220-1102 Operating Systems Study Guide

General Information - 31% of the CompTIA A+ 1102 questions are devoted to operating systems. Over half (64%) of the questions about operating systems will begin with a scenario.

Microsoft Windows - is the most widely used workstation operating system. It can be installed on a wide variety of compatible hardware from many manufacturers, and it is commonly used in homes, schools, and offices.

Windows 10 Editions - has had **15 total editions released**. Windows 10 was offered as a free upgrade from Windows 7, Windows 8, and Windows 8.1. For the purposes of the exam, only the Windows Home, Pro, Pro for Workstations, and Enterprise editions will be focused on.

Home - Windows 10 **comes preinstalled** on vendor hardware and is referred to as the original equipment manufacturer (OEM) OS. Windows 10 is also available as a retail product but lacks the ability to join a domain, which other Windows editions offer.

Pro - allows the user to join corporate domains, which makes it the **most common** OEM OS and the premier Windows retail edition offering.

Pro for Workstations - supports up to four CPUs and 6 TB of memory as well as remote directory memory access (RDMA) and non-volatile dual inline memory modules (NVDIMM), which makes it **ideal for high-end workstations** that require more than two CPUs and over 2 TB of memory.

Enterprise - offers all the same functionality as Pro and **can be volume licensed** for larger enterprises.

Domain access is the ability of the OS to connect to a domain-joined network of computers that provide centralized authentication, administration, and auditing. It is often found in large corporate networks. Domain access is supported in the Windows Pro, Pro for Workstations, and Enterprise editions.

Workgroup is the default mode for the Windows OS and is a decentralized collection of computers or workstations. Windows Home only has the workgroup capability and not domain access.

Desktop Styles/User Interface - are very similar to previous editions of Windows going back to Windows 95. Users are, however, able to easily customize and personalize the desktop and user interface through the Settings menu. Standard items found on the Windows desktop include the Start menu, the taskbar, and various icons or shortcuts.

Availability of Remote Desktop Protocol (RDP) - is not supported on Windows Home, but it is supported on Windows Pro, Pro for Workstations, and Enterprise.

Random-Access Memory (RAM) Support Limitations - Home supports 128 GB of RAM and two CPUs. Pro supports 2 TB of RAM and two CPUs. Pro for Workstations supports 6 TB of RAM and four CPUs. Enterprise supports 6 TB of RAM and two CPUs.

BitLocker - is an **encryption program** that allows for drive encryption to protect files. BitLocker is **not** available with Home edition but is available with Pro, Pro for Workstations, and Enterprise.

gpedit.msc - The **group policy feature** is available on all of the covered editions except for Home. Group policy allows for all domain-connected computers to have group policies and permissions applied through the domain. Group policies may also be applied locally by using the **gpedit.msc** command.

Upgrade Paths - vary depending on the edition of Windows installed. It is recommended that the OS is upgraded with **like-to-like editions**. Upgrading to an elevated edition requires the use of an activation key. Also, be aware of the recommendations to upgrade to newer versions of the current version before upgrading to 10. For example, before upgrading to 10 from 8, it is recommended that the OS is first upgraded to 8.1.

In-Place Upgrade - is a straight upgrade from the current edition to the latest edition as long as system requirements are met.

Microsoft Command-Line Tools - are command lines specific to Microsoft operating systems. You will need to know the appropriate command-line tool when given a scenario.

Navigation - using the command line allows the user to navigate the file system using predetermined commands.

cd—The **cd** command allows the user to change directories and is shorthand for the **chdir** command.

dir— The **dir** command allows the user to view a listing of files and folders/subdirectories in a directory.

md—The **md** command allows the user to make a directory and is shorthand for the **mkdir** command.

rmdir— The **rmdir** command allows the user to delete directories. The **rd** command is shorthand for this.

Drive Navigation Inputs - The **cd** command allows for navigation within the current drive. To navigate to another drive, you may use the drive letter followed by a semicolon command.

