DUMPSARENA

Mac Integration Basics

Apple 9L0-406

Version Demo

Total Demo Questions: 6

Total Premium Questions: 65

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

Topic Break Down

Topic	No. of Questions
Topic 1, Installation and Configuration	4
Topic 2, User Accounts	7
Topic 3, File Systems	2
Topic 4, Data Management	5
Topic 5, Applications and Processes	4
Topic 6, Network Configuration	4
Topic 7, Network Services	22
Topic 8, Peripherals	3
Topic 9, Security	14
Total	65

QUESTION NO: 1

Which directory-access protocol is commonly used to retrieve user, group, and other directory information from a network directory server?

A. LDAP

B. SMTP

C. SMB

D. VNC

ANSWER: A

Explanation:

LDAP is correct. Lightweight Directory Access Protocol (LDAP) is a standard protocol that clients use to search for and retrieve information stored in a directory service. A Mac can use LDAP directory services to look up account names, group membership, contact information, and other centrally stored identity data. LDAP can be used independently or as part of a broader directory-service implementation.

LDAP does not itself provide file sharing, remote-screen control, or email delivery. Apple documents LDAPv3 as one of the directory-service plug-ins available through Directory Utility. See Apple Directory Utility: Configure LDAP connections and RFC 4511: Lightweight Directory Access Protocol.

QUESTION NO: 2

Which TWO sharing services can be enabled in the Sharing pane of OS X System Preferences to provide remote access to a Mac? (Select two.)

A. Screen Sharing

B. Remote Login

C. Internet Sharing

D. Bluetooth Sharing

E. Content Caching

ANSWER: A B

Explanation:

Screen Sharing and Remote Login are correct. Screen Sharing lets another authorized user view and control the Mac's desktop remotely. Remote Login enables Secure Shell (SSH) access, allowing authorized users to sign in to the Mac from another computer and use command-line tools.

These services are configured separately because they provide different kinds of remote access. Screen Sharing is intended for graphical desktop control, whereas Remote Login provides encrypted command-line access. Apple documents both services in its guidance for configuring sharing on a Mac. See Allow remote login to your Mac and Turn Screen Sharing on or off.

QUESTION NO: 3

Migration Assistant can transfer information to a new Mac from which TWO sources? (Select two.)

A. Another Mac

B. A Time Machine backup

C. An iCloud account

D. A DVD-R disc

E. A printer shared by a Windows computer

ANSWER: A B

Explanation:

Another Mac and a Time Machine backup are correct. Migration Assistant can transfer user accounts, applications, documents, settings, and other eligible data from an existing Mac. It can obtain that information directly from another Mac over a supported connection or from a Time Machine backup that was created from the previous Mac.

Migration Assistant does not use an iCloud account as a complete system-migration source, and it cannot transfer a Mac user environment from an optical disc. Apple documents transferring information from another Mac or from a Time Machine backup during setup or later through Migration Assistant. See Apple Mac User Guide: Transfer your data to your new Mac.

QUESTION NO: 4

You are NOT able to access a Windows file server using your OS X computer's "Connect to Server" command. What is a possible cause of this problem?

A. You need to select the "Windows support" option in the Sharing pane of System Preferences before accessing a Windows file server.

B. You need to prefix the Windows server address with "smb://" in the "Connect to Server" dialog.

C. It is NOT possible to access Windows file servers using the "Connect to Server" command.

D. You need to install Boot Camp on your OS X computer before accessing a Windows file server.

ANSWER: B

Explanation:

You need to prefix the Windows server address with "smb://" in the "Connect to Server" dialog. SMB (Server Message Block) is the standard network file-sharing protocol used by Windows file servers, and Finder uses the server URL's protocol prefix to identify the service it should contact. In Finder, choosing Go > Connect to Server opens a dialog where a server can be entered in URL form, such as `smb://fileserver.example.com` or `smb://192.0.2.10`. Specifying `smb://` is particularly useful when the server name alone is ambiguous, when Finder cannot infer the intended file-sharing protocol, or when documenting a connection path for users. After entering the SMB URL, the user can select Connect and, if required, authenticate with credentials authorized for the Windows server or shared folder. Apple's macOS guidance explicitly identifies SMB as a supported protocol for connecting to shared computers and servers through Finder. The same SMB URL form can also include a share name when appropriate, for example `smb://fileserver.example.com/Shared`. See Apple's documentation for connecting to a computer or server from a Mac and its overview of file sharing on Mac.

QUESTION NO: 5

What term best describes the OS X feature that restricts the system resources, such as files, that an application can access?

A. Execute disable

B. Sandboxing

C. Firewall

D. Library randomization

ANSWER: B

Explanation:

Sandboxing is the OS X security mechanism that limits an application's access to system resources according to a defined set of entitlements. A sandboxed app operates within its own restricted container and does not receive unrestricted access to files, hardware, user data, or system services. Access beyond that container must be explicitly permitted, such as through an entitlement or through a user-mediated action like selecting a file in an Open dialog. This containment model helps protect the system and the user's data if an app is defective or compromised, because the app is limited to only the resources it has been authorized to use. Apple describes App Sandbox as an access-control technology designed to contain damage from a compromised app and to provide access only to resources needed for its intended functionality. Although the question uses the earlier OS X name, the same core App Sandbox model remains part of macOS application security. See Apple's App Sandbox documentation and the Apple Platform Security app security overview.

QUESTION NO: 6 - (HOTSPOT)

HOTSPOT

In the screenshot, click the Icon of the preference pane where you turn on the OS X personal firewall.

Hot Area:



ANSWER:



Explanation:

The correct location is the **Security & Privacy** preference pane. In the System Preferences window shown, this pane is represented by the house-and-lock icon in the Personal row. Opening it provides the security controls for the Mac, including the **Firewall** tab. From that tab, an administrator can unlock the preference pane if necessary and choose **Turn On Firewall** to enable the built-in OS X application firewall.

The OS X personal firewall is host-based: it applies protections directly on the Mac rather than requiring a separate network device. Once enabled, it controls incoming network connections and helps prevent unapproved services or applications from accepting connections. The Firewall options can also be used to manage application access and, in supported OS X versions, enable additional protections such as stealth mode. These controls belong with the Mac's broader privacy, account-security, and system-protection settings, which is why they are housed in Security & Privacy rather than a hardware or network configuration pane.

Apple's security documentation describes the firewall as part of the Mac's security configuration and explains that it can be enabled and managed through the Security & Privacy settings. See Apple's Change Firewall settings on Mac guide for the current equivalent interface and configuration details. The highlighted Security & Privacy icon is therefore exactly the correct hotspot for turning on the OS X personal firewall.