macOS Support Essentials 10.12

Supporting and Troubleshooting macOS Sierra

Exam Preparation Guide

Contents

Becoming an Apple Certified Support Professional

The Apple Training and Certification program keeps 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 two macOS certifications:

- Apple Certified Associate—Mac Integration
- Apple Certified Support Professional (ACSP)

ACSP certification is for the help desk professional, technical coordinator, or power user who supports macOS users, manages networks, or provides technical support for Mac users. ACSP certification verifies that you understand macOS core functionality and that you can complete these tasks:

- Configure key services
- Perform basic troubleshooting
- Support multiple Mac users

Passing the macOS Support Essentials 10.12 Exam is an essentials part of earning your ACSP certification. For more information, visit Training and Certification: Get certified.

ACSP certification benefits

Besides differentiating you as a skilled user and support professional for macOS Sierra, an ACSP certification enables you to benefit from the power of the Apple brand. When you pass the certification exam, you receive an email that details 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 so you can easily share your certification news with your networks on these sites.

You also receive a login for the Apple Certification Records System, where you can take the following actions:

- Update your profile and opt in to display your Apple Certification in the Apple Certified Professionals Registry.
- Review your certification progress.
- Download your certification logo to use on business cards, résumés, websites, and more.
- Provide access to employers to verify your certifications.

Recommended Exam Preparation

The following exam preparation is recommended:

- Complete the Sierra 101: macOS Support Essentials 10.12 course.
- Study the Apple Pro Training Series book *macOS Support Essentials 10.12* by Kevin M. White and Gordon Davisson.
- Gain experience with macOS.
- Read this guide and practice completing the sample tasks and answering the review questions.

Complete the course

AATPs offer courses where you can learn more about macOS by using it. You'll also benefit from the expertise of Apple Certified Trainers and your peers. LearnQuest is an AATP and you can visit their website to find nearby course offerings.

Study the book

Apple Pro Training Series *macOS Support Essentials 10.12* is the basis for the ASCP exam. You can purchase the book from several locations:

- iBooks Store—if you use an iOS device or Mac
- Safari—Safari is an on-demand digital library that offers subscription access to the Apple Training and Apple Pro Training Series, as well as thousands of other reference videos and books.
- Peachpit—Visit the Peachpit website to save 30 percent.

This book may be available in other languages. See the Peachpit website for details.

Gain experience with macOS

There's no substitute for time spent learning macOS technology. After you read the book, take the course, or both, spend time increasing your familiarity with macOS to ensure your success on the certification exam.

Use this guide

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 practicing the tasks and answering the review questions in the following sections.

The tasks and questions cover the knowledge domains that are assessed by the ASCP exam. Although this guide divides the tasks and review questions into lessons or knowledge areas, questions are presented randomly during the exam.

Exam Details

The macOS Support Essentials 10.12 exam is computer-based and offered at Apple Authorized Training Providers (AATPs). To find the closest AATP, visit Training and Certification: Find an Apple Authorized Training Partner. LearnQuest is Apple's global training partner. If you don't see a session scheduled at your nearest LearnQuest training center, contact LearnQuest to find out whether a session can be scheduled. All LearnQuest training centers offer all macOS and pro apps exams, even if they don't offer the corresponding course.

Here are the macOS Support Essentials 10.12 exam details:

- There are five unscored demographic questions. You have 5 minutes to complete them.
- There are 80 scored technical questions. You have 120 minutes to complete them.
- The exam uses a random pool of multiple-choice and interactive-media questions.
- A passing score is 75 percent. Scores aren't rounded.
- Details on exam scoring are at Training and Certification: Exam and Certification Questions.
- You may not access any resources or references during the exam.
- Some exams are available in multiple languages. For details, visit Training and Certification: Localized Apple Certification Exams.

If you have questions about exams, visit Training and Certification: Exam and Certification Questions.

Part One: Installation and Configuration

After you complete Part One, "Installation and Configuration," in *macOS Support Essentials 10.12,* you should be able to perform the following tasks:

- Describe the process for creating an external macOS Recovery volume.
- Describe how you can get the macOS installer.
- State the minimum hardware and software requirements for installing macOS Sierra.
- Verify that a Mac meets the minimum hardware requirements to install macOS Sierra.
- List four steps you should take before you install macOS Sierra.
- State the types and sources of data that Migration Assistant can migrate from.
- Identify the latest version of firmware that's available for a Mac that's running macOS Sierra.
- Navigate to the Support or Downloads pages on the Apple website to find the latest compatible firmware update.
- Describe the process for reinstalling macOS Sierra by using the macOS Recovery volume.
- Describe how formatting a Mac hard disk into a single partition can simplify the process of preparing to install macOS Sierra.
- Describe how formatting a Mac hard disk into multiple partitions can simplify the process of configuring and using the Mac.
- Describe how to simplify maintaining multiple operating systems by installing them on a multiple-partition drive.
- Describe how to simplify keeping operating system data and user data separate by installing macOS Sierra on a multiple-partition drive.
- Describe the macOS Sierra installation process, including choosing Installer interface options.
- List the utilities available to the user when a Mac starts up from the macOS recovery volume.
- Configure a Mac with macOS Sierra for use on a local area network with Internet access.
- State where in macOS you configure network settings.
- Describe how to use configuration profiles to manage settings on a Mac.
- Describe how to use Setup Assistant to configure settings on a Mac.
- Describe how software and security updates are made available to client Mac computers.
- Identify any software updates that were installed on a Mac that's running macOS Sierra.
- Define the terms "version number," "build number," and "serial number" as they pertain to a macOS Sierra installation.
- On a Mac that's running macOS Sierra, identify the system version number, build number, and serial number.

Lesson 1—"Install macOS Sierra" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What are the minimum requirements for upgrading a Mac to macOS Sierra?
2. What are the four steps you must take before upgrading a Mac to macOS Sierra?
3. How can you identify whether a Mac requires a firmware update?
4. What are the advantages and disadvantages of using a single- or multiple-partition disk with macOS Sierra?
5. How can you get the macOS installer?
6. What option do you have during the macOS Sierra installation?
7. If a macOS Sierra installation fails, where can you find out more about why it failed?

Answers

1. These are the minimum requirements for upgrading macOS Sierra:
   - Mac OS X 10.7.5 or later
   - 2 GB of memory
   - 8.8 GB of available storage space
   - A compatible Mac model (as listed in Upgrade to macOS Sierra)

   In addition, some features require an Apple ID or a compatible Internet service provider.
2. These are the four steps you should take before upgrading a Mac to macOS Sierra:
   a. Verify app compatibility.
   b. Back up important files and folders.
   c. Document critical settings.
   d. Install Apple software and firmware updates.
3. You can identify a Mac firmware version by opening the full system report in System Information or System Profiler. You can verify whether the Mac firmware is up to date by visiting the Apple support website, which shows available firmware updates.
4. Single-partition drives are easier to set up initially, but they aren't as flexible for administration and maintenance. Multiple-partition drives require repartitioning during setup but provide several separate partitions, which can be used to segregate user data and host multiple operating systems.
5. You can download the macOS Sierra installer from the App Store for free.
6. During macOS Sierra installation, the only option you have is to define an installation destination other than the Mac computer's current default system disk.
7. To find out more about why a macOS Sierra installation failed:
   1. Open Console.
   2. Go to /var/log/.
   3. Open and review install.log.

Lesson 2—"Set Up and Configure macOS" review questions

After you complete this lesson, you should be able to answer the following questions:

1. Which tool guides you through the initial macOS Sierra configuration?
2. Which key features do you gain by setting up iCloud?
3. After you configure macOS Sierra, where can you manage iCloud settings?
4. What's a profile? How do you manage profiles?
5. Where can you find the system version number, build number, and hardware serial number? What's the significance of these numbers?

Answers

1. Setup Assistant guides you through the macOS Sierra configuration process.
2. iCloud is a free service from Apple that provides cloud storage and communication services for apps, including Mail, Contacts, Calendars, Reminders, Notes, Safari, Keychain, Photos, and any other apps that support iCloud integration. iCloud also provides Find My Mac technology for help locating a lost or stolen Mac.
3. After you set up macOS Sierra, you can manage iCloud settings from iCloud or Internet Accounts preferences.
4. A profile is a document with the filename extension .mobileconfig that contains system settings as defined by an administrator. When you open a profile document, macOS Sierra installs the profile and configures the settings. You can manage installed profiles through Profiles preferences.
5. You can find the system version, build number, and hardware serial number are located in the About This Mac dialog or the login screen. The system version number defines the specific version of macOS Sierra currently installed. The system build number is an even more specific identifier used primarily by developers. The hardware serial number is a unique number used to identify your Mac.

Lesson 3—"Use macOS Recovery" review questions

After you complete this lesson, you should be able to answer the following questions:

1. Which utilities are available when you start up from macOS Recovery?
2. Which two resources does the local hidden macOS Recovery HD need to reinstall macOS Sierra?
3. How can you use create an external macOS installation disk?