- **C**— Changes to C drive
- **D**— Changes to D drive
- **x**— Changes to X drive

Command-Line Tools - can also be used for numerous other functions, such as testing or tracing network connectivity or paths. You should be familiar with common command-line tools.

ipconfig—is used to display basic connectivity information, such as the IP address, subnet mask, and default gateway. This command is highly useful in diagnosing network issues.

ping—is used to verify network connectivity by sending an Internet Control Message Protocol (ICMP) packet to a specified address, such as the default gateway.

hostname—is used to pull up the identity of the computer the Command Prompt is open on.

netstat—is used to display all the listening and established connections on the host network.

nslookup—is used to verify DNS addresses. This command can be used for inline query or interactively.

chkdsk—is used to view information about the hard disk, including the creation and viewing of reports, as well as to correct file system problems and disk errors.

net user—is a subcommand used to list all local accounts on the host system.

net use—is used to map drive letters to network shares.

tracert—is used to show the path a packet takes on a network to arrive at a specified destination.

format—is used to remove data from disks and prepare disks for new use.

xcopy—is used to copy folders and files.

copy—is used to copy specified files.

robocopy—is used to copy files while keeping permissions intact.

gpupdate—is used to update group policies.

gpresult—is used to view the report/values of the Resultant Set of Policy (RSoP) for a remote user and the users' computer.

shutdown—can be used for scheduling a complete shutdown or a restart remotely or locally.

sfc—System File Checker is a utility command that verifies and checks the version of the file system.

[command name]/?—The **/?** command is used to provide help for a specified command.

 diskpart - is a tool for managing disks, partitions, and volumes.

pathping—is a mixture of the **tracert** and **ping** commands.

winver—is used to display a GUI dialog box.

Microsoft Windows 10 Operating System (OS) - you must be able to use common features and tools offered by the Windows 10 OS. Questions pertaining to these features will be scenario based.

Task Manager - is a utility that displays and manages running applications and services, logged-in users, and system performance.

Services - tab shows you the name of running services along with identification information, such as its description, group, and status.

Startup - tab shows what services have been set to begin upon startup and their associated identifying information.

Performance - tab shows how the CPU, Memory, Disk I/O, and network resources are utilized. It can be very helpful in identifying a bottleneck in a slow-running computer.

Processes - tab lists the currently running processes and resource consumption.

Users - tab shows currently logged-in users, their status, and applications run by these users.

Microsoft Management Console (MMC) Snap-In - is a GUI for running administrative and configuration tools.

Event Viewer (**eventvwr.msc**)— is used to view application error logs, system errors, and security audit records.

Disk Management (**diskmgmt.msc**)— is used to view disk information on the physical disk and the formatted file systems it contains.

Task Scheduler (**taskschd.msc**)— allows you to configure automated tasks that will run on a schedule at specified times.

Device Manager (**devmgmt.msc**)— allows you to view the status of devices, view the properties, and modify the configuration parameters.

Certificate Manager (**certmgr.msc**)— is used to manage and view the certificates used by the OS and web browser.

Local Users and Groups (**lusrmgr.msc**)—As a system administrator, you need to know how to create and delete users and maintain their accounts, as well as how to establish secure passwords.

Performance Monitor (**perfmon.msc**)— displays in real time how the computer uses memory, disk, CPU, and the network, to help diagnose performance issues.

Group Policy Editor (**gpedit.msc**)— is used to edit the local group policy for the OS.

Additional Tools - MMC offers these additional tools beyond the original monitoring and configuration.

System Information (**msinfo32.exe**)— displays advanced hardware and driver information.

Resource Monitor (**resmon.exe**)— shows how resources are being utilized by the CPU, memory, disk, and network.

System Configuration (**msconfig.exe**)— can be run by the **msconfig** command. It allows you to change how Windows boots and what programs start with Windows.

Disk Cleanup (**cleanmgr.exe**)— frees up space while not affecting the integrity of the files.

Disk Defragment (**dfrgui.exe**)— relocates pieces of large files to continuous space on a disk for optimized performance.

Registry Editor (**regedit.exe**)— allows the user to view and change the Windows registry. The registry contains some operating system and application settings that may need to be changed in advanced troubleshooting.

Microsoft Windows 10 Control Panel Utility - includes tools and utilities to view, change, and troubleshoot system settings. Questions in this section will begin with a scenario.

Internet Options - is a utility to manage network settings beyond basic IP connectivity. The settings are separated into multiple tabs.

Devices and Printers - The screen lists printers, scanners, cameras, monitors, and other connected peripheral devices; the settings of these devices can also be accessed.

Programs and Features - is used to view and uninstall desktop applications installed on the OS.

Network and Sharing Center - configure network adapters, create new network and dial-up connections, and configure network file and printer sharing.

System - is the Control Panel utility that shows the hardware overview.

Windows Defender Firewall - protects the computer by controlling what applications can access the network from this computer and also how this computer can be accessed over the network.

Mail - emails can be configured, including Microsoft Outlook. Additional data files, RSS feeds, internet calendars, address books, and SharePoint lists can also be configured here.

Sound - screen is where you can manage devices to play and record sounds and configure sounds that the operating system produces for startup, shutdown, alerts, and prompts.

