macOS Support Essentials 11

Supporting and Troubleshooting macOS Big Sur Exam Preparation Guide

Contents

Becoming an Apple Certified Support Professional

The Apple Certified Support Professional (ACSP) certification is for the help desk professional, technical coordinator, or power user who manages networks or provides technical support for Mac users. This exam verifies that you understand the key concepts covered in this document and in the macOS Support Essentials 11 book and related materials. If you pass the exam, you earn the ACSP 11 certification. For more information, visit the Training and Certification website.

About the ACSP certification

With the ACSP certification, you differentiate yourself as a skilled professional, gain a competitive edge in an evolving job market, and benefit from the power of the Apple brand.

When you pass the exam, an email notifies you about how you receive your Apple certificate along with instructions on how to order a framed version.

Taking the exam

You can take this exam online through the Pearson OnVUE online proctoring system. You take your exam from your home or office, with an online proctor and webcam. Watch this brief video to learn more about the Pearson OnVUE experience. You need a private space and current, government-issued identification to take the exam.

To take the exam online, do the following:

- Sign in to or create an account in the Apple Certification Records System (ACRS) using your Apple ID. Make sure that your name in your ACRS account matches your name on your government-issued identification.
- Click “Take an Exam” to pay for and schedule your exam.
- At the scheduled time, sign in to ACRS, click “Take an Exam,” and check in with the proctor.

After you complete the exam, Pearson emails your exam score to you.

Preparing for the exam

Complete the following to prepare for the exam:

- Study the Apple Pro Training Series book *macOS Support Essentials 11: Supporting and Troubleshooting macOS Big Sur* by Arek Dreyer and Adam Karneboge. Questions on the exam can come from the material presented in the book's reference and exercise sections or relevant Apple support articles.
- Gain experience with macOS. The best way to build expertise with technology is to use it. Spend some time getting familiar with the technology and practicing the exercises.
- Read this guide and practice by completing the sample tasks and answering the review questions. This guide helps you study and prepare—whether you've learned about macOS Big Sur from the book or on the job.
- Consult some of the many third-party reference, troubleshooting, and online tutorials for users of various levels, from novice to power user.
- Post any questions you have to one of the macOS Support Communities that Apple hosts.

Exam details

- macOS Support Essentials 11 End User Exam (9L0-453)
- This exam costs about $250 USD. Certification exam prices are subject to change and may vary based on currency values. In some countries and regions, additional taxes may apply.
- The exam contains about 100 scored technical questions. You have 150 minutes to complete them.
- A passing score is 72 percent. Scores aren't rounded.
- The exam uses a random pool of multiple-choice and interactive-media questions.
- You may not access any resources or references during the exam.
- For more information about Apple technical exams, visit the Frequently Asked Questions page.

Part One: Installation and Configuration

Lesson 1—Introduction to macOS

Goals

- Describe macOS.
- Describe new macOS Big Sur 11 features.

Review questions

1. Which two Apple-developed and -engineered industry standards that Apple shared with the developer community have contributed to the success of macOS?
2. What is the default file system for all Mac computers running macOS Big Sur?
3. When you upgrade a Mac with a version of macOS earlier than macOS High Sierra (SSD storage) or Catalina (Fusion or hard disk drives), the startup disk is formatted with macOS Extended (HFS+) Journaled. What happens to the startup disk when you upgrade to macOS Big Sur?
4. What are some of the new features of macOS Big Sur?
5. Which privacy and security enhancements does macOS Big Sur improve?
6. Where can you access a guided tour to learn about new macOS Big Sur 11 features and how to navigate your Mac?

Answers

1. Multicast domain name server (DNS) for networking and the Swift programming language for writing software are two industry standards that Apple shared with the developer community that have contributed to the success of macOS.
2. The default file system for all Mac computers is Apple File System (APFS).
3. The startup disk is automatically converted to APFS when you upgrade to macOS Big Sur.
4. macOS Big Sur new features include the following:
    - New design for refined experience
    - New Control Center for macOS
    - Updated Notification Center with notifications and widgets in a single dedicated column
    - Updated Safari with new privacy reports
    - Improved Messages
    - Redesigned Maps
    - New App Store privacy information
    - Time Machine improvements
    - Improved accessibility features
    - Mac Catalyst improvements

5. macOS Big Sur privacy and security enhancements include the following:
    - Signed system volume—macOS Big Sur introduces a cryptographically signed system volume that protects against malicious tampering. It also means that your Mac knows the exact layout of your system volume, allowing it to begin software updates in the background while you work.
    - Faster updates—When macOS Big Sur is installed, software updates begin in the background and complete faster than before—so it's easier than ever to keep your Mac up to date and secure.
    - Privacy information on the App Store—A new section on each app's page on the App Store helps you understand the privacy practices of the app before you download it.
    - Self-reported privacy practices—Developers self-report their app privacy practices on the App Store. See the types of data their app might collect—like usage data, contact information, or location—and whether that data is shared with third parties.
6. You can see a guided tour in the Finder when you click the Help menu. You can choose the following commands:
    - See What's New in macOS
    - New to Mac? Tour the Basics.

Lesson 2—Update, Upgrade, Reinstall macOS

Goals

- Describe the differences between a macOS update, upgrade, and reinstallation.
- Describe the macOS Installer.
- Update macOS.
- Upgrade macOS.
- Reinstall macOS.
- Verify system information.
- Troubleshoot a macOS upgrade or reinstallation.

Review questions

1. What are the differences between a macOS update, upgrade, install, and reinstall?
2. What steps should you take before you upgrade to macOS Big Sur?
3. What are the system requirements to upgrade to macOS Big Sur?
4. How do you check your Mac for software updates?
5. How can you get the macOS installer?
6. How do you reinstall macOS from macOS Recovery?
7. What can you use to troubleshoot macOS installation issues?
8. What does the macOS Installer do with incompatible files and settings during an upgrade?

Answers

1. The following are the differences between a macOS update, upgrade, install, and reinstall:
   - macOS update—Installs an incremental update of macOS but doesn't upgrade it to the next major version.
   - macOS upgrade—Installs the next major standalone version.
   - Install—Installs macOS on a volume that doesn't have macOS—for instance, a volume you erased.
   - Reinstall—Installs the same major version of macOS on a disk that already has macOS installed. This overwrites the existing system files but leaves apps, user home folders, and other files in place.
2. Before you upgrade to macOS Big Sur, you should take these steps:
   a. Verify installation requirements.
   b. Plug MacBook computers into power.
   c. Verify app compatibility.
   d. Back up important content.
   e. Document network settings.
   f. Open Software Update in System Preferences or open the App Store.
3. These are the system requirements to upgrade to macOS Big Sur:
   - OS X Mavericks 10.9 or later
   - 4 GB of memory
   - 35.5 GB of available storage space for an upgrade from macOS Sierra 10.12, or 44.5 GB of available storage space to upgrade from an earlier release
   - Compatible internet service provider
   - Apple ID for some features
4. To check your Mac for software updates, go to the App Store, click Updates, and click the Update buttons for the app updates that you want to install. Or you can click the Update All button to install all of the updates.
5. The macOS Installer is free and available in the App Store.
6. To reinstall macOS from macOS Recovery, start up from macOS Recovery, go to Utilities, select Install macOS, and continue to the license agreement. If it's acceptable, click Agree, select your volume or show all disks, and select your volume and install.
7. To troubleshoot macOS installation issues from the macOS Installer, select the Window menu and then choose Installer Log.
8. The Install macOS Big Sur app moves incompatible files and settings into a Relocated Items folder in the /Users/Shared folder of your startup volume for review after the upgrade is complete.

Lesson 3—Set Up Your Mac

Goals

- Complete initial macOS configuration.
- Adjust common system settings.
- Identify and install a configuration profile.

Review questions

1. Which tool guides you through the initial macOS Big Sur configuration?
2. Which feature can significantly improve Apple ID security on Mac computers that have iCloud enabled?
3. Which key features do you gain by setting up iCloud?
4. Where can you manage iCloud settings after you configure macOS Big Sur?
5. What is a configuration profile? How do you install or remove a configuration profile?
6. Where can you find system information and repair and warranty coverage information for your Mac?