Answers

1. The macOS Recovery System provides access to Restore System from Time Machine Backup, Install/Reinstall macOS, Get Help Online through Safari, Disk Utility, Startup Disk, Firmware Password Utility, Network Utility, Terminal, and Reset Password.
2. The local hidden macOS Recovery HD doesn't include macOS Sierra installation assets. So you need high-speed Internet access and the ability to verify access to the installation assets. You can verify Mac computers that were upgraded to macOS Sierra by entering the Apple ID used to download it. Verification is automatic for newly purchased Mac computers that include macOS Sierra.
3. You can create a macOS Recovery disk that includes the macOS Sierra installation assets with the createinstallmedia tool in macOS Installer.

Lesson 4—“Update macOS Software” review questions

After you complete this lesson, you should be able to answer the following questions:

1. Which app can you open to initiate Apple software updates?
2. By default, which items are always installed through automatic software updates?
3. How can you prevent a user from installing software updates?
4. Which apps can you use to manually acquire and install macOS Sierra software updates?
5. What’s the best way to discover what software is installed on a Mac?

Answers

1. Open the Mac App Store to initiate Apple software updates.
2. By default, system files and security updates are automatically installed when available.
3. You can prevent automatic updates for all users by disabling the options in App Store preferences. You can further restrict a user’s ability to use the App Store by configuring parental controls for the user’s account.
4. You can download macOS Sierra software updates from the Apple Support website using any current web browser. Updates may be installation packages that are installed by using Installer.
5. The Installations section of System Information shows the history of software installed from the App Store or the macOS Installer.

Part Two: User Accounts

After you complete Part Two, "User Accounts," in *macOS Support Essentials 10.12*, you should be able to perform the following tasks:

- Create and manage user accounts on a Mac that's running macOS Sierra.
- Describe the key features and benefits of iCloud.
- Describe the process for and result of deleting a user account from a Mac.
- Describe the process for restoring a user account on a Mac.
- List the five types of user accounts in macOS Sierra.
- Compare the user account types in macOS Sierra.
- Identify the three attributes of user accounts in macOS Sierra.
- Describe a security risk related to enabling the Guest User account in macOS Sierra.
- Describe a security risk related to enabling the Sharing Only account in macOS Sierra.
- Describe a security risk related to using an Administrator account as the primary user account in macOS Sierra.
- Describe an advantage of using an Administrator account as the primary user account in macOS Sierra.
- List the default folders in a user home folder.
- Compare the functions of each of the default folders in a user's home folder in macOS Sierra.
- List the resources that an administrator can limit in the Parental Controls pane of System Preferences.
- Describe three errors that can occur when fast user switching is enabled and two users access the same file or peripheral in macOS Sierra.
- Describe messages that indicate whether a file, peripheral, or app is busy.
- Describe errors that can occur when fast user switching is enabled and two users access a specific app at the same time.
- Describe why some apps can't be opened by more than one user at a time.
- Describe a security risk that can result when fast user switching is enabled and other local users switch to their accounts.
- Describe how users who fast-switch to their accounts can access volumes mounted by other logged-in users.
- Secure the user environment on a Mac that's running macOS Sierra.
- Describe how to enable and disable a firmware password.
- Describe the functions and features of Keychains in macOS Sierra.
- Describe how to reset a user account password using an Apple ID.
- Describe the privacy controls available for a user account.
- Describe the security features offered by iCloud for macOS Sierra.
- Compare the ways to change and reset passwords.

- Compare how each of these passwords functions in macOS Sierra: login, firmware, resource, keychain, and Apple ID.
- Compare the roles of keychains, keychain items, and keychain first aid.
- Describe how resetting a user account password can cause the keychain and user account password to get out of sync.
- Describe how the Firmware password feature prevents users from changing passwords for user accounts other than their own.

Lesson 5—"Manage User Accounts" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What are the types of user accounts in macOS Sierra? How are they different?
2. What are some security risks associated with each user account type?
3. Which two local user password types are supported by macOS Sierra?
4. What are account attributes?
5. How can you limit a user account from having full access to all apps?
6. What types of resource contention issues can occur when fast user switching is enabled?
7. Which storage-related security risk can occur when fast user switching is enabled?

Answers

1. Standard is the default account type, administrative users can make changes to the system, a guest user doesn't require a password, and sharing-only users can access only shared files.
2. Standard user accounts are very secure, assuming they have strong passwords. Administrative users can make changes that may negatively affect the Mac or other user accounts. A guest user could fill shared folders with unwanted files. Sharing-only users are generally very secure as long as they don't have too much access to other user's items.
3. In macOS Sierra, the default local user account requires a local account password. macOS Sierra supports local accounts that already use an Apple ID password, but you can't create new accounts that use an Apple ID password.
4. Account attributes are the individual pieces of information used to define a user account. Examples include full name, account name, user ID, universally unique ID (UUID), group, and home folder.
5. You can use Parental Controls to limit user account access to apps. Examples of limitations include enforcing a simple Finder, limiting apps and widgets, limiting App Store content, setting time limits, and filtering content for several apps that are included in macOS Sierra.
6. Resource contention occurs when fast user switching is enabled and a user tries to access an item that another user has open in the background. Document contention occurs when a user attempts to open a document that another user has already opened. Peripheral contention occurs when a user attempts to access a peripheral that's already in use by another user's open app. App contention occurs when a second user attempts to access an app that is designed to run only once on a system.
7. When fast user switching is enabled, all users are allowed to see other users' locally connected disks.

Lesson 6—"Manage User Home Folders" review questions

After you complete this lesson, you should be able to answer the following questions:

1. A user's home folder contains which default folders?
2. When you delete a local user account, the Users & Groups preferences gives you three options for dealing with the user's home folder content. What are they?
3. Which three primary sources can Migration Assistant pull from?
4. How do you make macOS Sierra associate a new local user account with a manually migrated or restored user's home folder?

Answers

1. The default folders in a user's home folder are Desktop, Documents, Downloads, Library (hidden), Movies, Music, Pictures, and Public.
2. When you delete a local user account, macOS Sierra can archive the home folder content into a compressed disk image, leave the home folder content in the /Users folder, or delete the home folder content. Optionally, macOS Sierra can perform a secure erase on the home folder content.
3. Migration Assistant can migrate information from other Mac computers, Windows PCs, and other disks, including Time Machine backups.
4. To make macOS Sierra associate a new local user account with a manually migrated or restored user's home folder, follow these steps:
    a. Copy the restored user's home folder to the /Users folder.

    b. Open System Preferences.

    c. Click on the Users and Groups pane.

    d. Create a new local user account with the same account name that was used for the user's home folder. macOS Sierra prompts you to associate the new local user account with the restored home folder.

Lesson 7—"Manage Security and Privacy" review questions

After you complete this lesson, you should be able to answer the following questions:

1. Which types of items can you store in a keychain?
2. How does the Keychain Access help protect your information?
3. Where are keychain files stored?
4. What app should you use to manage keychain settings?
5. When and why would you set up an iCloud Security Code?
6. What's required to set up iCloud Keychain on multiple Apple devices?
7. How can you limit the use of Location Services?
8. How can you ensure that audio recordings used for Dictation service remain private?
9. Which feature can you enable to locate a lost Mac?

Answers

1. You use Keychains to store secrets such as resource passwords, digital certificates, and encryption keys. The keychain system can also securely store Safari AutoFill information, Internet Account settings, and secure text notes.

2. Keychain manages encrypted files that are used to securely save your items. By default, users have login and Local Items keychains that use the same password as their account. Not even other administrative users can access your keychain secrets unless they know the keychain password.

3. Each user starts with a login keychain saved at /Users/*username*/Library/Keychain/login.keychain and a Local Items/iCloud keychain saved in the /Users/*username*/ Library/Keychains/*UUID* folder. Administrative users can manage macOS authentication assets with the /Library/Keychain/System.keychain. Apple maintains several items in /System/Library/Keychains/ for macOS use.

4. You can manage keychains from the /Applications/Utilities/Keychain Access app.

5. You don't need an iCloud Security Code if you set up two-factor authentication. For Apple IDs that do not have two-factor authentication enabled, you can set up an iCloud Security Code the first time you enable iCloud Keychain for a specific Apple ID. You can use the iCloud Security Code to set up other devices for the iCloud Keychain service and you can use it to regain access to the iCloud keychain if you lose all your Apple devices.

6. If you set up two-factor authentication for your Apple ID, your additional Apple devices are automatically configured to use iCloud Keychain. If you didn't set up two-factor authentication for your Apple ID, you must authorize your additional Apple devices to use iCloud Keychain by:

   - Using an Apple ID, password, and iCloud Security Code

   - Using an Apple ID and password and authorizing access from another Apple device that is configured for iCloud Keychain

7. You can use the Privacy pane of Security & Privacy preferences to configure app access to Location Services, Contacts, Calendars, Reminders, social network services, and Accessibility.

8. If you enable the Use Enhanced Dictation feature in the Dictation & Speech preferences, Audio recordings used for the Dictation service are not sent to Apple.

9. iCloud Find My Mac enables you to remotely locate a lost Mac. You enable this feature in iCloud preferences. To locate a lost Mac, use the iCloud website or the Find My iPhone app on an iOS device.

Lesson 8—"Manage Password Changes" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What does the master password do?