User Accounts - You can add, manage, and remove local users and their roles for the computer in User Accounts. Each user will have their own profile with different settings and user folders.

Device Manager - lists all hardware connected to the computer and provides management for drivers of the devices.

Indexing Options - systematically indexes files, including Office documents, PDFs, text files, etc.

Administrative Tools - is a shortcut to tools used in the administration of the OS.

File Explorer Options - allows you to change how files are shown and searched.

Show Hidden Files - Hidden is a file flag that signifies that users don't usually need to see certain files, like system and configuration files. Windows settings can be changed to show these files if they need to be accessed.

Hide Extensions - In Windows files have extensions at the end of the file name, after a period (e.g., .txt, .docx, .exe). To make the file names cleaner and prevent users from making accidental changes to the extensions, these are usually hidden. This can be changed with this setting.

General Options - tab of the **File Options** utility allows you to change the general behavior of the file browsing interface.

View Options - tab allows you to change appearance options, including showing hidden files and file extensions.

Power Options - You can choose what pressing the power button on the computer should do and configure the monitor and computer power to be reduced after a specified period of inactivity.

Hibernate - is a mode that saves the current state of the computer and shuts it down. When started again, it restores to the same state, but without consuming power in the meantime.

Power Plans - There are three that can be configured and selected depending on the current need: Power Saver, Balanced, and High Performance.

Sleep/Suspend - mode doesn't shut down the computer like Hibernation does, but instead significantly reduces the power to the components for a quick restart where you left it.

Standby - The term *Standby* is sometimes used interchangeably with *Sleep* but is not used in the current Windows versions.

Choose What Closing the Lid Does - This option is only available on devices that contain a lid closure sensor.

Turn on Fast Startup - function places the system into hibernation during shutdown so that the system can boot more quickly.

Universal Serial Bus (USB) Selective Suspend - This function allows the administrator to choose to suspend power to a device connected to a specified USB port.

Ease of Access - allows for a Windows OS to be configured for motor- and sensory-impaired users.

Windows Settings - is designed to make configuring and personalizing the Windows OS more convenient for end users. Questions on these topics will begin with a scenario.

Time and Language - Changes related to date, time, and language settings can be configured here.

Update and Security - Settings related to the configuration of updates and security can be accessed here.

Personalization - applet can be used to change the display settings of the OS, including backgrounds, colors, fonts, etc.

Apps - section allows you to change the source of apps as well as uninstall apps.

Privacy - allows you to configure privacy settings on the OS.

System - applet offers the option to configure OS settings, including monitor configurations, the display settings, resolution, and scale settings, among others.

Devices - applet, you are able to view, configure, and control connected devices.

Network and Internet - Here, you can configure network adapters, create new network and dial-up connections, and configure network file and printer sharing.

Gaming - applet provides integration between the XBox platform and the computer through the XBox game bar.

Accounts - section is used to manage and configure user accounts and other accounts on the OS.
Microsoft Windows Networking Features - able to configure networking features on a client/desktop. This will be presented as a scenario-based question.
Workgroup vs. Domain Setup - There are three primary networking models in the Windows OS: the homegroup, the workgroup, and the domain. Workgroup allows the OS to be both a server and a client and is primarily used in small office/home office (SOHO) setups. With the domain networking model, the client must be joined to the domain.
Shared Resources - Windows allows sharing of files and folders over the network, allowing a shared space for network users. For convenience, **network shares** can be mapped to a drive letter. For the users and applications, the network share appears like a local disk. Other resources, such as hardware-based resources, can also be shared among the networking group.
Administrative shares are created automatically to allow remote administrators to configure the computer. These shares are not shown and are not accessible to non-administrative users.
Printers - You can use the **printer sharing** functionality to allow printing from other computers to the printer connected locally. To print using a shared printer on a remote computer, it needs to be **mapped** first, installing the drivers for the printer.
File Servers - may also be shared among the networking group.
Mapped Drives - allows for network shares to be connected to a specified drive letter for ease of access among the networking group.
Local OS Firewall Settings - Windows comes with configurable firewall rules to allow or block certain applications or network ports and control security.
Application Restrictions and Exceptions - When installing a new application that needs access to the network, Windows may ask if it should be allowed and add an exception to the firewall. You may also apply application restrictions through the firewall.
Configuration - Windows Firewall can be manually configured to allow or deny applications and network ports. It can also be switched off completely for the type of network. This effectively allows all network traffic and has to be used extremely carefully to avoid exposing the computer to potential network threats and unauthorized access.
Client Network Configuration - The client will automatically connect and configure to the connected router or server if the router supports DHCP with an IP address, subnet mask, default gateway, and the DNS server. These configurations may also be configured manually.
Internet Protocol (IP) Addressing Scheme –can be dynamically acquired from a DHCP server on the network, or configured manually. The IP address needs to be in the same subnet with other hosts and the gateway but be unique.
Domain Name System (DNS) Settings - DNS are servers that resolve names (e.g., microsoft.com) to an IP address that the computer can communicate with. More than one DNS server can be configured for reliability.
Subnet Mask - determines what hosts are on the same network as the local computer. It needs to match all the computers and network devices on the local network.
Gateway - A default gateway is a router that can forward the network traffic from the local network to other remote networks. At least one of its interfaces has to be on the same local network as the computer.
Static vs. Dynamic - A **static IP address** is a specific IP address that is assigned to a computer on the network. A static IP address will remain the same until manually changed. A **dynamic IP address** changes each time the computer connects to the network based on currently available IP addresses.
Establish Network Connections - There are multiple ways to connect a Windows computer to a local or remote network.

