4.1.11 Lesson Review

Date: 11/22/2025, 1:46:29 PM

Time Spent: 35:04

Score: 100%

Passing Score: 80%

Question 1 ✓ Correct

When configuring fan settings in the UEFI setup program, which option would you select to prioritize a quieter operation over cooling performance?

○ Fanless

○ Balanced

● Quiet ✓ Correct

○ Cool

Explanation

The "Quiet" setting prioritizes reducing fan speed to minimize noise, even if it allows for slightly higher system temperatures. This option is specifically intended for quieter operations.

The "Balanced" setting aims to provide a compromise between cooling performance and noise level, but it does not specifically prioritize quieter operation over cooling.

The "Cool" setting is designed to enhance cooling performance by running fans at higher speeds, which typically results in more noise, not less.

While "Fanless" might suggest a quieter operation, it is not a typical setting for active cooling systems in UEFI. It implies no fan operation, which could lead to overheating unless the system is specifically designed for passive cooling.

Related Content

4.1.5 Fan Considerations

resources\questions\q_fan_considerations_and_temperature_monitoring_01.question.xml

Question 2 ✓ Correct

Which security measure generates and stores cryptographic keys?

○ BIOS/UEFI password

○ Chassis intrusion detection

● Trusted Platform Module (TPM) ✓ Correct

○ DriveLock

Explanation

A Trusted Platform Module (TPM) is a special chip on the motherboard that generates and stores cryptographic keys. The TPM can be used by applications (such as Bitlocker on Windows systems) to generate and save keys that are used for encryption.

A BIOS/UEFI password controls access to the BIOS/UEFI setup program.

Chassis intrusion detection helps you identify when a system case has been opened.

DriveLock is a disk encryption solution.

Related Content

4.1.8 Trusted Platform Modules

resources\questions\q_trusted_platform_modules_02.question.xml

Question 3 ✓ Correct

You have purchased a new notebook. This notebook system uses UEFI firmware and comes with Windows 11 preinstalled. However, you want to use Linux on this system.

You download your favorite distribution and install it on the system, removing all Windows partitions on the hard disk in the process. When the installation is complete, you find that the operating system won't load when the system is rebooted.

Which of the following would allow your computer to boot to Linux?

○ Enable Secure Boot in the UEFI configuration.

○ Set the boot order to boot from the hard disk first in the UEFI configuration.

○ Enable the TPM chip on the motherboard.

● Disable Secure Boot in the UEFI configuration. ✓ Correct

○ Reinstall Windows 11 on the system.

Explanation

In this scenario, you should disable the Secure Boot option in the UEFI configuration. Secure Boot requires the operating system installed on the hard drive to be digitally signed. If it isn't digitally signed, the UEFI firmware will not boot it by default.

Reinstalling Windows 11 does not meet the requirements of this scenario.

If Secure Boot is already enabled, the TPM chip on the motherboard must already be enabled as well.

The boot order configuration is not preventing the system from booting in this scenario.

Related Content

4.1.6 Boot Passwords and Secure Boot

resources\questions\q_boot_passwords_and_secure_boot_02.question.xml

Question 4 ✓ Correct

Which of the following is a typical boot device option that can be prioritized in the system firmware's boot option sequence?

○ External monitor

○ Bluetooth device

● Network/PXE (Preboot Execution Environment) ✓ Correct

○ Printer

Explanation

Network/PXE is a typical boot device option that can be prioritized in the system firmware's boot option sequence. It allows the computer to boot via the network adapter by retrieving boot instructions from a configured server.

Bluetooth devices are not typically used as boot devices. They are primarily used for wireless communication and do not have the capability to store or execute boot instructions.

An external monitor is a display device and does not function as a boot device. It is used to display output from the computer but cannot store or execute boot instructions.

A printer is an output device used for printing documents and cannot be used as a boot device. It does not have the capability to store or execute boot instructions.

Related Content

- 4.1.1 BIOS and UEFI
- 4.1.3 Boot and Device Options
- 4.1.4 USB Permissions
- 4.1.5 Fan Considerations
- 4.1.6 Boot Passwords and Secure Boot
- 4.1.8 Trusted Platform Modules
- 4.1.11 Lesson Review

resources\questions\q_boot_and_device_options_04.question.xml

Question 5 ✓ Correct

In the context of system firmware, what is the primary purpose of configuring USB permissions through the UEFI setup program?

○ To install drivers for USB devices.

● To enable or disable USB ports for security reasons. ✓ Correct

○ To increase the data transfer speed of USB devices.

○ To update the firmware of USB-connected devices.

Explanation

The primary purpose of configuring USB permissions through the UEFI setup program is to enable or disable USB ports, which can be an important security measure to prevent unauthorized access or data transfer.

Configuring USB permissions in the UEFI setup program does not affect the data transfer speed of USB devices. Speed is determined by the USB version and hardware capabilities.

Installing drivers for USB devices is typically done within the operating system, not through the UEFI setup program.

Updating the firmware of USB-connected devices is not related to configuring USB permissions in the UEFI setup program. Firmware updates are usually performed through specific software tools provided by the device manufacturer.