2. When users change their own account passwords, how are their login keychains affected?

3. What options are available when you try to change the password for a user account with an Apple ID password?

4. How can you reset a user's lost account password?

5. How does resetting a user's account password affect that user's login keychain?

6. How does Firmware Password Utility help prevent users from making unauthorized password changes?

Answers

1. Use the master password to reset local account passwords.
2. When users change their own account passwords, the system keeps their login keychain passwords in sync.
3. When you change the password for a user account with an Apple ID password, you can change to a separate, locally saved password or to the Apple ID password.
4. You can reset local account passwords in Users & Groups, by the master password at login, by a FileVault recovery key at startup, and by the Reset Password assistant in macOS Recovery. Users with local accounts with an Apple ID and password can manage their Apple IDs and passwords at https://appleid.apple.com or https://iforgot.apple.com.
5. The account password reset process won't change any keychain passwords. Therefore, the user's keychains don't automatically open when the user logs in with a new password. The user will have to manually change the keychain passwords using the Keychain Access utility.
6. The Firmware Password Utility prevents users from starting up from another system disk. This prevents them from using macOS Recovery to reset local passwords without authorization.

Part Three: File Systems

After you complete Part Three, "File Systems," in *macOS Support Essentials 10.12*, you should be able to perform the following tasks:

- Describe the implications and process for converting Legacy FileVault data to FileVault.
- State the requirements for FileVault.
- Describe how to securely erase the remaining space on a drive connected to a Mac that's running macOS Sierra.
- Describe how to force eject an item that's in use.
- Describe how to reset home folder permissions.
- Describe how to enable FileVault on a volume connected to a Mac that's running macOS Sierra.
- Describe how to decrypt a FileVault-encrypted volume using a recovery key.
- Describe how to get information about the format, partition scheme, bus type, and available space on local hard disks and volumes.
- Use Disk Utility and System Information.
- Differentiate between hard disks, partitions, and volumes.
- Compare GUID, APM, and MBR partition map schemes.
- Compare the volume formats supported by macOS Sierra:
    - Mac OS Extended
    - Mac OS Extended (Journaled)
    - Mac OS Extended (Journaled, Case-Sensitive)
    - UFS

    - FAT32
    - NTFS
    - ExFAT
    - Mac OS Extended (Journaled, Encrypted)
- Describe how file system journaling works in macOS Sierra.
- Describe how FileVault secures user data.
- Describe the Disk Utility First Aid feature.
- Compare the Disk Utility erase options, including single-pass, 3-pass, and 7-pass erases.
- Describe the function of the Secure Empty Trash feature in the Finder.
- Describe how power failures and force ejecting a disk can corrupt a volume.
- Identify three ways to unmount a disk from the Finder.
- Describe target disk mode.
- Manage file ownership and permissions.
- Describe how to use the Get Info window in the Finder to manage permissions for files and folders.
- Describe how to use Disk Utility to repair file and folder permissions.
- Describe the function of each of the permission settings and ACL settings on macOS Sierra files and folder.
- Identify the owner and group for any file on a Mac that's running macOS Sierra.
- Use the Get Info command in the Finder.
- Identify the owner and group permission settings for users' home folders in macOS Sierra.
- Describe why the root of any user's home folder in macOS Sierra is accessible to other users.
- Describe the permissions settings on the Shared folder in macOS Sierra that allow it to act as a shared storage location for local user accounts.
- Describe what it means to "ignore volume ownership," including when it's useful to do so, and one potential risk when ignoring ownership.
- Describe how anyone can access any file on the drive while ownership is ignored.
- Describe how the macOS Sierra file-system organization enables multiple users to safely share local files and folders.
- Define the term "sticky bit" as it applies to the macOS Sierra file system.

Lesson 9—"Manage File Systems and Storage" review questions

After you complete this lesson, you should be able to answer the following questions:

1. How are disks, partitions, and volumes different from one another?
2. What are the two primary partition schemes for Mac formatted disks? What are their differences?
3. What two-volume formats are supported for a macOS Sierra system volume?

4. How does file system journaling work?

5. What is Core Storage, and what two major macOS Sierra features are implemented through Core Storage?

5. What are the five ways you can eject a volume or disk from the Finder?

6. What is the potential side effect of improperly unmounting or ejecting a disk or volume?

7. Which two built-in macOS Sierra apps can you use to gather information about storage devices?

8. What are the four erase options available in Disk Utility? How are they different?

9. How can you encrypt a disk without losing its contents?

10. What does the Disk Utility First Aid feature do?

11. What is target disk mode and how is it engaged?

Answers

1. Disks are the storage hardware. Partitions are logical disk divisions that are used to define storage space. Volumes, contained inside partitions, are used to define how individual files and folders are saved to storage.

2. GUID Partition Table is the default partition scheme on Intel-based Mac computers. Apple Partition Map is the default partition scheme on PowerPC based Mac computers.

3. The volume formats supported as system volumes for macOS Sierra are Mac OS Extended (Journaled) and Mac OS Extended (Journaled, Encrypted).

4. File system journaling records which file operations are in progress at any given moment. This way, if a power failure or system crash occurs and the system restarts, it can quickly verify the integrity of the volume by "replaying" the journal.

5. Core Storage is a file system management layer that's used by macOS Sierra to provide disk encryption as used by FileVault, and to combine separate disks as used by Fusion Drive.

6. These are the five methods used to eject a volume or disk in the Finder:

   - Drag the disk icon to the Trash in the Dock.
   - In the Finder sidebar, click the small Eject button next to the volume you want to eject.
   - Select the volume you want to eject and then choose File > Eject.
   - Select the volume you want to eject and then use the Command-E keyboard shortcut.
   - Select the volume you want to eject and Control-click to reveal a pop-up menu. Select Eject.

7. Improperly unmounting or ejecting a drive or volume may cause data corruption. macOS Sierra automatically verifies and repairs an improperly unmounted or ejected volume the next time it becomes available to the Mac.

8. Disk Utility and System Information can both be used to gather information about storage devices.

9. These are the four erase options in Disk Utility:

   - Don't Erase Data—Fastest and replaces the volume's directory structure
   - Pass Erase—Writes a pass of random data followed by a pass of zeros on the disk
   - Pass Erase—Writes two separate passes of random data followed by a third pass of zeros on the disk

- 7-Pass Erase—Most secure; writes seven separate passes of random and patterned data on the disk

10. From the Finder, you can encrypt a disk without losing its contents by right-clicking the disk and then choosing Encrypt from the shortcut menu.
11. Use the Disk Utility First Aid feature to verify and repair the partition scheme and directory structure of a volume. These elements contain the information used to locate files and folders on the volume.
12. Target disk mode shares a Mac computer's internal disks through FireWire ports. You can engage Target disk mode from Startup Disk preferences or by holding down the T key as you turn on the Mac.

Lesson 10—"Manage FileVault" review questions

After you complete this lesson, you should be able to answer the following questions:

1. How does FileVault protect user data?
2. What are the system requirements for using FileVault?
3. Which users are allowed to unlock a FileVault-protected system?
4. What are the two ways you can save the FileVault recovery key when you enable FileVault in Security & Privacy preferences?
5. How can you unlock a Mac protected by FileVault when all users have lost their passwords?

Answers

1. FileVault protects the entire system volume and all its data by using strong XTS-AES 128 encryption. During system startup, a user must enter a password to decrypt the system volume.
2. To enable FileVault, Mac computers must have the hidden macOS Recovery HD volume on the system disk. Also, any Legacy FileVault accounts must be decrypted and returned to normal accounts before FileVault can be enabled.
3. Any user who's FileVault enabled can unlock a FileVault-protected system. This includes any local or cached network user account that was enabled when FileVault 2 was set up or created after FileVault 2 was enabled. Also, administrators may return to Security & Privacy preferences to enable additional accounts.
4. When you enable FileVault in the Security & Privacy preferences, you can either manually save the FileVault recovery key using your own devices, or you can save the recovery key on Apple's servers through an iCloud account.
5. Use the recovery key that was generated during the FileVault setup process to unlock a FileVault-protected Mac. Use the recovery key during system Mac startup to reset the user's account password.

Lesson 11—"Manage Permissions and Sharing" review questions

After you complete this lesson, you should be able to answer the following questions:

1. How do you identify the ownership and permissions of a file or folder in the Finder?
2. How do ACLs differ from standard UNIX file system permissions?
3. What's the locked file flag?
4. Why is the root (or beginning) level of a user's home folder visible to other users?

5. How does the default organization of the file system allow users to safely share local files and folders?
6. What's unique about the permissions of the /Users/Shared folder?
7. What does it mean when you choose the option to "ignore volume ownership" in the Finder? What are the security ramifications of ignoring volume ownership?