Virtual Private Network (VPN) - uses another underlying network, usually the internet. It allows secure access to a remote location over public infrastructure.

Wired - connections usually come in a form of **ethernet** to the computers. It requires cabling to every computer and may require other network devices like switches and routers.

Wireless - network connections use Wi-Fi technology to connect. Because it is not physically restricted in the area, the network will usually have another layer of security in the form of a password or **more complex authentication**. Once connected, the functionality is very similar to a wired connection.

Wireless Wide Area Network (WWAN) - Similar to mobile phones that can access the internet from anywhere, a WWAN is a cellular network that can be used to connect to the network. Some tablets and laptops come with built-in cellular hardware.

Proxy Settings - is a form of a gateway. A common example is a web proxy that is set up to filter access to the internet from a local network to improve security.

Public Network vs. Private Network - public is one that is accessible to everyone within range while a private is protected and limited to those who have proper authentication.

File Explorer Navigation – Network Paths - is achieved through pre-configured network paths. The Universal Naming Convention (UNC) path is the standard way to navigate to the server and fileshare in the Windows OS.

Metered Connections and Limitations - Metered connections are **based on usage** and come with limitations to keep usage down. When using a metered connection, updates, whether they be for the OS, application, or system security, will not download and install.

Application Installation and Configuration - There are multiple methods for installing new applications and software. Some things need to be taken into consideration for the successful installation and use of applications. You must be able to apply installation and configuration concepts. Questions on these concepts will be scenario based.

System Requirements for Applications - The system needs to have **enough resources** to allow installation of new applications. The specific requirements depend on the application and can be usually found in the supporting documentation for the application.

32-bit vs. 64-bit Dependent Application Requirements - Application requirements must **match the architecture of the CPU and OS** for either 32-bit or 64-bit architectures. However, if the architecture supports 64 bits, it will be able to properly run 32-bit applications.

A **dedicated graphics card** is a separate hardware device for graphics and display, while an **integrated graphics card** is pre-built into the motherboard of the computer. When installing applications, the graphics card, both integrated and dedicated, must be compatible with the requirements of the application and OS.

Video Random-Access Memory (VRAM) Requirements - are for graphic-intensive applications, such as **gaming**. For the application to function properly, the VRAM requirements of the program must be met by the device.

RAM Requirements - To run an application, it needs to be loaded into memory. There should be sufficient RAM available or the application will run slowly, slowing down other processes too, or it will not be able to run at all.

Central Processing Unit (CPU) Requirements - of an application are typically given in gigahertz (GHz) and show the amount of processing power the application requires. These requirements need to be met or exceeded for proper functionality.

External Hardware Tokens - are physical devices that can be connected to the device for increased security. The requirements for the hardware token must be met or exceeded by the host computer.

Storage Requirements - Before running an application, its files need to be stored on the computer's disk. There should be enough free disk space to copy and use the program's files.

OS Requirements for Applications - An application expects to work with a specific operating system. The installation of the software should be compatible with the OS. Refer to the application's documentation to find out what operating systems are supported.

Application to OS Compatibility - The application needs to be compatible with the host OS. Many applications come in multiple OS-compatible versions so make sure you are installing a Windows-compatible application on a Windows OS.

32-bit vs. 64-bit OS - Applications that require a 64-bit OS will not be compatible with a 32-bit OS, but a 32-bit application will be compatible with a 64-bit OS.

Distribution Methods - There are multiple ways to distribute software installation files.

Physical Media vs. Downloadable - The only way to install new software on a computer that is not connected to any network is to have the application on a **portable media**, **CD**, or **USB disk**. This can also be useful for large applications or slow networks. The installation files can be run directly from the media or copied to the hard disk first and then installed.