Answers

1. Setup Assistant guides you through the macOS Big Sur configuration process.
2. Two-factor authentication can improve Apple ID security if iCloud is enabled.
3. A key feature of iCloud is providing cloud storage and communication services for apps, including iCloud Drive, Photos, Contacts, Calendars, Reminders, Safari, Siri, Notes, and Find My. iCloud Keychain is also enabled if the Apple ID you entered has two-factor authentication. If the Apple ID you entered belongs to the @mac.com, @me.com, or @icloud.com domain, Mail is also configured.
4. After you set up macOS Big Sur, you can manage iCloud settings by opening System Preferences, selecting Apple ID, then selecting the iCloud pane.
5. A configuration profile is a document with the filename extension .mobileconfig that contains system settings as defined by an administrator. When you open a configuration profile document, macOS Big Sur displays an alert in Notification Center. Click the notification to open the Profiles preferences. Review the information about the profile, then click Install. When you install the profile, macOS configures the settings contained in the profile. You can remove installed profiles through Profiles preferences.
6. You can find system information and repair and warranty coverage information for your Mac in the About This Mac window.

Lesson 4—Use the Command Line

Goals

- Describe when the command-line interface is useful.
- Use man (manual) pages to find more information about commands.
- Manipulate files in the command-line interface.

Review questions

1. What are some advantages of using the command-line interface?
2. What are the four parts of a command string?

3. Which terminal command should you use to perform the following tasks?
    - Print working directory
    - List
    - Change directory
    - Indicate parent directory
    - Indicate current user home folder
    - Create a folder
    - Run the command with root account access
    - Clear the Terminal screen
    - Use the Spotlight index to find a file
4. Which key should you use if you want to automatically complete filenames, pathnames, and command names?
5. What is the default shell interpreter in macOS Big Sur?

Answers

1. The command-line interface provides these advantages:
    - Additional administrative and troubleshooting options
    - More access to the file system
    - A remote login using the Secure Shell (SSH) protocol
    - Any administrator can run commands as the system administrator user or root using sudo
    - The ability to automate repetitive tasks using scripting
    - The ability to remotely administer multiple, even thousands, of Mac computers simultaneously using Apple Remote Desktop
    - Man page documentation that provides an explanation of command usage and references to other related commands
2. The four parts of a command string are as follows:
    - Command name
    - Command options
    - Arguments
    - Extras
3. Use these commands to perform the following tasks:
    - Print working directory: `pwd`
    - List: `ls`
    - Change directory: `cd`
    - Indicate parent directory: `..`
    - Indicate current user home folder: `~`
    - Create a folder: `mkdir`

- Run the command with root account access: `sudo`
- Clear the Terminal screen: `clear` or press Control-L
- Search for files with the Spotlight index: `mdfind`

4. You should use the tab key to automatically complete filenames, pathnames, and command names.
5. The Z shell (zsh) is the default shell in macOS Big Sur, but the bash shell is still available.

Lesson 5—Use macOS Recovery

Goals

- Access macOS Recovery utilities.
- Manage Startup Security Utility.
- Set a firmware password to secure macOS startup for Intel-based Mac computers.
- Manage Secure Boot and external boot options for Intel-based Mac computers with the T2 chip.
- Reinstall macOS from macOS Recovery.
- Create an external macOS Recovery disk.

Review questions

1. Which utilities are available when you start up from macOS Recovery?
2. How do you start up from macOS Recovery on a Mac with Apple silicon?
3. What are the different macOS Recovery options and startup key combinations for Intel-based Mac computers?
4. What are three security policies for a Mac with Apple silicon?
5. Which tool should you use to set a firmware password for your Intel-based Mac?
6. How do you access Startup Security Utility?
7. When are you asked to enter the firmware password when you set a firmware password for an Intel-based Mac?
8. When does your Mac require you to enter an administrator password before you can access macOS Recovery?
9. What are the default Startup Security Utility options for Secure Boot and Allowed Boot Media for an Intel-based Mac with the T2 Security Chip?
10. What does the Secure Boot setting of Full Security provide to an Intel-based Mac with the T2 Security Chip?
11. How can you create an external macOS installation disk?
12. How do you revive or restore a Mac with Apple Silicon?

Answers

1. When you start up from macOS Recovery, you can access the Restore from Time Machine Backup; Install/Reinstall macOS; Get Help Online through Safari; Disk Utility; Startup Disk; Startup Security Utility; and Terminal options and utilities. With Terminal, you can use the `resetpassword` command to reset a password for a local account. Additionally, for Mac computers with Apple silicon, you can use Share Disk to share files with another Mac that's connected by a USB, USB-C, or Thunderbolt cable.

2. If your Mac with Apple silicon is turned on, shut down your Mac. Press and hold the power button until you see “Loading startup options.” A new screen appears that displays the available startup volumes and an Options icon. Use the arrow keys or the mouse or trackpad to select Options, then press Return or click Continue.
3. For Intel-based Mac computers, macOS Recovery installs different versions of macOS depending on the startup key combination you use:
   - Command-R—Installs the macOS that was installed on your Mac without upgrading to the latest version.
   - Option-Command-R—Upgrades to the latest macOS that’s compatible with your Mac.
   - Option-Shift-Command-R—Installs the macOS that came with your Mac or the version closest to it that’s still available.
4. The three security policies for a Mac with Apple silicon are Full Security, Reduced Security, and Permissive Security.
5. You can use Startup Security Utility to set a firmware password for your Intel-based Mac.
6. Startup Security Utility is available only when you start from macOS Recovery. From the Utilities menu, choose Startup Security Utility.
7. You’ll see a prompt for a firmware password if you turn on your Intel-based Mac and press a modifier key or keys to change the way the Mac starts up, such as T, D, Command-S, Command-R, or Option.

   The firmware password prompt appears after you restart or turn on your Intel-based Mac and then immediately press and hold boot modifier keys like Option or Command-R. You release the keys when you see the Apple logo, a spinning globe, or the prompt for a firmware password.
8. If your Mac has FileVault or Activation Lock turned on, you must provide an administrator password before you can access macOS Recovery.
9. By default, for an Intel-based Mac with the Apple T2 Security Chip, Secure Boot is set to Full Security, and Allowed Boot Media is set to “Disallow booting from external or removable media.”
10. For an Intel-based Mac with the Apple T2 Security Chip, the Full Security setting ensures that your Mac will start up only from operating systems that are trusted by Apple and are still being signed by Apple.
11. You can create a macOS Recovery disk that includes the macOS Big Sur tools and installation assets with the createinstallmedia command-line tool in the macOS Installer app.
12. Use Apple Configurator 2 to revive or restore your Mac with Apple Silicon.

Lesson 6—Update macOS

Goals

- Configure automatic macOS software update settings in Software Update preferences.
- Configure automatic App Store software update settings in App Store preferences.
- Automatically update Apple-sourced software.
- Manually update Apple software.

Review questions

1. Which software does the automatic software update method in macOS Big Sur attempt to update?
2. What account credentials do you need to change Software Update preferences?
3. How does macOS tell you that a software update is available from the App Store?
4. How does macOS tell you that a system update is available?
5. Which app should you open to initiate Apple software updates?
6. Which items are always installed, by default, through automatic software updates?
7. What's the best way to learn what software is installed on a Mac?

Answers

1. macOS attempts to update this software:
   - Updates and upgrades to macOS and software bundled with macOS
   - Updates to software you obtained from the App Store
2. You need administrator account credentials to change Software Update preferences.
3. For software updates, macOS displays an Updates Available notification with an App Store icon when updates are available and ready. In addition, a red badge appears next to the App Store icon. The Mac checks for updates daily. Use the keyboard shortcut Command-R to refresh the list of updates.
4. For system updates, macOS displays an Updates Available notification in an alert with a System Update icon. In addition, a red badge appears next to the System Preferences icon. The Mac checks for updates daily. Open the Software Update preferences to refresh the list of available updates.
5. You should open the App Store to initiate software updates. The Software Update preferences in System Preferences manage system software updates.
6. System files and security updates are automatically installed, by default, when they're available.
7. System Information shows all software installed through the App Store or the Installer app, including installations from Apple and third parties.

Part Two: User Accounts

Lesson 7—Manage User Accounts

Goals

- Recognize various user account types and user attributes.
- Create and manage user accounts.
- Restrict access for children with Screen Time settings.
- Adjust login and fast user switching settings.

