DUMPSBOSS.

OS X Support Essentials 10.9

Apple 9L0-415

Version Demo

Total Demo Questions: 8

Total Premium Questions: 136

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Installation and Configuration	18
Topic 2, User Accounts	12
Topic 3, File Systems	19
Topic 4, Data Management	9
Topic 5, Applications and Processes	17
Topic 6, Network Configuration	21
Topic 7, Network Services	6
Topic 8, System Security	19
Topic 9, Peripheral Devices	7
Topic 10, Troubleshooting	8
Total	136

QUESTION NO: 1

Any account password reset process won ' t change any keychain passwords. Therefore, the user ' s keychains won ' t automatically open when the user logs in with her new password. The user will have to manually change her keychain passwords using the Keychain Access utility.

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

B. How does a user that changes his own account password affect his login keychain?

C. How does network service order affect network connectivity?

D. How does the Spotlight search service use metadata?

ANSWER: A

Explanation:

How does resetting a user ' s account password affect that user ' s login keychain? is correct because a login keychain is normally protected using the user's existing account-password-derived credentials. When an administrator or password-reset process changes the account password without knowledge of the previous password, it cannot also unlock and re-encrypt the existing login keychain using the old secret. As a result, after the reset, the user can authenticate to macOS with the new account password but may be prompted for the former keychain password when accessing saved passwords, Wi-Fi credentials, certificates, or other protected keychain items. If the old password is known, the user can use Keychain Access to change the login keychain password so it matches the current account password. If the old password is unavailable, the existing login keychain generally cannot be recovered; creating a new login keychain allows macOS to store new credentials going forward. Apple documents this distinction between resetting a Mac login password and retaining access to the prior login keychain in its Reset your Mac login password guidance. Keychain Access is Apple's supported utility for managing keychains and their passwords; see the Keychain Access User Guide.

QUESTION NO: 2

If an issue disappears when a Safe Boot is successful, you must find and remove the third-party startup resource that caused the issue. The best way to isolate the problem is to start up the Mac in Verbose mode and then observe where the startup process fails. Verbose mode is initiated by holding down Command-V during system startup.

A. Which changes are made when OS X Safe Boots?

B. What backup destination disks does Time Machine support?

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

D. How do you further resolve an issue that disappears when the Mac successfully safe-boots?

ANSWER: D

Explanation:

"How do you further resolve an issue that disappears when the Mac successfully safe-boots?" is the correct choice because the scenario specifically concerns the next troubleshooting steps after a successful Safe Boot. In OS X, Safe Boot starts the system with a restricted set of startup components, prevents many items from opening automatically, loads only required kernel extensions, and performs certain maintenance checks. Therefore, if the symptom does not occur in this mode, the evidence points to software or a startup-related component that is normally loaded during a standard startup rather than to the core operating system alone.

The appropriate follow-up is to isolate the resource that differs between safe and normal startup, such as login items, third-party extensions, startup items, or other added software. An administrator can test these components in a controlled manner, re-enable them incrementally as needed, and remove or update the component that reproduces the issue. Starting in Verbose mode with Command-V can provide additional boot-stage messages that help identify where startup behavior changes. Apple describes Safe Mode's restricted startup behavior and its use in diagnosing startup-related problems in Use safe mode on your Mac. Apple's OS X Mavericks support materials are also available through the Apple Support Manuals archive.

QUESTION NO: 3

How can a user with the short name anna exclude the /Users/anna/Downloads/ folder from Time Machine backups?

A. Open Time Machine, choose Preferences from the Time Machine menu, click the Exclusions tab, click the Add (+) button, navigate to the /Users/anna/Downloads/ folder, and click Submit.

B. Open the Time Machine pane of System Preferences, click Options, and add the /Users/anna/Downloads/ folder to the list of excluded items.

C. Control-click the anna account ' s Downloads folder in the Finder, click the Sharing and Permissions disclosure button, click the Add (+) button, add the Time Machine user to the list of users, and set the Time Machine user ' s access to " No Access. "

D. In Terminal, execute the command sudo defaults write /Library/Preferences/com.apple.TimeMachineexcludedFolders -array-add /Users/anna/Downloads.