Answers

1. You can use the Info or Inspector windows in the Finder to identify an item's ownership and permissions.
2. Standard UNIX file system permissions allow for permissions to be set only for one owner, one group, and all others. ACLs allow for an unlimited list of permissions entries.
3. The locked file flag prevents anyone, including the item's owner, from editing an item. Only the item's owner can unlock the item to then allow modification.
4. The root level of a user's home folder is visible to other users so they can navigate to the Public shared folder.
5. Every home folder contains a Public folder that other users can read and a Drop Box folder that other users can write to. All other subfolders in a user's home folder (except the optional Sites folder) have default permissions that don't allow access by other users. The Shared folder is also set for all users to share items.
6. The Shared folder is set up to allow all users to read and write files, but only the user who owns an item can delete it from the Shared folder. This is accomplished using the sticky bit permissions setting.
7. You can choose to ignore ownership on any nonsystem volume. This will ignore any ownership rules and grant any logged-on user unlimited access to the contents of the volume. It's a potential security risk because it will allow any local user account to have full access to the volume, even if that user didn't originally mount the volume.

Part Four: Data Management

After you complete Part Four, "Data Management," in *macOS Support Essentials 10.12*, you should be able to perform the following tasks:

- Manage user and system files on a Mac that's running macOS Sierra.
- Compare the features and functions of aliases and links as implemented in macOS Sierra.
- Describe how to create aliases and links.
- Describe the structure and purpose of the AppleDouble metadata format.
- Describe how to navigate to and view the contents of hidden folders in the Finder.
- Describe how to install fonts.
- List the four default top-level folders visible in the Finder: Applications, Library, System, and Users.
- Describe the types and function of metadata as it applies to the file system.
- Compare the System, Local, User, and network domains, including what resources are stored in each, and the order in which macOS Sierra searches for resources in the file system.

- Describe macOS Sierra extended attributes and give an example of information the system keeps as an extended attribute.
- Compare these file types: extensions, frameworks, fonts, preferences, startup items, and logs.
- Compare file system packages and bundles and their purposes.
- Identify where each of these file types are in the file system: extensions, frameworks, fonts, preferences, startup items, and logs.
- Describe how Spotlight metadata is used in macOS Sierra.
- Describe how and why the Finder hides certain folders by default.
- Identify potential privacy and security issues with Spotlight.
- Describe where metadata indexes and plug-ins are stored in the macOS Sierra file system.
- Archive files on a Mac that's running macOS Sierra.
- Describe how to manage a zip archive of selected items in the Finder.
- Compare disk images created with Disk Utility and zip archives created by the Finder.
- Describe the options available when you create a new blank image using Disk Utility in macOS Sierra.
- Configure and manage Time Machine on a Mac that's running macOS Sierra.
- Describe how encryption is used in a Time Machine backup.
- Describe how to configure Time Machine to back up and restore data from specific volumes to specific destinations.
- Describe how Time Machine works.
- Identify the files that are always omitted from Time Machine backups.
- Describe issues with backing up large database files that are frequently updated.
- List issues such as space limitations that interfere with backups.
- Describe the archive format used by Time Machine.
- Describe why a specific archived file may not be available due to backup or retention schedule parameters.

Lesson 12—"Use Hidden Items, Shortcuts, and File Archives" review questions

After you complete this lesson, you should be able to answer the following questions:

1. Why does the Finder hide certain folders at the root of the system volume?
2. What two methods are used to hide items from the Finder?
3. What does macOS Sierra use bundles and packages for?
4. How does an alias differ from a symbolic link?
5. Why would you use an archive file instead of a disk image? Why would you use a disk image instead of an archive file?
6. What type of file does the Finder create when you select the Archive option?
7. What action on macOS Sierra is set as the default for opening zip archive files?

8. Which macOS Sierra app is responsible for creating and managing disk images?

Answers

1. The Finder hides traditional UNIX resources from average users because they don't need access to those items. If users do need access to UNIX items, they can use Terminal.
2. The Finder doesn't show items with periods at the beginning of their filenames or items with the hidden file flag enabled. Both methods for hiding items can be managed only from the command-line interface.
3. Bundles and packages are used to combine complex items into individual folders. Packages have the additional advantage of appearing as a single item in the Finder. This allows software developers to combine resources into a single item and prevents users from seeing and potentially damaging those resources by deleting or moving files.
4. Both aliases and symbolic links act as a shortcut to an original item. However, an alias contains additional information that allows the system to keep track of the original item if it's renamed or moved within the same volume. In contrast, any change to an original item breaks a symbolic link.
5. Archive files are much simpler to create in the Finder and are compatible with third-party operating systems. Disk images are more difficult to create and manage but offer greater flexibility, primarily because they can be easily modified and converted. However, macOS Sierra disk images aren't compatible with third-party operating systems.
6. The Archive option in the Finder creates compressed zip archive files.
7. By default on macOS Sierra, double-clicking a zip archive causes the system to expand the contents of the zip archive next to the same location as the original zip archive.
8. Disk Utility is the primary app for creating and managing disk images.

Lesson 13—"Manage System Resources" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What are the four default top-level folders visible in the Finder?
2. What are six common system resources? What purpose does each resource serve?
3. What are the four system resource domains? What purpose does each domain serve?
4. What purpose does the ~/Library/Containers folder serve? What items are in this folder?
5. What happens when a user double-clicks a font file?
6. How can you identify duplicate fonts?
7. How does System Integrity Protection (SIP) help ensure that macOS Sierra system resources remain secure?

Answers

1. These are the four default top-level folders visible in the Finder:
    - The Applications folder—Apps that local users have access to
    - The Library folder—System resources that local users have access to
    - The System folder—System resources

- The Users folder—Local user home folders

2. These are the six common system resources and the purposes they serve:
   - Extensions—Attach themselves to the system kernel to provide hardware and peripheral driver support
   - Frameworks—Shared code libraries that provide additional software resources for apps and system processes
   - Fonts
   - Preference files—App and system configuration information
   - LaunchAgents and LaunchDaemons—Used by `launchd` to provide services that automatically start when needed at system startup or at user login
   - Logs—Text files that contain error and progress entries from nearly any app or system service
3. These are the four system resource domains and the purpose they serve:
   - User, which contains apps and system resources specific to each user account
   - Local, which contains apps and system resources available to users on a local Mac
   - Network, which is optional and contains apps and system resources available to any Mac that has an automated network share
   - System, which contains apps and system resources that provide basic system functionality
4. The ~/Library/Containers folder contains resources for sandboxed apps. macOS Sierra creates and maintains a separate container folder for each sandboxed app that a user can open. A sandboxed app is more secure because it can access only items inside its container. Only items intended for sharing are in a group containers folder.
5. When a user double-clicks a font file the font file automatically opens a preview of the font in the Font Book app. From here, the user can click the Install Font button to copy the font into ~/Library/Fonts.
6. The Font Book app shows a small dot next to the name of any font that has duplicate resources.
7. SIP prevents users and processes with administrator or root access from modifying core macOS Sierra items. Protected items include the /System, /bin, /sbin, and /usr folders along with core macOS Sierra apps.

Lesson 14—"Use Metadata, Spotlight, and Siri" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What's file system metadata? What are some examples?
2. What are some of the common file flags used by macOS Sierra?
3. What are file system tags? Where can you find tags in the user interface?
4. How does the Spotlight search service use metadata?
5. Where does Spotlight store its metadata index databases and its plug-ins?
6. What are some privacy and security concerns with Spotlight?
7. How do you resolve an issue where a Spotlight search doesn't find the correct items?
8. How can you ensure that Siri doesn't send audio recordings to Apple?

Answers

1. Metadata is information stored outside of a file or folder. It provides additional information about files and folders. Examples include file flags, extended file attributes, and permissions.
2. Common file flags include the locked flag, which locks files from changes, and the hidden flag, which hides the item in the Finder.
3. File system tags are a type of metadata that allow you to quickly assign keywords, or "tags," to any item. A user can customize the tag names and colors.
4. The Spotlight search service creates index databases of file system metadata so that it can perform normally time-intensive searches nearly instantly. File system tags can be found in the Finder sidebar, Spotlight search, and any Open or Save document dialogs.
5. Spotlight metadata index databases are stored at the root of every volume in a /.Spotlight-V100 folder. However, a Legacy FileVault user's database is stored in the user's encrypted home folder. And the Mail app maintains its own database in each user's home folder at ~/Library/Mail/V2/MailData/Envelope Index. Spotlight plug-ins can be located in any of the Library folders in a folder named Spotlight.
6. Though Spotlight indexes file and folder permissions, other users can search the contents of locally attached nonsystem volumes when ownership is ignored on those volumes.
7. Forcing a rebuild of the Spotlight index databases is a common technique to resolve search issues. You can force a rebuild by adding an item to the Spotlight preferences Privacy list and then removing the item. This deletes the current index database and forces the system to build a new one.
8. You can prevent Siri from sending audio to Apple by disabling Siri from Siri preferences.

Lesson 15—"Manage Time Machine" review questions

After you complete this lesson, you should be able to answer the following questions:

1. Which backup destination disks does Time Machine support?
2. How does Time Machine maintain a backup history of the file system?
3. Which types of files are omitted from Time Machine backups?
4. Why is Time Machine inefficient at backing up large databases?
5. Why might a previously backed-up item no longer be available in Time Machine?
6. What are the four ways you can restore data from a Time Machine backup?
7. When you restore from Time Machine, how can you tell which backups are available immediately and which are available only when the backup disk is connected?