Review questions

1. What are the types of local user accounts in macOS Big Sur? How are they different?
2. What other types of user accounts can macOS use in addition to local user accounts?
3. Can a standard account user install apps and app updates from the App Store?
4. If FileVault is turned on and you turn on the option “Allow guests to log in to this computer,” what happens when you log in with the guest account?
5. What are user account attributes? How do you view account attributes?
6. How can you limit the amount of time that a user account can access apps?
7. What does fast user switching allow you to do?

Answers

1. The local user accounts in macOS include the following:
    - Administrator—Administrator user accounts are part of the admin group and are allowed full access to all apps, preferences, and shared resource locations.
    - Standard—Standard users are allowed to take advantage of nearly all the resources and features of a Mac, but they generally can’t change preferences that might affect other users.
    - Guest—The default guest account is similar to a standard user, but it doesn’t require a password. When a guest user logs out, the home folder is deleted, including any home folder items that would normally be saved, such as preference files or web browser history.
    - Sharing only—“Sharing only” accounts share files with someone on a different computer, but that user can’t log in to your Mac.
    - System Administrator (root user account)—The System Administrator account has more access to files than administrator user accounts, such as files in user home folders. You can use it to perform tasks that require more privileges than administrator user accounts have. It is turned off by default on macOS.
    - Group—A group account is a list of user accounts that gives you greater control over file and folder access.
2. macOS uses two other user accounts in addition to the local user accounts:
    - Network user accounts—Available to multiple Mac computers and stored on a shared directory server such as Active Directory that centralizes identification, authentication, and authorization information. The home folder for a Network user account is usually stored on a network file server.

- Mobile user account—A network user account that has been synced with the local user database so that you can use a mobile user account even when your Mac can't contact the shared directory server. The home folder for a mobile user account is usually stored on the startup disk.

3. Yes, standard account users can install apps and app updates from the App Store.
4. When FileVault is turned on and you log in with the guest account, your Mac restarts, and Safari is the only app available. When the user with the guest account quits Safari, the guest account home folder is deleted and the Mac restarts.
5. User account attributes are the individual pieces of information that define a user account. Examples include user ID, group, account name, full name, login shell, home directory, universally unique ID (UUID), Apple ID, and aliases. To view user account attributes, open the Users & Groups preferences in System Preferences, Control-click a user account, then choose Advanced Options.
6. You can use Screen Time to manage downtime, app limits, and content and privacy restrictions.
7. Fast user switching lets a Mac switch between user accounts without users logging out or quitting apps.

Lesson 8—Manage User Home Folders

Goals

- Describe user home folders.
- Delete users' accounts and archive their home folder contents.
- Migrate and restore home folders.

Review questions

1. Which folders, by default, are contained in a user's home folder?
2. How do you turn on the Stacks feature to organize your desktop?
3. Why don't you see your Library folder in your home folder by default? What does your Library folder contain?
4. Which folder can you use to share a file with another user on the same computer?
5. What options do you have when you delete a local user account?
6. What does Migration Assistant do?
7. How do you associate a new local user account with a manually migrated or restored user's home folder in macOS?

Answers

1. The default folders in a user's home folder include the Desktop, Documents, Downloads, Movies, Music, Pictures, and Public folders.
2. To turn on Stacks, click the Desktop to make the Finder the active app, then choose Use Stacks from the View menu. You can also Control-click the desktop, then choose Use Stacks.
3. In your home folder, your Library folder is hidden in the Finder by default. Your Library folder includes user-specific preference files, fonts, contacts, keychains, mailboxes, favorites, screen savers, and other app resources.
4. Every user has a Dropbox folder, located in their Public folder, that they can use to transfer files to other users. Other users can't add or make changes to the files in your public folder.

5. You have three options when you delete a local user account:
    - Save the home folder in a disk image.
    - Leave the home folder unchanged.
    - Delete the home folder.
6. Migration Assistant transfers settings, user accounts, and content from a Mac, Windows computer, or Time Machine backup to your Mac.
7. Follow these steps to associate a new local user account with a manually migrated or restored user's home folder:
    a. Copy the restored user's home folder to the /Users folder.
    b. Open System Preferences and select Users & Groups.
    c. Create a new local user account with the same account name as the user's home folder. You'll be asked to associate the new local user account with the restored home folder.

Lesson 9—Manage Security and Privacy

Goals

- Describe password types and use.
- Manage secrets in Keychain.
- Turn on iCloud Keychain and manage it.
- Manage systemwide security and user privacy.
- Approve System Extensions.
- Approve Legacy system extensions.
- Use Find My.
- Secure your Mac with Activation Lock.
- Lock your screen.

Review questions

1. What are the different types of passwords you can use to secure a Mac?
2. What types of items can you store in a keychain?
3. How does Keychain Access help protect your information?
4. Where are keychain files stored?
5. What app should you use to manage keychain settings?
6. How does two-factor authentication provide added security to your Apple ID?
7. Which macOS systemwide and personal settings can you manage in Security & Privacy preferences?
8. Which feature should you use to find a lost Mac?
9. How can you limit the use of Location Services?
10. How can you ensure that audio recordings used for Dictation service remain private?
11. What are the three conditions that must be met before a standard user account can install a legacy system extension on a Mac with Apple silicon?

Answers

1. You can use these different types of passwords to secure a Mac:
   - Local user account password—Used to log in to your Mac
   - Apple ID and password—For iCloud, iTunes Store, and the App Store
   - Keychain passwords—Protects authentication assets in encrypted keychain files
   - Resource passwords—For email, websites, file servers, apps, and encrypted disk images
   - Firmware password—Prevents your Intel-based Mac from starting up from any disk other than your designated startup disk
2. Keychains securely store your resource passwords, certificates, keys, website forms, Safari AutoFill information, and secure text notes.
3. Keychain Access manages encrypted files that are used to securely save your items. These files are impenetrable unless you know the keychain password. If you forget the keychain password, you lose the file contents forever.
4. Keychain files are stored throughout macOS for different users and resources:
   - A user's login keychain is stored in /Users/*username*/Library/Keychain/login.keychain-db.
   - Other local keychains are stored in /Users/*username*/Library/Keychains/*others*.keychain.
   - A user's Local Items or iCloud keychain (depending on if iCloud keychain is turned on) is stored in /Users/*username*/Library/Keychains/*UUID*/.
   - A system keychain with authentication assets that aren't user specific is stored in /Library/Keychains/System.keychain. Examples include Wi-Fi wireless network passwords, 802.1X network passwords, self-signed certificates, and intermediate and root certificate authorities (CAs) that you installed.
   - Most of the items in /System/Library/Keychains/ don't appear by default, with the exception of System Roots, which contains root certificates that Apple provides as part of macOS and are used to identify trusted network services.
   - macOS contains other keychains, but you should leave these files alone unless a trusted source instructs you to access them to resolve an issue.
5. You should use Keychain Access to view and modify most keychain items.
6. With two-factor authentication, your Apple ID account can only be accessed after you approve the sign-in with a device you trust, such as your iPhone, iPad, or Mac.
7. You can manage these macOS systemwide and personal settings in the Security & Privacy preferences:
   - General settings—Provides the option to require a password to wake a Mac from sleep or screen saver mode and to define a delay before this requirement sets in. Also allows you to configure a custom message to show at the login window or when the screen is locked.
   - Advanced settings—Provides the option to require users to automatically log out of accounts after a certain amount of inactivity and to require an administrator password to access systemwide preferences.
   - FileVault settings—Provides the option to enable and configure FileVault.
   - Firewall settings—Provides the option to enable and configure personal network firewall settings.
8. Find My helps you find a lost Mac by allowing you to remotely access the Mac computer's Location Services service.