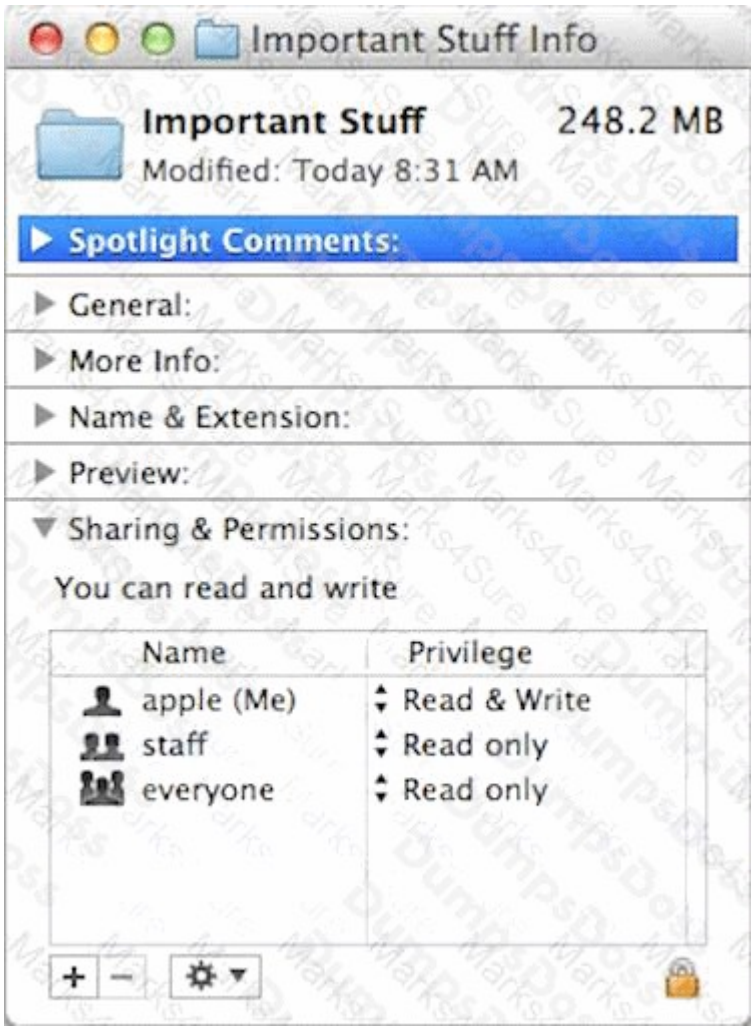
ANSWER: B

Explanation:

Open the Time Machine pane of System Preferences, click Options, and add the /Users/anna/Downloads/ folder to the list of excluded items. Time Machine exclusions are configured through the Time Machine preference pane rather than through Finder permissions or a separate Time Machine user account. In OS X Mavericks, selecting *Options* displays the list of items that Time Machine will omit from subsequent backups. The user can use the add control to browse to the Downloads folder in anna's home directory and add that folder to the exclusion list. Once the settings are saved, Time Machine retains the exclusion as part of its backup configuration and does not include newly backed-up contents of that folder. This is the appropriate method because exclusions are managed at the folder level by Time Machine itself, while the folder remains available locally to anna and continues to use its normal file-system permissions. Apple's Time Machine guidance describes adding files or folders to the excluded-items list in Time Machine settings: Exclude items from Time Machine backups. Additional Time Machine setup and settings information is available from Back up your files with Time Machine.

QUESTION NO: 4

Review the screenshot, and then answer the question below.



If you change the folder privilege for " everyone " to Read & Write, Finder, by default, will change the permissions of items inside the folder to match.

A. True

B. False

ANSWER: B

Explanation:

False is correct because changing the *everyone* privilege in a folder's Finder Get Info window changes the access-control entry on that folder itself; it does not automatically propagate that change to the folder's existing contents. Finder treats a folder and the files and subfolders it contains as separate filesystem objects, each of which can retain its own permissions and access-control list entries.

To intentionally make existing enclosed items use the folder's sharing and permission settings, an administrator must use the explicit *Apply to enclosed items* command from the Action (gear) menu in the Sharing & Permissions section. That separate action is significant because it recursively updates the contents and can replace their current permission settings. Simply selecting *Read & Write* for *everyone* therefore does not perform that recursive update by default.

Apple documents that permissions can be changed for a file, folder, or disk and that changes to enclosed items require the dedicated apply command. See Apple's Change permissions for files, folders, or disks guide and its Apply permissions to enclosed items in a folder guide.