Answers

1. Time Machine can back up to any Mac OS Extended volume or network shares hosted from Time Capsule or macOS Server.
2. Time Machine starts with a full copy of the file system to the backup disk. Then it maintains a list of changes to the file system, and every hour copies only the changes to the backup disk. In the backup, it creates a simulation of the full file system using hard links for files that haven't changed.

3. Time Machine ignores temporary files, Spotlight indexes, items in Trash, log files, and anything else that can be considered a cache. Time Machine also ignores files that an app defines as exempt, or files that you define as exempt in Time Machine preferences.
4. Time Machine is inefficient at backing up large databases because it must back up the entire database file every time any change, no matter how small, is made to the database.
5. A previously backed-up item won't be available if your backup volume filled up and Time Machine had to start deleting older items to make room for newer ones.
6. Methods for restoring from a Time Machine backup include navigating through the backup history with Time Machine, restoring a user account through Migration Assistant, restoring an entire system with macOS Recovery, and manually restoring items by using the Finder.
7. In Time Machine Restore, bright tick marks in the time line indicate backups that you can restore immediately. Light tick marks indicate backups that are only available when the backup disk is connected.

Part Five: Applications and Processes

After you complete Part Five, "Applications and Processes," in *macOS Support Essentials 10.12*, you should be able to perform the following tasks:

- Manage and support apps on a Mac that's running macOS Sierra.
- Describe how to lock and unlock files.
- Describe the features and functions of Quick Look.
- State the location of Quick Look plug-ins.
- List the file types supported by Quick Look in a default installation of macOS Sierra.
- List the apps included with macOS Sierra use Quick Look.
- Describe the key features of the App Store app.
- Describe the key requirements for using the App Store app to purchase and install apps.
- Describe the process for signing in and out of the App Store when you're using a valid Apple ID.
- Verify the currently active Apple ID that's being used with the App Store.
- Describe Auto Save.
- Describe Versions.
- Describe the requirements and process for running a Java app on macOS Sierra.
- Describe the purpose and benefit of app sandboxing.
- Compare 32- and 64-bit modes of operations for macOS Sierra apps.
- Compare the traditional installation of apps on macOS Sierra through drag and drop and installation packages.
- Describe the ways you can update apps that were installed using drag and drop or installation packages.
- Compare the ways to remove apps in macOS Sierra through Launchpad, Trash, and uninstallers.
- Describe how to manage documents between iCloud and a compatible apps.

- Describe the dictation feature in macOS Sierra.
- Identify the languages and commands supported by the dictation feature.
- Define protected memory.
- Describe the app environments supported by macOS Sierra.
- Define 64-bit memory addressing.
- On a Mac that's running macOS Sierra, identify processes and apps that are using a significant percentage of RAM or processor time.
- Use Activity Monitor.
- On a Mac that's running macOS Sierra, list installed apps.
- Use System Information.
- Identify three ways to force quit an app.
- Describe how the Finder identifies which app should be used to open a file.
- Describe where app preferences are stored.
- Describe the format of preference files.
- Identify the preference pane that enables Accessibility features in the Finder and other apps.
- Describe how to use VoiceOver.
- Describe the Accessibility features and functions in macOS Sierra.
- Describe how to troubleshoot app environment issues in macOS Sierra.
- On a Mac that's running macOS Sierra, install and remove apps.
- Describe the function, purpose, and benefits of the Resume feature in macOS Sierra as it relates to Auto Save and Versions.
- Describe the tools and methods that are used to control the Resume feature in macOS Sierra.
- Describe the diagnostic reporting and log features supported in the Console app included with macOS Sierra.
- Describe the function, purpose, and benefits of the Gatekeeper feature as it relates to installing apps.
- Compare the three security options supported by Gatekeeper.
- Describe how Dashboard widgets work.
- Describe the security implications of installing Dashboard widgets.

Lesson 16—"Install Applications" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What are the requirements for purchasing apps from the App Store?
2. In the App Store, how can you verify which Apple ID is being used for purchases?
3. How may Apple IDs can be part of a Family Sharing group?

4. What are the four primary app environments supported by macOS Sierra? Which ones require an additional download and installation?
5. What are the advantages of app sandboxing?
6. What are the advantages of code signing?
7. Which items fall under the file quarantine system?
8. Which two security options does Gatekeeper allow? Which Gatekeeper option is the macOS Sierra default?
9. What are the two ways Gatekeeper enables you to install apps?
10. What are three ways you can uninstall apps?

Answers

1. To purchase items from the App Store, you need the following things:
   - OS X 10.6.6 or later
   - An Apple ID
   - An Internet connection
2. In the App Store, you can view the current Apple ID by selecting Store from the menu bar. You can get more details about this Apple ID by choosing View My Account in the same menu.
3. A Family Sharing group can have up to six members.
4. These are the four primary app environments supported by macOS Sierra:
   - Native macOS Sierra apps.
   - UNIX apps, which are primarily accessed through Terminal
   - Java apps, which are cross-platform apps
   - X Window System apps, which run inside the UNIX windowing environment

   macOS Sierra doesn't include the Java app or X Window System runtime. You must download and install them after the initial macOS Sierra installation.
5. Sandboxed apps are allowed access only to specific items. They're otherwise completely cut off from the rest of the system so they can't cause harm. All App Store apps must be sandboxed.
6. Code-signed items include a digital signature that the system can use to verify the authenticity and integrity of the app or process and its resources.
7. Any item downloaded using one of the built-in macOS Sierra apps is marked for quarantine. Third-party apps may not mark downloaded items for quarantine.
8. Gatekeeper allows apps downloaded from:
   - The App Store
   - The App Store and identified developers
9. Traditional installation methods are generally categorized as either a drag-and-drop installation, where the user copies the app to the local system, or as an installation package, where an installer process places the items on the local system.

10. These are the three ways you can uninstall apps:
    - Open Launchpad, hold down the Option key, and click the X button.
    - In the Finder, drag the primary app to Trash and then empty Trash.
    - Use a custom-built uninstaller package.

Lesson 17—"Manage Documents" review questions

After you complete this lesson, you should be able to answer the following questions:

1. In macOS Sierra, what identifies the app type that should open when you double-click a document?
2. How do you engage Quick Look? Which apps support it?
3. What technology enables Quick Look to preview so many file types?
4. What's Auto Save? How can you identify an app that supports Auto Save?
5. How deep is the version history of a file that you share through email?
6. Which apps can manage document locking?
7. Where can you adjust app Auto Save and Resume options?
8. When you upgrade from iCloud to iCloud Drive, what behavior change occurs?
9. Where can you access items saved in iCloud Drive?
10. Where do you save documents in iCloud Drive if you want to access them from an iOS device?
11. If you have iCloud Desktop & Documents enabled on one Mac and you enable it for another Mac, what happens to the user's Desktop & Documents folders?
12. If you disable iCloud Desktop & Documents, what happens to the user's Desktop & Documents folders?

Answers

1. macOS Sierra uses a document filename extension to determine the document type. The Launch Services process maintains a database of installed apps and the document types they can open.
2. Quick Look is engaged by pressing the Space bar when a document is selected. Apps that support Quick Look include the Finder, Time Machine, Mail, and most open-and-save browser dialogs.
3. Quick Look uses plug-ins that give it the capability to preview documents. These plug-ins live in Quick Look folders in any Library folder on macOS Sierra.
4. Auto Save allows compatible macOS Sierra apps to automatically save changes to users' documents. A user just saves a document once, then never has to think about saving changes again. Apps that support Auto Save feature a Duplicate function in the File menu instead of a default Save As function.
5. Documents sent through email or otherwise copied to a shared location don't retain any version history.
6. Any app that supports Auto Save and the Finder can manage document locking.
7. You can deselect "Reopen windows when logging back in" from the logout verification dialog. From General Preferences, you can perform these actions:
    - Deselect "Close windows when quitting an application."

- Select “Ask to keep changes when closing documents,” which turns off Auto Save.

8. When you upgrade an iCloud account to use iCloud Drive, you won’t be able to directly access documents from OS X Yosemite 10.10 or earlier or iOS 8 or earlier. If you’re using OS X Yosemite 10.10 or earlier, you can still access Cloud Drive items from the iCloud website: www.icloud.com.

9. iCloud Drive items are available in the Finder or in any app that uses standard macOS Open or Save dialogs.

10. iOS 8 or later devices can access documents in iCloud Drive if they are saved in specific application folders. For example, Pages for iOS can access Pages documents if they are stored in the Pages folder in iCloud Drive.

11. If you enable iCloud Desktop & Documents on additional Mac computers, the Desktop & Documents content from those Mac computers are moved into subfolders inside the iCloud Desktop & Documents folders. For example, adding an additional Mac named "MyMac" results in Desktop & Documents folders containing "MyMac - Desktop" and "MyMac - Documents."

12. When you disable iCloud Desktop & Documents, the items are moved into a subfolder within iCloud Drive, and the local Desktop and Documents folders are created as new empty folders for the local user. Users must navigate to iCloud Drive and manually copy their files to the new (empty) Desktop & Documents folders.