9. You can use the Privacy pane of Security & Privacy preferences to configure app access to Location Services, Contacts, Calendars, Reminders, and social network services. When a new app requests information that's considered personal, macOS asks you for permission.
10. To ensure that your voice recordings remain private, you can manage your Enhanced Dictation settings manually. The Enhanced Dictation option is enabled by default. When you use Enhanced Dictation, your Mac immediately converts what you say into text without sending your dictated speech to Apple. If you turn Enhanced Dictation off or use Siri, what you say and dictate is recorded and sent to Apple to be converted to text. Apple also tracks other information such as your name, nickname, location, and much of the user data sent from your device.
11. Before a standard user account can install a legacy system extension on a Mac with Apple silicon the Security Policy for that macOS must be configured with Reduced Security, and the "Allow user management of kernel extensions from identified developers" checkbox must be selected. Additionally, the legacy system extension must be notarized.

Lesson 10—Manage Password Changes

Goals

- Change known passwords.
- Reset lost user passwords.

Review questions

1. How can you change your local computer account password?
2. How can you reset another user's account password in macOS Big Sur?
3. How does resetting a user's account password affect that user's login keychain?
4. In what situations can you reset a login password with an Apple ID?
5. In what situation can you reset a login password with a FileVault recovery key?

Answers

1. You can change your local account password from the General pane of Security & Privacy preferences or from Users & Groups preferences. In either case, you select Change Password and, in the input pane, you must enter your old password once followed by the new password twice. Finally, select Change Password.
2. You can reset other user account passwords if you have access to an administrator account on the Mac. To perform the reset from Users & Groups preferences, you must log in as an administrator, select the user account that you want to change, and click the Reset Password button. Then you must enter and verify the new password.
3. If your login password doesn't match your login keychain password, macOS creates a new empty login keychain for you. macOS sets your new login keychain password to match your login password. The previous login keychain is renamed and archived.
4. You can use your Apple ID to reset your login password if you escrowed your FileVault recovery key with your iCloud account or if your account has the "Allow user to reset password using Apple ID" option selected in the Users & Groups preferences.
5. You can use your FileVault recovery key to reset your login password if you selected "Create a recovery key and do not use my iCloud account" when you turned on FileVault and you have the recovery key. To

reset a user's lost account password, you can use the Reset Password assistant available from macOS Recovery with the local user selection option if FileVault and Activation Lock are not turned on.

Part Three: File Systems

Lesson 11—Manage File Systems and Storage

Goals

- Recognize systems that macOS supports.
- Manage disks, partitions, and volumes.
- Troubleshoot and repair partition and volume issues.

Review questions

1. What do you call the process of applying logic to storage in the form of partitions, containers, and volumes?
2. What are two APFS volume roles with macOS Big Sur?
3. What new layer of security does macOS Big Sur use to add cryptographic validation of the APFS System volume?
4. What is the default partition scheme that Mac computers use?
5. Which major volume formats does macOS Big Sur support?
6. What are some of the advantages of APFS?
7. What are the seven ways you can unmount and eject a volume or disk from the Finder?
8. Which two built-in macOS Big Sur apps can you use to gather information about storage devices?
9. What does the Disk Utility First Aid feature do?

Answers

1. Formatting is the process of applying logic to storage in the form of partitions, containers, and volumes.
2. macOS Big Sur uses these two APFS volume roles:
   - APFS System—A read-only volume for the operating system
   - APFS Data—A read-write volume for user data
3. macOS Big Sur introduces the concept of a signed system volume (SSV).
4. GUID Partition Map (GPT) is the default partition scheme that Mac computers use.
5. macOS Big Sur supports these major volume formats:
   - APFS—The macOS Big Sur default.
   - Mac OS Extended—Used with and before macOS High Sierra. Also known as HFS Plus.
   - FAT—A legacy volume format used by Windows PCs.
   - ExFAT—Created specifically for flash storage drives larger than 32 GB.
   - NTFS—Recent versions of Windows use this as their default native volume format. macOS can read but can't write to or start up from NTFS volumes.
6. APFS advantages include making common operations such as copying files and directories instantaneous, helping protect data from power outages and system crashes, and keeping files safe and secure with native encryption.

7. You can use these seven methods to unmount and eject a volume or disk in the Finder:
    - Drag the disk icon to the Trash icon in the Dock.
    - In the Finder sidebar, click the small Eject button next to the volume you want to unmount and eject.
    - Select the disk you want to unmount and eject, go to the menu bar, and choose File > Eject.
    - Select the volume you want to unmount and eject, then choose File > Eject [*diskname*].
    - Select the volume you want to unmount and eject, then use the Command-E keyboard shortcut.
    - Select the volume you want to unmount and eject, Control-click, then choose Eject [*diskname*] from the shortcut menu.
    - Select the disk you want to unmount and eject, click the Action button in the Finder window toolbar (it looks like a gear), and then choose Eject [*diskname*].
8. You can use both Disk Utility and System Information to gather information about storage devices.
9. The Disk Utility First Aid feature verifies and repairs the partition scheme and volume directory structures.

Lesson 12—Manage FileVault

Goals

- Describe how FileVault helps protect data.
- Enable FileVault protection.
- Describe how to regain access to a FileVault-protected Mac when all local user account passwords are lost.

Review questions

1. How does FileVault protect user data?
2. What do Mac computers with Apple silicon and Intel-based Mac computers with the T2 chip use to encrypt data on built-in storage?
3. What do Intel-based Mac computers without the T2 chip use to encrypt data on built-in storage?
4. How can you turn on FileVault if you didn’t do so in Setup Assistant?
5. What are the two ways you can save the FileVault recovery key when you turn on FileVault in Security & Privacy preferences?

Answers

1. FileVault encrypts the APFS Data volume portion of the built-in startup disk.
2. Mac computers with Apple silicon and Intel-based Mac computers with the Apple T2 Security Chip use the built-in hardware-accelerated Advanced Encryption Standard (AES) engine to encrypt data on the built-in storage for your Mac. These Mac computers encrypt data with 256-bit encryption keys that are tied to the chip’s unique identifier. FileVault should be turned on for additional security.
3. Intel-based Mac computers without the T2 chip use XTS-AES-128 encryption with a 256-bit key to help prevent unauthorized access to the information on your startup disk. FileVault performs the encryption at the file-system driver level of macOS.
4. You can turn on FileVault at any time from the Security & Privacy preferences.
5. If you lose a FileVault password, FileVault Recovery offers two ways to recover it:

- Use your Apple ID to unlock the FileVault volume and reset your password. This action generates a random FileVault recovery key and saves it to your iCloud account.
- Record the key that FileVault randomly generates. You must keep the key somewhere safe but not on your encrypted startup volume.

Lesson 13—Manage Permissions and Sharing

Goals

- Describe file ownership and permissions.
- Explore macOS default shared folders.
- Securely manage file and folder access.

Review questions

1. How do you identify the ownership and permissions of a file or folder in the Finder?
2. Which ownership tiers are used with POSIX-style permissions to separately define specific privilege rules for each file and folder?
3. How do access control lists (ACLs) differ from standard UNIX file system permissions?
4. How does the default organization of the file system let users safely share local files and folders?
5. What's unique about the permissions of the /Users/Shared folder?

Answers

1. You can use the Finder Info window to identify an item's ownership and permissions. In the Finder, you can open the Get Info window of each file or folder and find the permissions of each. Each file and folder has owner, group, and everyone permission settings.
2. These ownership tiers are used with POSIX-style permissions to separately define specific privilege rules for each file and folder:
   - Owner—By default, an item owner is the user who created the item or copied it to the Mac.
   - Group—By default, the group permissions for an item are inherited from the folder it was created in.
   - Everyone—This permission defines access for anyone who isn't the owner and isn't part of the item's group.
3. ACLs expand the standard UNIX permissions architecture to allow more file and folder access control. macOS has adopted a style of ACLs similar to what's available on Windows-based NTFS and UNIX file systems.
4. Every home folder contains a Public folder that other users can read and a Dropbox 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 to other users. The Shared folder is also set for all users to share items.
5. The Shared folder lets local users read and write files, but only the owner can delete it from the Shared folder. This folder's "sticky bit" permissions setting prevents other users from deleting files that they don't own.

Part Four: Data Management

Lesson 14—Use Hidden Items, Shortcuts, and File Archives

Goals

- Navigate to hidden files and folders.
- Examine packages and bundles.
- Manage aliases and links.
- Create and open ZIP archives and disk images.