On computers connected to a network, applications can be installed over the network and not from portable media or local files. If the application is acquired from the internet, the files are first copied to the local disk, then installed. Operating systems also include forms of application stores and repositories that make it easy to find and install new software.

ISO Mountable - application installation is one in which the application ISO is downloaded from the vendor and installed directly onto the host machine and acts as a virtual optical drive.

Other Considerations for New Applications - Besides hardware and compatibility requirements, there are other considerations before a new application is installed.

Impact on Device - Installing a new application may allow it access to other files on the computer. Some software can be **malicious** and may need to be researched before installation. Even if there are no ill intentions, some functions of the software may not be suitable for protected corporate environments with sensitive information.

Impact on Network - If a new application is installed on a computer that is connected to the network, it will effectively get access to the network and may **compromise the security** of other computers on the same network.

Impact on Operation - New applications can affect the operations of the OS and its information system. These effects can be negative and may **compromise the efficiency** of the computer.

Impact on Business - Before installing new applications on a computer connected to a business network, the effects of the application on the functioning of the business should be considered and evaluated for **potentially harmful effects** to the business.

Common OS Types

Workstation OSs - Workstation operating systems are designed to be used on a desktop or a laptop computer by one person at a time. These operating systems provide a convenient **graphical user interface (GUI)** and access to files and applications on the computer.

Windows - is the **most widely used** workstation operating system. It can be installed on a wide variety of compatible hardware from many manufacturers, and it is commonly used in homes, schools, and offices.

Linux - is a **kernel**, the core of the operating system. Interfaces and applications can be added to the kernel. These pre-configured combinations are known as **distributions**. This flexibility allows users to create various versions of systems for different cases. A distribution can have an extensive graphical user interface (GUI), like **Ubuntu,** or be better adapted to high performance server tasks, like **Red Hat**.

macOS - is the operating system **designed to run on Apple workstations**. It is included with every Macintosh computer and is the second most widely used workstation OS.

Chrome OS - is an operating system designed on the Chrome web browser and released by **Google**. The Chrome OS is a **cloud-based** OS with all of its data stored in Google Drive.

Cell Phone/Tablet Oss - are widely used, growing in hardware and performance, and raising the need for complex, powerful, yet convenient operating systems.

iPadOS - is an iPad-specific OS released by **Apple** that provides better multitasking functionality to the iPad, making it more of a small laptop than a tablet.

iOS - is the operating system on **Apple**'s iPhones and older iPads. It cannot be installed on devices not manufactured by Apple.

Android - is an operating system developed by **Google** specifically for mobile devices. It is based on the Linux kernel and is **free and open source**. Many devices from different manufacturers around the world make phones and tablets that run the Android operating system. It is the most used mobile OS.

Various Filesystem Types - file system allows storing, managing, and accessing files on a partition. A partition is a segment of a hard disk that functions as a separate entity. An OS usually supports different file systems, and a partition needs to be **formatted** with a specific file system before usage.

New Technology File System (NTFS) - is a file system that allows users to set and Manage **permissions** for files and folders for specific users and groups, making it very useful for secure network file sharing. Additionally, it provides indexing (for faster file search), compression, and encryption on the file system level. NTFTS is much **more advanced than FAT32** and is supported by all modern Windows versions.

File Allocation Table 32 (FAT32) - Providing very **basic features**, FAT32 is supported by many operating systems and supports partitions up to 2 TB in size.

Third Extended Filesystem (ext3) - is a default filesystem for **Linux OSs**.

Fourth Extended Filesystem (ext4) - is an updated version of ext3 that supports **larger partitions** and a larger number of files and improves performance.

Apple File System (APFS) - is **proprietary to Apple** and replaces the HFS and HFS+ filesystem on Apple OSs. It is the default filesystem on macOS Sierra 10.12.4 and iOS 10.3 and later.

Extensible File Allocation Table (exFAT) - is **designed for small flash and SSD drives** and is optimized for performance and media file storage.

Vendor Life-Cycle Limitations - Once an operating system is installed, it can continue running. But there are some limitations that you need to keep in mind and consider updating.

End-of-Life (EOL) - When an operating system reaches the end-of-life phase of its developer, there will be **no more updates**, patches, or technical support. There will probably be no more applications developed or supported for this OS version.

Update Limitations - When the OS **developer stops supporting** a specific version, there will be no more security patches released for that OS version. As new vulnerabilities get discovered, this may leave the computer with an outdated operating system exposed to security risks.