Lesson 18—"Manage and Troubleshoot Applications” review questions

After you complete this lesson, you should be able to answer the following questions:

1. Why would you want to open an app in 32-bit mode?

2. App extensions in macOS Sierra can add which four capability types?

3. How do you install new app extensions? After they’re installed, how do you manage app extension visibility?

4. How can you identify the apps that are installed on your Mac?

5. In macOS Sierra, what app do you use to examine open apps?

6. Which steps should you take when you troubleshoot app issues?

7. Which three ways can you forcibly quit an app from the graphical interface?

8. What does the diagnostic reporting feature do?

9. Where are app preferences stored?

10. Which file format is often used for preference files? How can you view the content of this file type?

Answers

1. Using the Finder Info window, you can force an app to open in 32-bit mode. This step is necessary for a 64-bit app to support older 32-bit plug-ins or app resources.

2. In macOS Sierra, app extensions allow features from an app to extend into the Finder, the Sharing menu, the Action menu, and the Today view in Notification Center.

3. App extensions are installed automatically because they’re bundled in the app that provides the extension. You can enable or disable installed app extensions from the Extensions preferences.

4. You can use System Information to scan the appropriate app locations and return a list of installed apps.

5. Use Activity Monitor to monitor open processes and apps.

6. General app troubleshooting steps include these:
   - Restarting the app
   - Trying another known working document
   - Trying another user account
   - Checking log files
   - Deleting cache files
   - Replacing preference files
   - Replacing app resources
7. These are the three ways to forcibly quit an app from the graphical interface:
   - From the Force Quit Application dialog accessed from the Apple menu
   - From the Dock app shortcut menu accessed by Control-clicking or right-clicking the app icon
   - From the /Applications/Utilities/Activity Monitor app
8. The diagnostic reporting feature automatically creates a diagnostic report log any time an app crashes or hangs. You can view the diagnostic report immediately. It's reported to Apple through the Internet. You can also view it later in the /Applications/Utilities/Console app.
9. Application preferences are almost always stored in a user's Library folder in the ~/Library/Preferences folder. Newer sandboxed apps must always store their preferences in a ~/Library/Containers/*Bundle ID*/Data/Library/Preferences folder, where *Bundle ID* is the unique bundle identifier for the app.
10. Most app preferences are property lists, which are XML files that have the .plist filename extension. You can view the content of these files using Quick Look, and edit them using the Xcode development app, which you can get from the App Store.

Part Six: Network Configuration

After you complete Part Six, "Network Configuration," in *macOS Support Essentials 10.12*, you should be able to perform the following tasks:

- Discuss Transmission Control Protocol/Internet Protocol (TCP/IP) networking.
- Discuss the purpose and format of Internet Protocol (IP) addresses and subnet masks.
- Describe how the IP uses a MAC address to send messages between computers over a local area network (LAN).
- Describe how the IP transfers messages between computers over a wide area network (WAN), including how IP addresses, subnet masks, and routers work.
- Describe how domain name service (DNS) is used to associate computer host names with IP addresses on a network.
- Define the terms *service*, *interface*, and *protocol*.
- Identify an IPv4 address, IPv6 address, and MAC address.
- Configure and manage a network interface on a Mac that's running macOS Sierra.

- Describe how computers are assigned IP addresses from a DHCP server.
- Describe how macOS Sierra connects to Wi-Fi networks upon startup or wake.
- Describe the criteria by which a Mac with macOS Sierra installed and functional Wi-Fi hardware auto-connects to a Wi-Fi network.
- Describe the secure Wi-Fi networks types that a Mac with macOS Sierra installed and functional Wi-Fi hardware can connect to.
- Describe how macOS Sierra stores and manages credentials for accessing secure Wi-Fi networks.
- Define SSID as it relates to Wi-Fi networks.
- Describe the purpose of SSIDs as it relates to Wi-Fi networks.
- Describe the features and purpose of ad-hoc networking as they relate to Wi-Fi networks on Mac computers.
- Describe how to configure Wi-Fi.
- Describe how to manage network locations.
- Describe how to manage VPN connections.
- List the interfaces and interface protocols supported in a default installation of macOS Sierra.
- Describe how Mac computers acquire and use self-assigned (link- local) TCP/IP addresses on a network.
- Describe the ways to configure a network interface for 802.1X.
- On a Mac that's running macOS Sierra, identify whether a network interface has received an IP address from a DHCP server or is using a link-local address.
- Use the Network Status pane of the Network preference.
- On a Mac that's running macOS Sierra, identify the Ethernet or Airport MAC address.
- Use Network Utility.
- On a Mac that's running macOS Sierra, identify a connection issue for a network interface.
- Use Ping in the Network Utility.
- List four common issues that can interrupt network services.
- On a Mac that's running macOS Sierra, configure and manage multiple networks.
- Describe how network port priority affects network connectivity.
- Given a list of network interface priorities and active interfaces, identify the interface used for network access.

Lesson 19—"Manage Basic Network Settings" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What do the terms "interface,""protocol," and "service" mean in relation to computer networks?
2. What's the purpose of Internet Protocol v4 (IPv4) addresses and subnet masks?
3. How does IPv4 addressing differ from IPv6 addressing?
4. How does the IP use the MAC address to send messages between computers on a local area network (LAN)?

5. How does the IP transfer messages between computers over a wide area network (WAN)?
6. How is the Domain Name Service (DNS) used to facilitate network naming?
7. What's used to identify a Wi-Fi network?
8. Which Wi-Fi authentication protocols are supported by macOS Sierra?
9. How can macOS Sierra automatically connect to a Wi-Fi network?
10. Through which mechanism can a standard user configure Wi-Fi settings?

Answers

1. An interface is any channel through which network data can flow. Hardware network interfaces are defined by physical network connections, and virtual network interfaces are logical network connections that ride on top of hardware network connections. A protocol is a set of rules used to describe a specific type of network communication. Protocols are necessary for separate network devices to communicate properly. Finally, a network service (as it pertains to Network preferences) is the collection of settings that define a network connection.
2. The IP address identifies the location of a network device. IP addresses are the primary identification used by the Internet protocol suite TCP/IP for both LANs and WANs. Subnet masks are used by network devices to identify their local network range and to determine whether outgoing data is destined for a network device on the LAN.
3. Most common IP addresses and subnet masks share the same IPv4 formatting. An IPv4 address is a 32-bit number represented in four groups of three-digit numbers, known as octets, separated by periods. Each octet has a value between 0 and 255. An IPv6 address is a 128-bit number that's presented in eight groups of four-digit hexadecimal numbers separated by colons. This allows for a huge range of addresses, and as a result IPv6 addressing essentially includes subnet information.
4. If a network device needs to send data to another network device on the same LAN, it addresses the outgoing packets based on the destination device's MAC address.
5. A network client uses the subnet mask to determine whether the destination IP address is on the LAN. If the destination IP address isn't on the LAN, it's assumed that the destination address is on another network, and the client sends the data to the IP address of the local network router. The network router then sends the data, through a WAN connection, to another router that it thinks is closer to the destination. This continues across WAN connections from router to router until the data reaches its destination.
6. The DNS is used to translate host names to IP addresses through forward lookups and translate IP addresses to host names through reverse lookups. DNS is architected as a hierarchy of worldwide domain servers. Local DNS servers provide name resolution and possibly host names for local clients. These local DNS servers connect to DNS servers higher in the DNS hierarchy to resolve both unknown host names and host local domain names.
7. A Service Set Identifier, or SSID, is used to identify a Wi-Fi network name and associated configuration.
8. macOS Sierra supports authenticated Wi-Fi by using the following authentication protocols: WEP, WPA/WPA2 Personal, and WPA/WPA2 Enterprise, which includes support for 802.1X authentication.
9. A new Mac can automatically connect only to Wi-Fi networks that have no standard authentication mechanism, known as an "open network." However, a configured Mac can automatically reconnect to authenticated Wi-Fi networks, if the appropriate information was saved to the Keychain system.

10. A standard user can connect to any non-WPA Enterprise Wi-Fi network through the Wi-Fi status menu. Because the system Keychain must be modified for WPA Enterprise connections, only an administrative user can establish these connection types.

Lesson 20—"Manage Advanced Network Settings" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What's a network location? Who can access network locations?
2. Which interfaces and protocols are supported by default in macOS Sierra?
3. How does network service order affect network connectivity?
4. In Network preferences, how can you tell which interface is currently being used for network activities?
5. What's the easiest way to configure VPN settings in macOS Sierra?
6. How is 802.1X configured on Mac computers?

Answers

1. A network location is a saved state of Network preferences that contains all network interface settings. Only administrators can define network locations, but if more than one location exists, all users can switch between the various network locations by using the Apple menu.
2. macOS Sierra supports the following network interfaces and protocols:
   - Ethernet IEEE 802.3 family of hardware network interface standards
   - Wireless (Wi-Fi) IEEE 802.11 family of hardware network interface standards
   - FireWire IEEE 1394 bridged network interface
   - Thunderbolt bridged network interface
   - Bluetooth wireless hardware network interface
   - Cellular networks that use USB adapters or iOS devices with cellular network service (Personal Hotspot)
   - Virtual private network (VPN) virtual network interface through Layer 2 Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec); Cisco's IPSec; and Internet Key Exchange version 2 (IKEv2)
   - Transmission Control Protocol/Internet Protocol (TCP/IP), also known as the Internet protocol suite
   - Dynamic Host Configuration Protocol (DHCP)
   - Domain Name Service (DNS) protocol
   - Network Basic Input/Output System (NetBIOS) and Windows Internet Naming Service (WINS) protocols
   - Authenticated Ethernet through the 802.1X protocol
3. The network service order list is used to determine the primary network service interface if there is more than one active service. All network traffic that isn't better handled through local connection to an active network service interface is sent to the primary network service interface. So in most cases, all WAN traffic, Internet traffic, and DNS resolution is sent through the primary network service interface.