Review questions

1. Why does the Finder hide certain folders at the root of the system volume?
2. Which two methods can you use to hide items in macOS?
3. What are some ways to navigate to hidden folders in macOS?
4. What's the difference between a package and a bundle?
5. What are the four primary file-system shortcut types that macOS uses and how are they used?
6. Why would you use an archive file instead of a disk image? Why would you use a disk image instead of an archive file?
7. What type of file does the Finder create when you select the Archive option?
8. What action on macOS Big Sur is set as the default for expanding ZIP archives?

Answers

1. The Finder hides certain folders—ones that contain resource items for macOS processes—from average users at the root of the system volume because the average user doesn't need access to those items. If you need access to these hidden files and folders, you can use Terminal.
2. You can hide items in macOS by using either of these methods:
   - Use Terminal to add a period to the beginning of a filename.
   - Enable the hidden file flag. (A hidden flag hides the items only in the Finder.)
3. You can navigate to hidden folders in the following ways:
   - Use the Go to Folder option in the Go menu (Shift-Command-G).
   - Hold down the Option key in the Go menu to make the Library option visible.
   - Press Shift-Command-Period in the Finder to display all hidden items.
4. These are the differences between a package and a bundle:
   - A package—Any folder that the Finder presents to the user as if it were a single file.
   - A bundle—A folder with a standardized hierarchical structure that holds executable code and the resources used by that code.

5. The macOS file system uses four primary shortcut types:
    - Aliases are more resilient than other shortcuts. When the original item is replaced or moved, the alias almost never loses the original item.
    - Symbolic links are pointers to the file-system path of the original item.
    - Hard links reference the original item and point to the bits on the physical storage device.
    - Firm links allow navigation between folders that straddle the read-only APFS System volume and the read-write APFS Data volume.
6. To differentiate why you would use a ZIP archive instead of a disk image or a disk image instead of a ZIP archive, follow this rationale:
    - Use Zip archives for small amounts of data. Zip archives are much simpler to create in the Finder and are compatible with most third-party operating systems.
    - Use disk images for larger amounts of data or to archive an entire file system, including files, folders, and associated metadata, into a single file. Disk images are more difficult to create and manage but offer greater flexibility, primarily because you can easily modify and convert them. Unlike ZIP archives that are widely compatible, disk images are mostly limited to Mac computers. Other systems would require third-party software to access Mac disk images.
7. The Finder creates a compressed ZIP archive file when you select the Archive option.
8. By default on macOS Big Sur, double-clicking a ZIP archive file expands the contents of the ZIP archive.

Lesson 15—Manage System Resources

Goals

- Explore and understand the macOS file layout.
- Discover common system files, their location, and their purpose.
- Describe System Integrity Protection.
- Manage font resources.

Review questions

1. What are the four default top-level folders that are visible in the Finder?
2. What are 10 common system resources? What purpose does each resource serve?
3. What are the three supported 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. How does System Integrity Protection help ensure that macOS Big Sur system resources remain secure?
6. Which app should you use to enable, disable, or validate a font or to add a font to the local font library?
7. How can you identify duplicate fonts?

Answers

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

- System—System resources
- Users—Local user home folders

2. These are 10 common system resources and the purposes they serve:
   - Application Support—Ancillary data that an app needs, such as help files or templates, might be in this folder.
   - Containers and Group Containers—These folders contain resources for sandboxed apps.
   - Extensions—Legacy system extensions, previously called kernel extensions (kexts), are found only in the /Library and /System/Library folders. Legacy system extensions are low-level drivers that attach themselves to the kernel, or core, of the operating system. Legacy system extensions provide driver support for hardware, networking, and peripherals.
   - Fonts—Files that describe typefaces used for both screen display and printing. Font management is covered later in this lesson.
   - Frameworks—Shared code libraries that provide additional software resources for apps and system processes.
   - Keychains—Help securely store sensitive information, including passwords, certificates, keys, Safari AutoFill information, and notes.
   - LaunchDaemons and LaunchAgents—Processes that launchd starts. LaunchAgents start up only when a user is logged in, whereas LaunchDaemons start processes that always run in the background.
   - Preference files—App and system configuration information.
   - Logs—Text files that contain error and progress entries from nearly any app or system service.
3. These are the three supported system resource domains and the purposes they serve:
   - User—Contains apps and system resources that are specific to each user account
   - Local—Contains apps and system resources that are available to users on a local Mac
   - System—Contains apps and system resources that provide basic system functionality
4. The ~/Library/Containers folder contains resources for sandboxed apps. macOS Big Sur 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 container folder.
5. System Integrity Protection prevents users and processes with administrator or root access from modifying core macOS Big Sur items. Protected items include the /System, /bin, /sbin, and /usr folders, along with core macOS Big Sur apps.
6. You can use Font Book to enable, disable, or validate a font or to add a font to the local font library.
7. The Font Book app displays a small dot next to the name of any font that has duplicate resources.

Lesson 16—Use Metadata, Siri, and Spotlight

Goals

- Describe how macOS stores and uses file metadata.
- Use metadata such as tags and comments to organize your files.
- Use Siri and Spotlight to search for local and internet resources.

Review questions

1. What is file system metadata? What are some examples?
2. What are some of the common file flags macOS Big Sur uses?
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 should 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 a file or folder that provides additional information about the file or folder. 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 you use to quickly assign keywords, or "tags," to any item. A user can customize the tag names and colors and can create multiple tags for a single file.
4. The Spotlight search service creates index databases of file system metadata so that it can perform normally time-intensive searches almost instantly. You can find file system tags 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 you can write to in a /.Spotlight-V100 folder. For your startup volume, the folder is /private/var/db/Spotlight-V100. And the Mail app maintains its own database in each user's home folder at ~/Library/Mail/V8/MailData/Envelope Index. Spotlight plug-ins can be located in any of the Library folders in a folder named Spotlight.
6. Although 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. If you experience issues with local file searching, you can force Spotlight to rebuild the index databases by managing the Spotlight preferences.
8. You can prevent Siri from sending audio to Apple by disabling Siri in Siri preferences.

Lesson 17—Manage Time Machine

Goals

- Describe Time Machine.
- Configure Time Machine to back up data.
- Restore files from a Time Machine backup.

Review questions

1. What can you back up with Time Machine?
2. Which types of files are omitted from Time Machine backups?
3. Why is Time Machine inefficient at backing up large databases?
4. What happens when you select a blank disk named “Untitled” as a Time Machine backup?
5. Which feature helps Time Machine restore data when your Time Machine backup disk is unavailable?
6. Which three ways can you restore data from a Time Machine backup?

Answers

1. Time Machine backs up all your personal files, including apps, music, photos, email, and documents, to an external storage device.
2. Time Machine saves space by ignoring files that don’t need to be backed up—ones that can be re-created after a restoration. Generally speaking, Time Machine ignores temporary files, Spotlight indexes, items in the Trash, and anything that can be considered a cache. Software developers can also instruct Time Machine to ignore specific app data that doesn’t need to be backed up.
3. 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.
4. If the external storage device doesn’t have any files on it yet Time Machine erases the disk and creates a new APFS (Case-sensitive) volume dedicated to Time Machine backups. Time Machine names the new volume “Backups of [*Computer Name*],” where *Computer Name* is the name of your Mac.
5. Time Machine creates local snapshots on your built-in startup disk to help when your backup disk is unavailable.
6. Methods for restoring from a Time Machine backup include the following:
    - Restore specific items from a Time Machine backup
    - Restore with Migration Assistant
    - Manually restore with the Finder

Part Five: Applications and Processes

Lesson 18—Install Apps

Goals

- Install apps from the App Store.
- Describe app support and identify security issues.
- Install apps using software packages and the drag-and-drop method.

Review questions

1. How can apps you purchased on one Mac be installed on another Mac you use?
2. Which programs allow businesses and educational institutions to acquire multiple licenses for App Store items?
3. How many Apple IDs can be part of a Family Sharing group?
4. From which two sources does macOS allow you to open apps by default?
5. Which security technologies does Mac use to help protect users when they install third-party apps?
6. How do you install apps that aren't downloaded from the App Store?
7. What are three ways you can uninstall apps?