Compatibility Concerns Between Oss - Applications that are available for one operating system may not be available for others. The developer of the application may limit its efforts to only one operating system. Some applications may be available for macOS and Windows (for example, Microsoft Office). Some applications may be available for macOS, Windows, and Linux (for example, Google Chrome). In any case, these are **different installation files of similar software**.

Another compatibility concern may be caused when updating an operating system to a newer version. **New versions** of operating systems can cause **issues with previously installed** hardware and applications. Many large organizations choose to not update their operating systems without thorough testing of the new version with the existing hardware and business-critical software.

OS Installations and Upgrades - To start using an operating system, it needs to be installed on the computer. To start the installation process, the computer needs to be **booted with the installation media**. You must be able to install and perform upgrades in various OS environments. Questions about these concepts will be scenario based.

Boot Method - allows the user to select how to boot a computer and what media to use. There are **multiple ways** to boot a computer.

USB - An **external device** may be connected to a computer from which to boot. There are many types of external devices, for example: external optical drive, external hard disk, and external flash drive. Common interfaces used to connect the external drives are **Universal Serial Bus (USB)** and **eSATA**. A USB **flash drive** is a very common way to install an operating system.

Optical Media - A computer may have a **built-in drive** to read optical discs. A computer can be booted from this device with an installation disc. This is another common way to install an operating system on a computer.

Network - A network-based installation is the **most effective** way to install and upgrade when dealing with a **large network**. The installation media is uploaded onto a file share with read-only access for the installer.

Solid-State/Flash Drives - An **internally connected hard disk** may be used to boot. The disk can include the operating system installation image or have the operating system installed. This is the most common way to boot a computer after the operating system installation was completed.

Internet-Based - boot, the information needed to boot is stored and retrieved from the internet via an internet connection.

External/Hot-Swappable Drive - can be connected to a device for boot functions. The boot information is stored on the external drive and not locally stored.

Internal Hard Drive (Partition) - It's important to distinguish between a hard disk and a partition. In many simple configurations, there is one bootable partition on a disk. But one disk can have more than one partition, as it may be useful to have different operating systems on the same computer (**multi-boot**). Also, one logical partition can span multiple physical hard disks.

Types of Installations - Depending on the current state of the computer, available hardware and environment, and desired setup, there are multiple ways to install an operating system.

Upgrade - This is an installation method that installs a newer operating system over an older one. Depending on the OS and versions, it may **preserve the settings, files, and applications**.

Recovery Partition - Some operating systems provide an option to create a recovery partition during the installation. It will be a bootable partition that can be used later and contains diagnostic and repair tools, or it may be used for a repair installation.

Clean Install - This installation disregards previous data in the destination. It can be used if the computer doesn't have any operating system installed or if the intent is to completely delete the previous operating system, files, applications, and settings.

Image Deployment - If many computers have identical hardware and need identical operating systems, settings, and applications, it can be accomplished with image deployment. There are different software tools for this task, but usually the process involves the following steps:
1. Select one computer.
2. Perform a clean installation of the desired operating system, configure, and install applications.
3. Create the image from this computer.
4. Make this image available on the network or portable media.
5. Copy the image to other computers.

Repair Installation - Some operating systems provide this option. It is usually initiated by booting with the installation media of the same version of operating system that was previously installed, then selecting the **repair option** from the menu. It rewrites system files and settings while keeping the user files. This mode may be useful for repair purposes if the installed operating system is not bootable or shows serious issues that can't be fixed otherwise.

Remote Network Installation - The **Preboot eXecution Environment (PXE) network boot** can use a remote server with the operating system's installation files to install the OS on the computer. Depending

on the configuration of the server, the installation process may require selecting installation options, just like booting from a CD, or it can be an unattended installation.

Other Considerations - It's important to consider unplanned consequences of an installation. These potential consequences include data loss, application support, and hardware compatibility.

Third-Party Drivers - must be compatible with the installed OS.

Partitioning - creates one or more logical drives on a physical disk. Each partition can be separately formatted and have a separate file system. In Windows, each partition can have a separate drive letter.

Master Boot Record (MBR) - is used with traditional BIOS and is the standard partition table. MB can have a maximum of four primary partitions or three primary partitions and one extended partition.

Globally Unique Identifier (GUID) Partition Table - A GUID Partition Table (GPT) contains information on how the disk is partitioned and is used with **UEFI BIOS**. Compared to the MBR, it supports larger drives and more partitions per drive with up to 128 primary partitions.

Drive Format - Formatting drives when partitioning is included in the Windows installation. Drives can be formatted with a quick format or a full format.

Upgrade Considerations - Here are some other considerations to keep in mind when upgrading and configuring the operating system.