4. In Network preferences, network service interfaces with a green status indicator are being used for network activities. All network traffic that isn't better handled through a local connection is sent to the primary network service interface. The primary network service interface is the topmost active interface in the listing.

5. The easiest way to configure VPN settings is to use a configuration profile containing all the relevant VPN setup information.

6. macOS Sierra uses two configuration methods for 802.1X. The first method is automatic configuration through the selection of a Wi-Fi network that requires WPA/WPA2 Enterprise authentication. The second method is semiautomatic configuration through an 802.1X configuration profile provided by an administrator.

Lesson 21—"Troubleshoot Network Issues" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What are four common issues that can interrupt network services on a Mac computer?

2. How do network devices acquire and use self-assigned TCP/IP addresses?

3. How can you identify the MAC addresses for all the Mac computer's network interfaces?

4. How can you verify basic connectivity to another network host?

5. How can you verify that DNS host name resolution is working?

6. How can you verify that the system can establish a connection to a remote network host?

Answers

1. These four common issues can interrupt network services on a Mac:

   - Ethernet connectivity issues, which can cause the hardware network interface to become inactive or introduce excessive packet errors

   - Wi-Fi connectivity issues caused by the selection of an improper Wi-Fi network or excessive wireless interference

   - DHCP service issues, which prevent proper TCP/IP configuration

   - DNS service issues, which prevent host name resolution

2. If DHCP is specified as the configuration for a TCP/IP connection and no DHCP service is available, the device automatically selects a random IP address in the 169.254.xxx.xxx range. It checks the local network to ensure that no other network device is using the randomly generated IP address before it applies the IP address. In most cases, though, this addressing isn't normal, and it's often indicative of a problem with DHCP services.

3. You can identify all the MAC addresses for the Mac computer's network interfaces from the Info pane in Network Utility.

4. The Ping tab in Network Utility enables you to test basic connectivity to another network host by sending and then waiting for the return of a ping packet.

5. The Lookup tab in Network Utility enables you to test name resolution against the currently configured DNS server.

6. The Traceroute tab in Network Utility enables you to verify the connection hops between your Mac and a remote host.

Part Seven: Network Services

After you complete Part Seven, "Network Services," in *macOS Support Essentials 10.12*, you should be able to perform the following tasks:

- Access network services on a Mac that's running macOS Sierra.
- Identify the network services provided by iCloud on a Mac that's running macOS Sierra.
- Describe how to configure network services for apps such as Safari, Mail, Messages, Contacts, Calendar, and the Finder.
- Describe how to configure sharing services.
- Describe how to set up and use screen sharing.
- On a Mac that's running macOS Sierra, with sharing services configured, a network connection, and a scenario where sharing services aren't working as expected, troubleshoot the configuration and connections to restore the service connection.
- Describe how to mount and unmount network share points.
- View /Network to find file services that are available on a network.
- Use the "Connect to Server" menu option in the Finder to access files from each of the five types of accessible file servers.
- Describe the relationship between client software, client configurations, server software, and server configurations relative to network service access.
- Describe the relationship between a network service and a network port.
- List three troubleshooting techniques for issues involving failure to connect to various network services.
- List the five types of file servers that are accessible by using the "Connect to Server" menu option.
- List service discovery protocols supported by macOS Sierra.
- Describe how macOS Sierra uses dynamic service discovery protocols to access network services.
- Describe how items inside /Network in macOS Sierra are populated and organized.
- Describe common issues that can occur when you connect to file sharing services and you're running macOS Sierra.
- List potential issues with metadata, file forks, and connecting to file servers that don't support AFP 3.1.
- Configure a firewall on a mac that's running macOS Sierra.
- Describe how firewalls work in macOS Sierra.
- Describe the advanced firewall settings in macOS Sierra.

Lesson 22—"Manage Network Services" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What's the relationship between clients and servers as it relates to network service access?
2. What's the relationship between a network service and a network port?

3. What's the primary interface for configuring network service apps?
4. How does macOS Sierra use dynamic network service discovery protocols to access network services?
5. Which two dynamic network service discovery protocols are supported by macOS Sierra?
6. Which five network file services can you connect to from the Finder "Connect to Server" dialog?
7. How are items inside the Finder Network folder populated?
8. In what two ways can you automatically connect a network share?
9. What are three common troubleshooting techniques for issues involving failure to connect to network services?
10. How can you verify that a specific network service is available from a service provider?

Answers

1. Client software is used to access network services that are provided by server software. The connection is established using a common network protocol known by both the client and server software. Thus, the client and server software can be from different sources.
2. Network services are established using a common network protocol. The protocol specifies which TCP or UDP port number is used for communications.
3. Internet Accounts preference is the primary interface in macOS Sierra for configuring built-in network apps.
4. Devices that provide a network service advertise their availability through a dynamic network service discovery protocol. Clients who are looking for services request and receive this information to provide the user with a list of available network service choices.
5. macOS Sierra supports Bonjour and Server Message Block (SMB), including support for the legacy Network Basic Input/Output System (NetBIOS) and Windows Internet Naming Service (WINS) dynamic network service discovery protocols.
6. From the Connect to Server dialog in the Finder, you can connect to these services and systems:
   - Server Message Blocks/Common Internet File System (SMB/CIFS)
   - SMB2/SMB3
   - Apple File Protocol (AFP)
   - Network File System (NFS)
   - Web-based Distributed Authoring and Versioning (WebDAV)
   - File Transfer Protocol (FTP) network file services
7. The Finder populates the Network folder using information provided by the dynamic network services discovery protocols. Computers that provide services appear as resources inside the Network folder, and service discovery zones or workgroups appear as folders. Any currently connected servers also appear in the Network folder.
8. To automatically connect a file share when a user logs in to the system, drag the share from the Finder to the user's login items in Users & Groups preferences. Or you can drag the share to the right side of the user's Dock, and it will automatically connect when the user clicks the share's icon in the Dock.

9. Review Network preferences, review the Network Utility statistics, and attempt to connect to different network services.

10. To verify whether a specific service is available from a service provider, first use the Network Utility Ping tab to verify basic connectivity. Then use the Network Utility Port Scan tab to verify that the specific service port(s) are open. You should always limit the port scan to the specific ports required for the network service you're testing.

Lesson 23—"Manage Host Sharing and Personal Firewall" review questions

After you complete this lesson, you should be able to answer the following questions:

1. Which sharing services can macOS Sierra provide?
2. What's the security risk of enabling client sharing services?
3. Which app can provide on-demand screen sharing even when the Screen Sharing service isn't enabled?
4. In macOS Sierra, what network service or services does Screen Sharing need?
5. What's AirDrop, and how do you know if a specific Mac supports it?
6. Assuming you have a brand-new Mac with macOS Sierra installed, what other devices will appear in the AirDrop browser with the default settings?
7. If other devices with AirDrop enabled don't appear in the AirDrop browser, which two settings on a Mac can you change to potentially make more devices appear?
8. In what primary way does the macOS built-in firewall differ from a traditional network firewall?
9. In macOS Sierra, what are the firewall settings?

Answers

1. The macOS Sierra sharing services include DVD or CD sharing, Screen Sharing, File Sharing, Printer Sharing, Scanner Sharing, Remote Login, Remote Management (ARD), Apple Events, Internet Sharing, and Bluetooth Sharing.
2. If a client sharing service is compromised, an unauthorized user can control your Mac and execute unwanted apps or processes.
3. Messages provides on-demand screen sharing that you can use when the system screen sharing service isn't enabled.
4. In macOS Sierra, Messages screen sharing uses iMessage. Users on both Mac computers must sign in to iCloud.
5. AirDrop provides a quick and easy way to share files locally through Wi-Fi. AirDrop creates a secure peer-to-peer network between local devices. From the Finder Go menu, you can verify that a Mac supports AirDrop.
6. When you open the AirDrop browser on a late-model Mac with macOS Sierra, the browser shows only other late-model Mac computers with OS X Yosemite 10.10 or later, and late-model iOS devices with iOS 7 or later.
7. On a late-model Mac, you'll find two settings at the bottom of the AirDrop browser that control AirDrop discovery. The first setting expands AirDrop discovery from only users in your Contacts to everyone within AirDrop range. The second setting makes AirDrop revert to the previous discovery method, which allows your Mac to discover older Mac computers and Mac computers running previous versions of Mac operating systems.