Answers

1. If you use more than one Mac, you can enable automatic downloads of purchased apps on your other Mac.
2. Apple Business Manager and Apple School Manager, allow businesses and educational institutions to acquire multiple licenses for App Store items.
3. A Family Sharing group can have up to six members.
4. macOS lets you open apps from the App Store and trusted developers. However, you can override this protection.
5. Mac uses these technologies to protect users when they install third-party apps:
    - Process security—Security mechanisms, including SIP, prevent access to resources unless specifically allowed. Systemwide privileges are allowed only when needed.
    - App sandboxing—Apps are granted access only to the items they need.
    - Code signing—The system uses code signing to verify the authenticity and integrity of the software.
    - Notarization—This indicates that Apple has performed a security check on the software and didn't find any malicious software.
    - File quarantine—A warning appears when you attempt to open an item downloaded from external sources, such as the internet.
    - Malware detection—The macOS software update automatically updates a maintained list of known malicious software.
6. In addition to the App Store, you can install software using drag-and-drop installations or installation packages.

7. You can uninstall apps in three ways:
    - Uninstall the app using Launchpad.
    - Drag the app to the Trash.
    - Use a custom-built uninstaller package.

Lesson 19—Manage Files

Goals

- Use Launch Services and Quick Look to open files.
- Describe how Launch Services uses the app database.
- Preview files with Quick Look and the Preview pane.
- Work with apps that support Auto Save and Versions.
- Save and open documents saved to iCloud.
- Optimize local storage to reclaim space on the system volume.

Review questions

1. What identifies the app that should open when you double-click a document in macOS?
2. How do you engage Quick Look? Which apps support it?
3. Which technology lets Quick Look preview so many file types?
4. What are the built-in quick actions available in the Finder?
5. What is Auto Save? How can you identify an app that supports Auto Save?
6. How deep is the version history of a file that you share through email?
7. Which apps can manage document locking?
8. Where do you set Auto Save and Resume options? How should you disable Auto Save?
9. If you have iCloud Desktop & Documents enabled on one Mac and you enable it for another Mac, what happens to the user's Desktop and Documents folders?
10. What happens to the user's Desktop and Documents folders if you turn off iCloud Desktop & Documents?
11. What four recommendations does the Storage Management window offer for optimizing storage?

Answers

1. macOS Big Sur uses a document filename extension to determine the document type. The Launch Services process maintains a database of installed apps and the document types that they can open.
2. You engage Quick Look 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 to preview documents. These plug-ins are stored in Quick Look folders in any Library folder on macOS Big Sur.
4. The list of available quick actions depends on the kind of file you select. The Quick Actions window includes these built-in options:

- Rotate an image or movie—Rotate Left is the default command, but you can press and hold the Option key to change it to Rotate Right.
- Mark up a document or image—After you choose Markup, the file opens in a Markup window.Trim a movie or audio file—Choose Trim, then use the yellow handles in the trimming bar. Click Play to test your changes, then click Revert or click Done to save your changes and close the window. After you click Done, you're asked to replace your original file, cancel, or save your changes in a new clip.
- Customize—Choose Customize to open the Extensions preferences in System Preferences.

5. Auto Save lets compatible macOS Big Sur apps automatically save changes to a document. A user saves a document once then never has to think about saving changes again. Apps that support Auto Save feature a Duplicate, Rename, or Move To command in the File menu.
6. Documents sent through email or otherwise copied to a shared location don't retain any version history.
7. Any app that supports Auto Save and the Finder can manage document locking.
8. 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" to disable the Auto Save feature for any app that supports it.
9. If you turn on iCloud Desktop & Documents on additional Mac computers, the Desktop and Documents content from those Mac computers is moved into subfolders inside the iCloud Desktop and Documents folders. For example, adding another Mac named "MyMac" results in Desktop and Documents folders containing "MyMac—Desktop" and "MyMac—Documents."
10. When you turn off 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 and Documents folders.
11. Recommendations for optimizing storage include the following:
    - Store in iCloud—Stores all files, photos, and messages in iCloud and keeps only recent files and optimized photos in local storage.
    - Optimize Storage—Enables the removal of watched movies and TV shows in the TV app.
    - Empty Trash Automatically—Automatically erases items that have been in the Trash for more than 30 days.
    - Reduce Clutter—Displays documents and other content stored on your Mac so that you can sort through and delete what you no longer need.

Lesson 20—Manage and Troubleshoot Apps

Goals

- Describe and support app types.
- Install Rosetta.
- Manage app extensions and widgets in Notification Center.
- Monitor and control processes and apps.
- Explore various app troubleshooting techniques.

Review questions

1. What is a Universal app?
2. What is Rosetta?
3. How do you install Rosetta?
4. What functionality do app extensions add to macOS Big Sur?
5. How do you install new app extensions? How do you manage app extension visibility after they are installed?
6. How can you identify the apps that are installed on your Mac?
7. In macOS Big Sur, what app do you use to examine open apps?
8. How can Activity Monitor help you identify if a Mac has sufficient physical memory for the task?
9. Which steps should you take when you troubleshoot app issues?
10. Which three ways can you forcibly quit an app from the graphical interface?
11. What does the diagnostic reporting feature do?
12. Which file format is often used for preference files? How can you view the content of this file type?
13. Where are app preferences stored?

Answers

1. Developers can compile their apps for both Mac computers with Apple silicon, and Intel-based Mac computers. The resulting app is called a Universal app.
2. Rosetta is a translation process for Mac computers with Apple silicon. With Rosetta, a Mac with Apple silicon can use apps (and other kinds of code like plug-ins, add-ons, and extensions) that were created for Intel-based Mac computers and not updated for Apple silicon.
3. If macOS detects that the code you're trying to run hasn't been updated for Apple silicon, macOS asks you to first install Rosetta. Just click Install in the dialog. You won't need to install Rosetta again.
4. App extensions let apps from different developers interact with each other in such way that one app's features appear that they are built into the other app.
5. App extensions are bundled with the app that offers them, so they install automatically. You can enable or disable installed app extensions from the Extensions preferences.
6. You can use System Information to scan the appropriate app locations and return a list of installed apps.
7. Use Activity Monitor to monitor open processes and apps.

8. Activity Monitor uses the Swap Used and Compressed memory statistics to display the historical memory used since the last startup. A low swap value is acceptable, but a high value indicates that a Mac doesn't have enough real memory to meet the app's demands.
9. Use these general app troubleshooting steps:
    a. Restart the app.
    b. Open another known working document.
    c. Try another app.
    d. Try another user account.
    e. Check diagnostic reports and log files.
    f. Delete cache files.
    g. Replace preference files.
    h. Replace app resources.
10. The three ways to forcibly quit an app from the graphical interface are as follows:
    - From the Force Quit Applications dialog
    - From the Dock
    - From the Activity Monitor app
11. The diagnostic reporting feature automatically creates a diagnostic report log any time an app crashes or doesn’t respond. You can view the diagnostic report immediately or view it later in the /Applications/Utilities/Console app. It's reported to Apple through the internet.
12. 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 Xcode, which you can get from the App Store.
13. 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.

Part Six: Network Configuration

Lesson 21—Manage Basic Network Settings

Goals

- Describe Transmission Control Protocol/Internet Protocol (TCP/IP) networking concepts.
- Configure and monitor network settings.
- Connect to a Wi-Fi network.

Review questions

1. Whats is a media access control (MAC) address?
2. How are Internet Protocol v4 (IPv4) addresses constructed?
3. What's the purpose of IPv4 addresses and subnet masks?
4. What's the default protocol that macOS uses to get an IP address?
5. How does IP transfer messages between computers over a wide area network (WAN)?
6. How is the 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 Big Sur?
9. How can macOS Big Sur automatically connect to a Wi-Fi network?
10. What does macOS Big Sur display when you click the Wi-Fi status menu?

Answers

1. The MAC address is a unique identifier of a physical network interface on a local network.
2. 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.
3. The IP address identifies the location of a network device. The IP suite TCP/IP uses IP addresses as the primary identification for both local area networks (LANs) and wide area networks (WANs). Network devices use subnet masks to identify their local network range and to determine whether outgoing data is destined for a network device on the LAN.
4. macOS uses Dynamic Host Configuration Protocol (DHCP) to automatically acquire preliminary TCP/IP configuration and to assign IPv4 addressing.
5. A network client uses the subnet mask to determine whether the destination IP address is on the LAN. If the destination address isn't local, the client assumes that the destination address is on another network, and it 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 process continues across WAN connections from router to router until the data reaches its destination.
6. The DNS is used to resolve a DNS name to the corresponding IP addresses.
7. A Service Set Identifier (SSID) is used to identify a Wi-Fi network name and associated configuration.