QUESTION NO: 5

In OS X Mountain Lion, which TWO types of file service hosts can you browse in the Network folder? (Select 2)

A. WebDAV

B. FTP

C. DFS

D. SMB

E. AFP

ANSWER: D E

Explanation:

SMB and AFP are the two file-sharing service types whose available hosts OS X Mountain Lion can discover and present when browsing the Finder Network folder. Finder's network browsing relies on local-network service discovery to identify computers advertising compatible file-sharing services. SMB is the standard network file-sharing protocol used for interoperability with Windows systems and other SMB servers. AFP (Apple Filing Protocol) was Apple's native file-sharing protocol in this OS X era and was commonly advertised by Macs and Apple file servers. When a host advertises either service on the local network, Finder can show that host in Network and allow the user to connect to its shared resources, subject to the host's sharing configuration and credentials. Apple's Finder documentation describes using Network to locate available computers and servers, while its file-sharing guidance identifies SMB as a supported Mac file-sharing protocol. AFP is a legacy protocol now retired from current macOS releases, but it remained supported and browseable in Mountain Lion, which is the version specified in this question. See Apple's Connect to a computer or server guide and Set up file sharing on Mac.

QUESTION NO: 6

How does the default organization of the file system allow users to safely share local files and folders?

A. The volume formats supported as system volumes for OS X are Mac OS Extended (Journaled) and Mac OS Extended (Journaled, Encrypted).

B. The keychain system manages encrypted files that are used to securely save your items. By default, every user has login and Local Items keychains that use the same password as his account. Not even other administrative users can access your keychain secrets without knowing the keychain ' s password.

C. 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 to other users. The Shared folder is also set for all users to share items.

D. The Archive option in the Finder creates compressed zip archive files.

ANSWER: C

Explanation:

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 to other users. The Shared folder is also set for all users to share items. This describes the default home-folder layout designed to support local, multiuser sharing while protecting each user's private data. A user can place files in their Public folder when they want other local users to be able to open them. Within Public, the Drop Box supports a safer handoff workflow: other users can deposit files there without being granted general access to the owner's home folder or its private contents. Standard folders such as Documents, Desktop, Library, and Pictures remain protected by default permissions, so another local account cannot browse them merely because it has administrator privileges or access to the same Mac. The Shared folder, located at the top level of the startup volume, provides a common location for material intended to be available to all local users. This organization combines intentional sharing locations with privacy-preserving default ownership and permissions. Apple's current guidance on file-sharing setup is available in Set up file sharing on Mac; its explanation of permission management is in Change permissions for files, folders, or disks on Mac.

QUESTION NO: 7

iCloud is a free service from Apple that provides cloud storage and communication services for applications, including Mail, Contacts, Calendars, Reminders, Notes, Safari, Keychain, Photos and any other applications that support iCloud integration. iCloud also provides Find My Mac technology for help locating a lost or stolen system.

A. What key features do you gain by setting up iCloud?

B. What does OS X use bundles or packages for?

C. What happens during system shutdown?

D. What can you enable to locate a lost Mac system?

ANSWER: A

Explanation:

What key features do you gain by setting up iCloud? is correct because the question text describes the principal benefits available after a user signs in with an Apple Account and enables iCloud services on a Mac. iCloud keeps supported personal information and app data available across devices signed in to the same account. This includes synchronization of information such as email, contacts, calendars, reminders, notes, Safari data, passwords through iCloud Keychain, and photos, subject to the services selected by the user and the OS version in use. It also provides iCloud storage for supported content and applications, allowing documents and data to remain available beyond a single local Mac. An especially important Mac-specific feature is Find My Mac: when enabled in iCloud and supported by the Mac's configuration, it can help a user locate, lock, or erase a missing Mac through the Find My service. Apple's iCloud overview describes iCloud as the service that securely stores and keeps information current across devices, while Apple's Find My documentation explains the capabilities available for locating a Mac. See Apple iCloud and Apple Find My User Guide.

QUESTION NO: 8 - (SIMULATION)

In the screenshot below, click the icon of the OS X Mountain Lion System Preferences pane where you can disable the feature that restores windows when apps are reopened.

ANSWER: See the explanation for the answer

Explanation:

Click the **General** System Preferences pane—the top-left icon under *Personal*.

In **General**, enable **"Close windows when quitting an application"**. This prevents an app's previous windows from being restored when it is reopened.