- **Backup Files and User Preferences -** When upgrading to a newer version of the Windows OS, a backup of all files should be made to ensure recoverability if the installation goes wrong. The Windows upgrade process is designed, however, to retain files and most user preferences.
- **Application and Driver Support/Backward Compatibility -** Windows upgrades are typically designed to be backward compatible with older versions. How far back the compatibility reaches depends on the upgrade version. This applies to applications and driver support as well.
- **Hardware Compatibility -** Ensure that the system's hardware is supported to install and configure the desired operating system. The essential BIOS, CPU, and RAM need to support the installation. The hardware should have supported drivers to be used optimally by the OS.
- **Feature Updates -** Feature updates are available for older OS versions and will continue to be available until the end-of-life (EOL) date for the version. Technicians must be aware of EOL as it relates to feature updates for their OS version(s).
- **Product Life Cycle -** The product life cycle begins when a product is released and ends when the product is no longer supported, its EOL.

macOS/Desktop OS Features and Tools - macOS and Linux operating systems come with similar utilities, tools, and commands for configuration and maintenance. You must be able to identify common features and tools of the macOS/Desktop OS.

Installation and Uninstallation of Applications - on the macOS is similar to the Windows OS. The application must be provided to the OS, mounted to the OS, and then installed on the OS. Applications on the macOS are available through Apple's proprietary App Store.

File Types - common types of files for the macOS, including ZIP, ISO, DMG, PKG, and APP.

.dmg—is a disk imaging file and acts just like an ISO or ZIP file.

.pkg—is an automated package installer file and can be found in a DMG, ZIP, and physical media.

.app—contains applications and includes files and resources the app needs as well as the executable.

App Store - is where apps for the macOS can be downloaded and purchased with a valid Apple ID.

Uninstallation Process - Applications that need to be uninstalled can be located using the Finder menu. The application being deleted is moved into the trash bin. Alternatively, you can simply select the application and press "Command" + "Delete".

Apple ID and Corporate Restrictions - The Apple ID is the **digital identity of the user** of a device. One Apple ID can be used on multiple devices and is linked to the Apple Wallet and App Store for purchases. Apple retains complete control over what is published to the App Store via corporate restrictions. Open-source applications are not available on the macOS unless submitted to and approved by Apple.

Best Practices - for maintaining the system, data, and performance. These are the most important ones.

Backups - Scheduled backups create a **copy of data and configuration** that can be restored later if needed. The best practice is to frequently create backups of files and have a copy of important files at a **remote location**. This remote location may be cloud storage that can be accessed over the internet.

Antivirus - software often depends on the signatures of viruses and other malicious software that needs to be updated. Make sure that the security software is configured to get frequent updates after installing it.

Updates/Patches - In macOS, the **System Preferences** for the **App Store** provide the configuration for system updates. You can choose to either manually or automatically download and install the updates. Patches are smaller updates, usually addressing specific functions and features, security, and bugs. These are managed similarly to system updates. The best practice is to allow **automatic installation** of patches to improve security if the environment allows this disruption.

Drivers and hardware firmware sometimes get updated too. These are managed similarly to system updates. Again, the best practice is to **install driver updates as quickly as possible** after they're released to improve hardware performance, but after ensuring there are no compatibility issues.

System Preferences - The macOS is highly customizable through System Preferences and can be personalized to fit preferences and requirements.

Displays - adjust display resolution and brightness as well as color tone and AirPlay preferences.

Networks - controls the network connectivity of the device, such as Wi-Fi preferences, as well as geographically controlled network preferences.

Printers and Scanners - section displays all relevant printer preferences, such as print priority, and settings related to connected printers and scanners. Scanners are likewise located here.

Privacy - The Security & Privacy section contains numerous settings and preference choices to ensure the security of the device, such as the lock screen, the FileVault, and the firewall.

Accessibility - allows for the customization of preferences to accommodate visual-, hearing-, and motor skills-impaired users.

Time Machine - is the macOS's automated backup feature and can be set to make specified backups, both incremental and full.

Multiple Desktops - feature allows you to create multiple Spaces that can be used to organize what the user is working on. These multiple desktops can be switched back and forth as needed.

Mission Control - is a program that allows you to view everything that is open and also quickly swap between programs. Mission Control also allows you to create multiple desktops.

Keychain - feature in the Mac operating system is a tool used for password management. Items that can be stored in Keychain include passwords, private keys, certificates, and secure notes.

Spotlight - is a search feature on the macOS. It creates an index of all the items and files on your system so you can look up items quickly.

iCloud - program comes as a default on all Apple products. It is a method for storing data in the cloud. This is beneficial as a backup method for Mac users.