8. macOS Big Sur supports authenticated Wi-Fi by using the following authentication protocols:
   - Wired Equivalent Privacy (WEP)
   - Wi-Fi Protected Access (WPA)/WPA2 Personal
   - WPA/WPA2 Enterprise, which includes support for 802.1X authentication
   - WPA3 Personal/WPA3 Enterprise, which includes support for 802.1X authentication
9. A 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 is saved to the keychain system.
10. When you click the Wi-Fi status menu, macOS Big Sur displays the Wi-Fi network your Mac is currently using (marked by a blue Wi-Fi symbol next to it) as well as any Wi-Fi network in broadcast range that your Mac has previously joined or you have a valid keychain item for. It also displays the option "Other Networks." If you're signed in with an Apple ID, the Wi-Fi status menu also displays instant hotspots in range associated with that Apple ID.

Lesson 22—Manage Advanced Network Settings

Goals

- Describe the macOS network configuration architecture.
- Manage multiple network locations and service interfaces.
- Configure advanced network settings.

Review questions

1. What's a network location? Who can access network locations?
2. Which interfaces and protocols are supported by default in macOS Big Sur?
3. How does network service order affect network connectivity?
4. How can you tell which interface is currently being used for network activities in Network preferences?
5. What's the easiest way to configure virtual private network (VPN) settings in macOS Big Sur?
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 use the Apple menu to switch between the various network locations.
2. macOS Big Sur 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
   - Thunderbolt Bridge network interface
   - Bluetooth wireless hardware network interface
   - Cellular networks that use USB adapters or iOS devices with cellular network service (Personal Hotspot)

- VPN interface through Layer 2 Tunneling Protocol (L2TP) over Internet Protocol Security (IPSec), Cisco's IPSec, and Internet Key Exchange version 2 (IKEv2)
- TCP/IP, also known as the Internet protocol suite
- DHCP
- 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 more than one service is active. All network traffic that isn't better handled through a 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 resolutions are 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. You can manually reorder the network service order by dragging them into the order you prefer. Active services will still have priority over inactive services.
5. The easiest way to configure VPN settings is to use a configuration profile containing all the relevant VPN setup information.
6. macOS Big Sur uses two configuration methods for 802.1X:
   - Automatic configuration through the selection of a Wi-Fi network that requires WPA/WPA2/WPA3/ Enterprise authentication
   - Semiautomatic configuration through an 802.1X configuration profile provided by an administrator

Lesson 23—Troubleshoot Network Issues

Goals

- Identify and resolve network configuration issues.
- Verify network configuration with Network preferences.
- Use Terminal to aid in troubleshooting.

Review questions

1. How can you identify the MAC addresses for all the Mac computer's network interfaces?
2. What's the term for the current data rate of a Wi-Fi connection, and where can you access this information about a specific Wi-Fi connection?
3. How can you verify basic connectivity to another network host?
4. How can you verify that DNS host name resolution is working?
5. How can you verify that the system can establish a connection to a remote network host?

Answers

1. You can identify all the MAC addresses for the Mac computer's network interfaces from the "ether" line in the output of the `ifconfig` command in Terminal.
2. You can view the current data rate, or Tx Rate, of a selected Wi-Fi connection in the Wi-Fi status menu. The Wi-Fi status menu gives you access to important information about your connections and also gives you access to troubleshooting tools like Wireless Diagnostics. You can open the Wi-Fi status menu by pressing and holding the Option key and clicking the Wi-Fi icon in your menu bar.
3. You can use the `ping` command in Terminal to test network connectivity to another network host by sending a ping packet and waiting for its return.
4. You can use the commands `nslookup`, `dig`, `host`, or `dscacheutil` in Terminal to test name resolution against the currently configured DNS server.
5. You can use the `traceroute` command in Terminal to verify the connection hops between your Mac and a remote host.

Part Seven: Network Services

Lesson 24—Manage Network Services

Goals

- Describe how macOS accesses shared network services.
- Configure built-in macOS network apps.
- Browse and access network file services using the Finder.
- Troubleshoot network shared service issues.

Review questions

1. What's the relationship between clients, servers, and 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 Big Sur use dynamic network service discovery protocols to access network services?
5. Which two dynamic network service discovery protocols does macOS Big Sur support?
6. Which five network file services can you connect to from the Finder "Connect to Server" dialog?
7. What is the default file-sharing protocol that macOS uses to connect a Mac that's running Big Sur to another computer?
8. How are items inside the Finder Network folder populated?
9. In what two ways can you automatically connect a network share?
10. How can you verify that a specific network service is available from a service provider?

Answers

1. Client software accesses network services that server software provides. The client and server software use network protocols and standards to communicate with each other.
2. Network services are established using a common network protocol. The protocol specifies which TCP or User Datagram Protocol (UDP) port to use for communications.
3. The Internet Accounts preferences are the primary interface in macOS Big Sur for configuring built-in network apps, such as Mail, Calendars, Notes, Reminders, Contacts, and Messages.
4. Some devices that provide a network service advertise their availability through a dynamic network service discovery protocol. Clients that are looking for services request and receive this information to provide the user with a list of available network service choices.
5. macOS Big Sur supports Bonjour and Server Message Block (SMB), including support for the legacy NetBIOS and WINS dynamic network service discovery protocols. Bonjour is the primary set of dynamic network service discovery protocols that macOS native services and apps use.

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. SMB is the default, preferred file-sharing protocol for macOS Big Sur.
8. The Finder populates the Network folder using information that the dynamic network service discovery protocols provide. 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.
9. 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 the Users & Groups preferences. Alternatively, you can drag the share to the right side of the user's Dock, and it automatically connects when the user clicks the share's icon in the Dock.
10. To verify whether a specific service is available from a service provider, first use the `ping` command in Terminal to verify basic connectivity. Then use `nslookup`, `dig`, `host`, or `dscacheutil` in Terminal to verify DNS resolution. Then use the `nc` command in Terminal to verify that the specific service ports are open. (You should always limit the port scan to the specific ports required for the network service you're testing.)

Lesson 25—Manage Host Sharing and Personal Firewall

Goals

- Examine and turn on host-sharing services built into macOS.
- Examine and turn on content caching services built into macOS.
- Use screen-sharing tools to access other network hosts.
- Use AirDrop to share files.
- Secure shared services by configuring the personal firewall.
- Troubleshoot shared service issues.

Review questions

1. Which sharing services does macOS Big Sur include?
2. What is content caching?
3. Which app can provide on-demand screen sharing even when the Screen Sharing service isn't enabled?
4. Which network service or services does Screen Sharing need in macOS Big Sur?
5. What's AirDrop?
6. What options are available for AirDrop discoverability on macOS Big Sur?
7. What are the firewall settings in macOS Big Sur?

8. How does enabling stealth mode affect the way your Mac communicates with other hosts? How does blocking all incoming connections affect it?

Answers

1. macOS Big Sur includes these sharing services:
   - Screen Sharing
   - File Sharing
   - Media Sharing
   - Printer Sharing
   - Remote Login
   - Remote Management (ARD)
   - Remote Apple Events
   - Bluetooth Sharing
   - Internet Sharing
   - Content Caching
2. Content caching helps reduce internet bandwidth usage and speed up software installation and iCloud content sharing on Mac computers, iOS and iPadOS devices, and Apple TV devices.
3. Messages provides on-demand screen sharing that you can use when the system Screen Sharing service isn't turned on.
4. In macOS Big Sur, 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 within local Wi-Fi and Bluetooth range. AirDrop creates a secure peer-to-peer network between local devices.
6. To change AirDrop discoverability on macOS Big Sur, click "Allow me to be discovered by" at the bottom of the AirDrop interface and choose No One, Contacts Only (only users in your Contacts), or Everyone.
7. In macOS Big Sur, the firewall settings are as follows:
   - 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.
8. When stealth mode is enabled, your Mac doesn't respond to unauthorized network connections, including network diagnostic protocols like ping, traceroute, and port scan. Your Mac still responds to other allowed services, including Bonjour, which announces your Mac computer's presence and prevents your Mac from being hidden on the network. When you block all incoming connections, your Mac won't respond to incoming network connections except for those required for basic network services or established connections, such as those needed to browse the web or check email. This setting prevents shared services or apps hosted on your Mac from working remotely.