8. With the firewall built into macOS Sierra, connections are allowed or denied on a per-app basis. This is unlike traditional network firewalls, where access rules are based on network service port numbers.
9. In macOS Sierra, these are the firewall settings:
   - Block all incoming connections.
   - Automatically allow built-in software to receive incoming connections.
   - Automatically allow downloaded signed software to receive incoming connections.
   - Enable stealth mode.

Part Eight: System Management

After you complete Part Eight, "System Management," in *macOS Support Essentials 10.12*, you should be able to perform the following tasks:

- Manage peripheral devices connected to a Mac that's running macOS Sierra.
- Given the System Information utility, identify 64- and 32-bit kernel extensions.
- Describe how to connect Bluetooth devices to a Mac.
- Identify the buses supported by macOS Sierra to connect to and communicate with peripheral devices.
- Compare uses of the buses and their characteristics, such as speed, power requirements, and connector types. Include these buses: Bluetooth, SCSI, ATA, Serial ATA, FireWire, USB PC Card bus, and Thunderbolt.
- Given the System Information utility, identify connected peripherals and the buses that they use.
- Use System Information.
- Define the term "device driver" as it applies to macOS Sierra.
- List three ways a device driver can be implemented in macOS Sierra.
- Configure printing and printer sharing on a Mac.
- Describe how to configure printing on a Mac.
- Describe the role of Postscript Printer Description (PPD) files in macOS printing.
- Discuss the steps that occur during the startup and sleep modes.
- Identify each of the processes that start up in macOS Sierra at system startup, in the order in which they launch.
- Map visual and audible cues to the stages of the macOS Sierra startup sequence.
- Describe the role of BootROM and the Power On Self Test (POST) in macOS Sierra startup.
- Describe the role of the launchd processes during macOS Sierra system initialization.
- Describe the role of startup scripts in the startup sequence of macOS Sierra.
- Describe the role of the login window process in user environment setup in macOS Sierra.
- Compare startup items with login items in macOS Sierra.
- Identify the stages of shutdown in macOS Sierra.

- Identify the stages of logout in macOS Sierra.
- Describe which types of computers and data are supported by the Power Nap feature in macOS Sierra.
- Identify the startup keyboard shortcuts and their functions in macOS Sierra.
- Describe the purpose and features of Verbose mode in macOS Sierra.
- Describe the purpose and features of Single-User mode in macOS Sierra.
- Troubleshoot and resolve issues related to macOS Sierra startup and shutdown.
- Describe the ways you shut down an unresponsive Mac.
- Describe how to identify and resolve kernel loading issues in macOS Sierra.
- Identify the location of files and scripts that are essential to macOS Sierra startup.
- Identify the items that load, and the order in which they load, when you start up in safe mode.
- Identify the keyboard combination to start up a Mac in safe mode.
- Describe how to isolate and then resolve an issue that disappears when a Mac is started up in safe mode.

Lesson 24—"Troubleshoot Peripherals" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What are the four primary peripheral bus technologies supported by Mac computers that are running macOS Sierra?
2. What must occur for a Mac to communicate with a Bluetooth peripheral? Where can you configure this?
3. What's a device driver? Which three primary types of device drivers are there?
4. How does macOS Sierra support third-party devices without needing third-party device drivers?
5. What can you infer about a connected peripheral if it doesn't appear in the System Information app?

Answers

1. These are the four primary peripheral bus technologies supported by macOS Sierra:
    - Universal Serial Bus (USB)
    - FireWire
    - Thunderbolt
    - Bluetooth wireless
2. Bluetooth devices must be paired for communication to occur. Bluetooth preferences in the System Preference app are responsible for pairing a Mac with Bluetooth peripherals. You can quickly open Bluetooth preferences from the Bluetooth status menu.
3. A device driver is software specially designed to facilitate the communication between macOS Sierra and a peripheral. Device drivers can be kernel extensions, framework plug-ins, or standalone apps.
4. macOS Sierra uses built-in generic drivers based on each device class. For example, generic drivers for scanners and printers can be used instead of official third-party drivers.

5. If a connected peripheral doesn't appear in System Information, the issue is probably hardware related. Troubleshoot accordingly.

Lesson 25—"Manage Printers and Scanners" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What does the Common Unix Printing System (CUPS) do?
2. What are PostScript Printer Description (PPD) files responsible for?
3. What's the best source for acquiring printer drivers for macOS Sierra?
4. Under what circumstances can a standard (nonadministrative) user configure a printer?
5. How do you share printers with other users?
6. How can you select a new printer driver for a configured printer?
7. If it appears that all configured printers are having problems, what's a potential quick fix?

Answers

1. Common UNIX Printing System (CUPS) manages printing for macOS Sierra, including local and shared printing.
2. PostScript Printer Description (PPD) files are printer driver files that instruct CUPS on how to communicate with specific printer models.
3. The Apple print drivers are the best source for configuring macOS Sierra printers. One way to acquire printer drivers for macOS Sierra is to let the software update system automatically download and install the appropriate printer drivers. Or you can manually download and install printer drivers from the Apple support website.
4. Assuming the default settings for macOS Sierra, a standard user can only configure directly attached or local network printers from the Print dialog. Also, the appropriate drivers must be installed before the standard user configures the printer.
5. You can enable printer sharing from Print & Scan or Sharing preferences. Windows clients may need additional drivers to access Mac shared printers through the Internet Printing Protocol (IPP).
6. It depends on the printer. From Printing & Scanning preferences, sometimes you can select a new printer driver from the Options & Supplies dialog. In many cases, to select a new printer driver for a configured printer, you must delete and then add the printer again.
7. If your printers are having problems, you can reset the printing system by Control-clicking in the printer list and then choosing "Reset printing system."

Lesson 26—"Troubleshoot Startup and System Issues" review questions

After you complete this lesson, you should be able to answer the following questions:

1. What are the primary system initialization stages in macOS Sierra? What visual and audible cues do these stages provide?
2. What does the firmware do? What's the Power-On Self-Test (POST)?
3. What role does launchd serve during Mac startup?

4. Which items are automatically started by launchd during Mac start up?
5. What are the primary user session stages in macOS Sierra? What visual and audible cues do these stages provide?
6. What's the difference between launch daemons, startup items, launch agents, and login items?
7. What are Safe Sleep and Power Nap?
8. What happens during user logout?
9. What happens during Mac shutdown?
10. Which keyboard shortcut is used to start up in safe mode?
11. Which keyboard shortcut can you temporarily use to choose another startup disk?
12. Which changes are made when macOS Sierra starts up in safe mode?
13. Which items aren't loaded when macOS Sierra starts up in safe mode?
14. How do you resolve an issue that disappears when a Mac successfully starts up in safe mode?

Answers

1. Each primary stage of system startup can be indicated by the following cues:
   - Firmware—A bright flash of the power-on light, followed by a light-gray screen on the primary display
   - Start up—A dark-gray Apple logo on the primary display
   - Kernel—A small, dark-gray spinning gear or spinning Earth icon below the Apple logo
   - System launchd—A white screen on all displays followed by the login screen
2. The firmware initializes the Mac computer's hardware and locates the startup file on a system volume. The POST checks for basic hardware functionality when a Mac powers on.
3. launchd is responsible for starting macOS Sierra processes. It also manages macOS Sierra initialization and starts loginwindow.
4. During macOS Sierra start up, launchd starts these daemons and scripts:
   - /System/ Library/LaunchDaemons
   - /Library/LaunchDaemons
   - /Library/StartupItems (through SystemStarter)
   - /etc/rc.local UNIX script (if it exists)
5. Each primary stage of a user session can be indicated by the following signs:
   - displays the login screen.
   - launchd loads apps like the Finder after user authentication.
   - The user environment is active any time a user logs in to macOS Sierra.
6. The administrator account launchd process launches Launch daemons and startup items during Mac start up. User account launchd processes launch agents and login items during user environment startups.

7. When a Mac battery drains, Safe Sleep saves the macOS Sierra state to permanent storage. Power Nap enables a Mac to automatically wake in low-power mode. This enables the Mac to perform app and macOS Sierra updates.

8. During user logout, the user's loginwindow process performs these actions:

   - Requests that user apps quit.
   - Automatically quits user background processes.
   - Runs logout scripts.
   - Records the logout to the main system.log file.
   - Resets device permissions and preferences to their defaults.
   - Quits the user's loginwindow and launchd processes.

9. When a Mac shuts down, loginwindow logs users out and then tells the kernel to quit the remaining macOS Sierra processes. Then the Mac shuts down.

10. Hold down the Shift key during startup to initiate safe mode.

11. Hold down the Option key during startup to open Startup Manager. This enables you to temporarily choose another startup disk.

12. Startup in safe mode performs the following permanent actions:

    - Attempts to repair the system volume structure
    - Deletes system third-party kernel extension (KEXT) caches
    - Deletes font caches

13. When macOS Sierra performs a startup in safe mode, it doesn't load KEXTs, third-party launch agents, third-party launch daemons, third-party startup items, third-party fonts, any user login items, or any user-specific launch agents.

14. If an issue disappears when a startup in safe mode is successful, remove the third-party startup resource that caused the issue. The best way to isolate the issue is to start up the Mac in Verbose mode and observe where the startup process fails. Hold down command-V to start Verbose mode.