Gestures - are small motions that a user can make using the trackpad to complete simple tasks. For example, to move between pages of a document, swipe left or right with two fingers. All the Gestures for Mac devices can be found under System Preferences, then by selecting Trackpad.

Finder - is the default file manager for Mac operating systems, similar to the FIle Explorer program in Windows. Finder allows users to search for, open, and delete files from one location.

Remote Disc - feature allows smaller Mac devices that do not have a disc drive to essentially "borrow" the disc drive of a nearby device. It allows the computer without the disc drive to access the files on a disc that is being used on another device.

Dock - in macOS is similar to the taskbar in Windows. It is the launching pad for all applications on Mac operating systems.

Disk Utility - can be used to create and restore **disk images**. It can also be used to check for **disk errors**.
FileVault - allows you to configure disk-level encryption for files and set user authentication for access.
Terminal - is where the user can run command lines on the macOS.
Force Quit - If an application becomes unresponsive and needs to be closed, you may need to force quit. It will **terminate the application** and you will lose unsaved work. It can be accomplished by selecting the application and pressing the quit button in the Activity Monitor.
Linux Client/Desktop OS - has its own set of OS-specific common features and tools that you must be able to identify.
Common Commands - To be successful in using Linux operating systems, you will need to be familiar with at least the most basic Linux commands. Being able to navigate the Linux terminal using these basic commands will be very beneficial. It's important to note that Linux commands are case sensitive, so take note of the case you are using when typing them.
ls—list command - list all the files or folders in a given directory. In order to use this command, navigate to the folder or directory you're interested in and type "ls". After hitting enter, a list of all the files and folders in that location will be displayed.
pwd—stands for **present working directory**, it displays the full path of the current working directory.
mv—is the **move** command. Allows a user to move a specified file to another location. Move is similar to a cut and paste command in Windows.
cp—**copy**. Its functionality is similar to that of the move file, except that it places a copy in the new location while leaving the file in the original location.
rm—**remove**. This is similar to a delete functionality, as it removes the file, directory, or other objects from the location.
chmod—To **modify Linux file permissions**, you must use the **chmod** command. Before changing Linux file permissions, it's important to first understand how they are represented. Each permission is represented by a letter: r–the read permission; w–the write permission; x–the execute permission.
chown—While the **chmod** command changes the permissions, the **chown** command **changes the ownership** of a file, directory, or other objects.
su/sudo—The **su** command stands for **switch user** (or substitute user). The **su** command can be used by adding a username that you wish to switch to after the command (example: su linuxuser1) or it can be used by itself, which will by default switch it to the root user. The **sudo** command switches the user for a single command, while **su** switches the user until it's switched back.
apt-get—APT stands for "advanced packaging tool." The **apt-get** command is a tool for **handling packages** in Linux. It is used to retrieve packages from authenticated sources for installation, upgrade, and removal of packages, along with their dependencies.
yum—The **yum** command is used in file management to **update and install packages for Red Hat**-based distributions.
ip—**display and configure information** related to a network interface card (NIC).
df—**processing files and displays the total free disk space** for a directory.
grep—**global regular expression print**. It is a search command. You can use it to search for a string of characters within a file or standard text output. For example, if you are viewing a file in the terminal and type the command **grep "unix"**, the terminal will display all of the instances of the word "unix" in that file.
ps— **process status.** Displays all of the currently running processes and their process numbers.
man—displays system **help for executable files**.
top—also displays a list of **running processes**.
find—can be used for **searching** for specific text within a file hierarchy.
dig—is used in networking and is a **DNS query utility**.
cat—displays the **contents** of a file.

nano—is a text-based **editor** for files.

Best Practices - for Linux are very similar to best practices for both Windows and Apple OSs.

Backups - Regular backups should be made of the system and stored in a separate location, such as a removable drive or the cloud.

Antivirus - programs are available for Linux distributions and should be monitored and kept up to date.

Updates/Patches - Linux distros manage updates differently. In Ubuntu, the settings are very similar to macOS and accessed via the Software & Updates settings. The best practice is to install updates as quickly as possible after they're released but after ensuring there are no compatibility issues. This practice applies to patches as well.

Tools - You should be aware of Linux-specific tools and their uses.

Shell/Terminal - is where the OS can be accessed via the command line. While there is GUI available for the Linux OS, the shell is a primary method of interaction with the system for many users.

Samba - is a free and open-source software (FOSS) package that can be installed on the Linux OS to make its underlying filesystem compatible with a Windows file server via the SMB Protocol.