Part Eight: System Management

Lesson 26—Troubleshoot Peripherals

Goals

- Manage peripheral connectivity.
- Pair Bluetooth devices with your Mac.
- Troubleshoot peripheral and driver issues.

Review questions

1. What are the three primary peripheral bus technologies supported by Mac computers running macOS Big Sur?
2. What must occur for a Mac to communicate with a Bluetooth peripheral? Where can you configure this pairing?
3. What is a device driver? What are the four primary types of device drivers?
4. How does macOS Big Sur 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. macOS Big Sur supports these three primary peripheral bus technologies:
    - Thunderbolt
    - Universal Serial Bus (USB)
    - Bluetooth wireless
2. To communicate with a Bluetooth peripheral you must pair the Bluetooth device to associate it with your Mac. You can quickly open Bluetooth preferences from the Bluetooth status menu.
3. A device driver is software designed to facilitate communication between macOS Big Sur and a peripheral. These are the four primary types of device drivers:
    - System Extensions
    - Legacy system extensions (also referred to as third-party kernel extensions)
    - Framework plug-ins
    - Standalone apps
4. macOS Big Sur uses built-in generic drivers based on each device class. For example, macOS Big Sur uses generic drivers for scanners and printers instead of third-party drivers.
5. If a connected peripheral doesn't appear in System Information, the issue is probably hardware related. Troubleshoot accordingly.

Lesson 27—Manage Printers and Scanners

Goals

- Describe technologies that enable macOS to print.
- Configure macOS for printers and multifunction devices.
- Manage and troubleshoot print jobs.

Review questions

1. Which Apple technology helps you find printers and print without downloading or installing printer drivers?
2. What does CUPS do?
3. Which two actions might you need to take to find and connect a Windows-based computer to your CUPS-shared print service?
4. Under what circumstances can a standard (non administrator) user configure a printer?
5. How does sleep mode affect users' access to shared print services?
6. How do you create a PDF document?
7. What are the three ways you can access a printer queue app?
8. What's a potential quick fix if it appears that a configured printer has an issue?

Answers

1. AirPrint helps you find printers and print without downloading or installing printer drivers.
2. CUPS manages printing for macOS Big Sur, including local and shared printing.
3. The CUPS-shared print service lets network clients locate your shared printer configurations using Bonjour. However, different versions of Windows might require you to add additional drivers. Network clients can also enter your Mac computer's IP address or DNS host name to access your Mac shared print service.
4. Assuming the default settings for macOS Big Sur, a standard user can configure only directly attached or local network printers from the Print dialog. Also, if a printer doesn't support AirPrint, the appropriate drivers must be installed before the standard user can configure the printer.
5. Users can't access shared print services on a Mac in sleep mode. But you can configure your Mac to not sleep, or to wake from sleep when other users access those resources.
6. You can create a PDF from any Print dialog by clicking the PDF button, then choosing an option in the pop-up menu to save or send the new PDF file.
7. If a printer queue is open, you can click its icon in the Dock. If the printer queue disappears from the Dock before you can click it, you can open the Printers & Scanners preferences, select the queue on the left, and click Open Printer Queue. You can also manually open a printer queue from the Finder by navigating to ~/Library/Printers and double-clicking a printer.
8. You can quickly resolve a printing issue by resetting the printing system by Control-clicking in the printer list and choosing "Reset printing system."

Lesson 28—Troubleshoot Startup and System Issues

Goals

- Describe the macOS startup process.
- Examine the essential files and processes that are required to successfully start up.
- Learn about macOS startup modes.
- Troubleshoot startup and login processes.

Review questions

1. How does a Mac with Apple silicon or an Intel-based Mac with the T2 chip ensure security during macOS Big Sur startup?
2. What are the primary system initialization stages in macOS Big Sur? What visual and audible cues do these stages provide?
3. What does the firmware do? What's the Power-On Self-Test (POST)?
4. What role does launchd serve during Mac startup?
5. What are two locations for launchd to find preference files that control how various processes are configured?
6. What are the primary user session stages in macOS Big Sur? What visual and audible cues do these stages provide?
7. What are the differences between launch daemons, startup items, launch agents, and login items?
8. What are Safe Sleep, Standby, and Power Nap?
9. What happens during user logout?
10. What happens during Mac shutdown?
11. How do you start up a Mac with Apple silicon in safe mode?
12. How do you start up an Intel-based Mac in safe mode?
13. For a Mac with Apple silicon, which keyboard shortcut can you use to temporarily choose another startup disk?
14. For an Intel-based Mac, which keyboard shortcut can you use to temporarily choose another startup disk?
15. What changes are made when macOS Big Sur starts up in safe mode?
16. Which items aren't loaded when macOS Big Sur starts up in safe mode?

Answers

1. A Mac with Apple silicon or an Intel-based Mac with the T2 chip verifies every step of the startup process to ensure that the hardware and software haven't been tampered with.
2. Each primary stage of system startup can be indicated by the following cues:
    - Firmware—Power on. POST. Startup chime.
    - Booter—The booter process starts. The Apple logo appears in the center of the main display.
    - Kernel—Kernel startup. The progress bar appears.
    - System launchd—Starting other items. The Apple logo is replaced with the login window.

3. 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.
4. launchd starts macOS Big Sur processes, manages macOS Big Sur initialization, and starts the loginwindow process.
5. During macOS Big Sur startup, launchd uses preference files for LaunchDaemons in the following locations:
   - /System/Library/LaunchDaemons
   - /Library/LaunchDaemons
6. Each primary stage of a user session can be indicated by the following signs:
   - The login screen appears.
   - launchd loads apps such as the Finder after user authentication.
   - The user environment is active any time a user logs in to macOS Big Sur.
7. The launchd process (with the process identification number of 1) launches all other system processes, including launch daemons and startup items, during Mac startup. When a user logs in, the launchd process running on behalf of the user account processes launch agents and login items.
8. Safe Sleep and Standby are modes the Mac uses to reduce power usage and to safeguard data. When a Mac goes to sleep, it copies the entire contents of system memory to an image file on the system volume. This way, if your Mac stays in sleep mode long enough to completely drain the battery, no data is lost when your Mac has to turn off.
   - Safe Sleep—Your Mac enters this mode if the battery becomes completely drained or if you leave your Mac idle for a long time. To wake your computer, restart your Mac as if it was shut down. All MacBook computers that are compatible with macOS Big Sur support this mode.
   - Standby—Your Intel-based Mac enters this mode as a power-saving standby when it's in sleep mode and completely idle for more than three hours. To wake your Mac, interact with the keyboard, trackpad, or mouse. You don't need to restart your computer.
   - Power Nap—Power Nap is a state that periodically runs updates while your Intel-based Mac is in sleep mode. The type of updated information varies depending on whether your Intel-based Mac is running on battery power or plugged into a power adapter.
9. 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
   - Quits the user's loginwindow and launchd processes
10. When a Mac shuts down, loginwindow logs users out and then tells the kernel to quit the remaining macOS Big Sur processes. Then the Mac shuts down.
11. For a Mac with Apple silicon, turn the Mac off. Then press and hold the power button until startup disks and Options appear. Press and hold the Shift key, then click Continue in Safe Mode.
12. For an Intel-based Mac, press and hold the Shift key during startup to initiate safe mode. Release the Shift key when you see the login window.

13. For a Mac with Apple silicon, turn the Mac off. Then press and hold the power button until startup disks and Options appear. Select your startup disk (with your pointer or with the Left arrow and Right arrow keys), then click Continue or press Return.
14. For an Intel-based Mac, press and hold the Option key during startup to open Startup Manager. Then you can temporarily choose another startup disk.
15. Startup in safe mode performs the following permanent actions:
    - Verifies your startup disk and, if there are issues, attempts to repair the system volume structure
    - Deletes kernel cache and other system cache files
    - Deletes font caches
16. When macOS Big Sur starts up in safe mode, it doesn't load kernel extensions, 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.