service on an OS X Server computer.
• Troubleshoot issues with the Calendar service.
• Add a service account to the Messages app on an OS X computer so that it can be used to chat with other Messages users via the Messages service in OS X Server.
• Explain the benefit of enabling the Contacts service option to allow users to search an LDAP directory.
• Explain how contact data is shared between OS X computers and the Contacts service in OS X Server.
• Explain how to configure an OS X computer to access shared contact information provided by the Contacts service in OS X Server.
• Configure the Contacts service so that users can store contact information on the server.
• Configure the Contacts service to provide contact information provided by a directory server.
• Configure the Contacts app on an OS X computer to access contact information provided by the Contacts service in OS X Server.

Lesson Twenty-two review questions
After completing Lesson Twenty-two, you should be able to answer the following questions.

1. What protocols can Mail service utilize?
2. What kind of DNS record should be set up for a mail server in production use?
3. What tools are used for filtering the Mail service?

Answers
1. POP, IMAP, and SMTP.
2. An MX record for the domain.
3. SpamAssassin filters for spam; ClamAV for virus scanning; and an external blacklist server can be set for junk mail filtering. Greylisting also helps reduce spam.

Lesson Twenty-three review questions
After completing Lesson Twenty-three, you should be able to answer the following questions.

1. What is a wiki? What is a blog?
2. What tools can an administrator use to specify users that are allowed to create wikis?
3. How does a network user specify which users and groups are allowed to edit a wiki?

Answers
1. A wiki is designed to be read and edited by many. A blog is designed to be read by many, but created by an individual.
2. Administrators can use the Wiki Creators list in the Wiki service settings of the Server app.
3. When creating a wiki with a web browser, a user can specify permissions for users and groups to access and edit the wiki.
Lesson Twenty-four review questions
After completing Lesson Twenty-four, you should be able to answer the following questions.

1. What protocol does Calendar use?
2. How does a user specify which users are allowed to edit or view his calendar?
3. What is the transport protocol for the Calendar service and how can that impact the troubleshooting of the service?

Answers
1. CalDAV, which is an extension of WebDAV.
2. In the Calendar app preferences, he can designate delegates and their rights.
3. CalDAV and WebDAV utilize HTTP as a transport and as a result the troubleshooting of it is similar to web services. You need to make sure DNS is correct and the proper ports are open.

Lesson Twenty-five review questions
After completing Lesson Twenty-five, you should be able to answer the following questions.

1. What protocol is used for the Messages service?
2. How would you limit access to the Messages service on OS X Server?
3. How would you enter the Messages name for the user Jet Dogg (short name: jet) on server17.pretendco.com?

Answers
3. The Messages name format for Jet Dogg is jet@server17.pretendco.com.

Lesson Twenty-six review questions
After completing Lesson Twenty-six, you should be able to answer the following questions.

1. On what protocols is the Contacts service based?
2. How can the information contained in a directory service be included in the Contacts searches?
3. Where is SSL for the Contacts service configured for use?
Answers

1. The OS X Server Contacts service is based on CardDAV (an extension to WebDAV), HTTP, and HTTPS, as well as vCard (a file format for contact information).

2. Make sure the “Include directory contacts in search” option is selected in the configuration of the Contacts service.

3. In the Settings pane of the Certificates tab of the Server app.