Related Content

4.1.4 USB Permissions

resources\questions\q_usb_permissions_01.question.xml

Question 6 ✓ Correct

An energy company is strengthening its defenses and wants to look for methods that successfully protect trade secrets by ensuring none of its company's computing assets are hijacked by malware.

To assist in safeguarding the sensitive information, what can the technician enable to ensure this will not happen?

○ TPM

○ HSM

● Secure boot ✓ Correct

○ Boot password

Explanation

The technician can configure secure boot, which is a unified extensible firmware interface (UEFI) feature designed to prevent malware from hijacking a computer.

A trusted platform module (TPM) is a specification for hardware-based storage of digital certificates, cryptographic keys, and hashed passwords.

A hardware security module (HSM) is a secure USB key or thumb drive used to store cryptographic material where a user must authenticate before they can access the keys stored on the module.

A boot password requires the user to authenticate before the operating system is loaded. Different system software will provide different support for authentication methods. This measure cannot keep malware from injecting code into the bootloader of the operating system.

Related Content

4.1.6 Boot Passwords and Secure Boot

resources\questions\q_boot_passwords_and_secure_boot_01.question.xml

Question 7

✓ Correct

Which of the following BEST describes the technology that was designed to replace the BIOS and is a firmware solution for controlling the startup process and loading the computer operating system into memory?

○ EEPROM

● UEFI ✓ Correct

○ CMOS

○ BIOS 2

Explanation

UEFI was designed to replace the BIOS and is a firmware solution for controlling the startup process and loading the computer operating system into memory.

CMOS is a legacy computer chip technology that was used to store system information prior to the introduction of EEPROM.

EEPROM is a non-volatile memory chip that stores the system startup information that is configured through UEFI.

BIOS (Basic Input/Output System) is firmware used to provide runtime services for operating systems. BIOS version 2 does not exist.

Related Content

resources\questions\q_bios_and_uefi_04.question.xml

Question 8 ✓ Correct

Which of the following BEST describes the role of the Trusted Platform Module (TPM) in enhancing system security?

● Assessing whether the TPM is used to store cryptographic keys securely, preventing unauthorized access to encrypted data. ✓ Correct

○ Evaluating if the TPM is enabled to allow booting from USB devices for recovery purposes.

○ Verifying that the TPM is configured to support legacy BIOS mode for compatibility with older hardware.

○ Checking if the TPM is used to control fan speed and temperature monitoring for system stability.

Explanation

The TPM is designed to securely store cryptographic keys, which is crucial for protecting encrypted data and ensuring that sensitive information is not accessed by unauthorized users.

While booting from USB devices can be useful for recovery, it is not related to the primary function of the TPM. The TPM is not involved in enabling or disabling boot options; its role is focused on security, particularly in storing cryptographic keys.

The TPM does not play a role in supporting legacy BIOS mode. This option confuses the TPM's security functions with compatibility settings, which are unrelated to the TPM's purpose.

The TPM is not involved in hardware management tasks such as controlling fan speed or temperature monitoring. This option misrepresents the TPM's role, which is centered around security and cryptographic functions, not hardware stability.

Related Content

4.1.8 Trusted Platform Modules

resources\questions\q_trusted_platform_modules_07.question.xml

Question 9 ✓ Correct

A company has recently upgraded its systems to UEFI-based firmware, and some employees are experiencing issues accessing system settings during boot.

Which of the following actions would BEST evaluate and resolve the issue of missing the key prompt to access the UEFI setup program?

- ● Use the Shift-click method on the Restart button from the Windows logon screen to access UEFI boot options. ✓ Correct
- ○ Reboot the computer and continuously press the Delete key until the UEFI setup program appears.
- ○ Adjust the boot order to prioritize the hard drive, ensuring the system boots correctly.
- ○ Disable Secure Boot in the UEFI setup to allow easier access to system settings.

Explanation

Using the Shift-click method on the Restart button from the Windows logon screen to access UEFI boot options provides a reliable way to access UEFI boot options without relying on the timing of key presses during boot. It evaluates the issue by offering an alternative access method, ensuring users can reach the UEFI setup even if they miss the initial prompt.

While pressing the Delete key is a common method to access the UEFI setup, it does not evaluate the issue of missing the prompt. This approach relies on timing and may not resolve the problem if the boot process is too fast.

Disabling Secure Boot does not affect the ability to access the UEFI setup program. Secure Boot is a security feature and does not influence the key prompt or access method for UEFI settings.

Adjusting the boot order is unrelated to accessing the UEFI setup program. This action focuses on the sequence of boot devices rather than resolving the issue of missing the key prompt for UEFI access.

Related Content

- 4.1.1 BIOS and UEFI
- 4.1.3 Boot and Device Options

- 4.1.4 USB Permissions
- 4.1.5 Fan Considerations
- 4.1.6 Boot Passwords and Secure Boot
- 4.1.8 Trusted Platform Modules
- 4.1.11 Lesson Review

resources\questions\q_bios_and_uefi_06.question.xml

Question 10 ✓ Correct

A user reports that their computer frequently overheats and shuts down during intensive tasks. Upon accessing the system firmware settings, you notice that the fan speed is set to "Quiet" mode.

Which of the following actions should you take to analyze and resolve the overheating issue?

○ Disable USB ports to reduce power consumption and heat output from connected devices.

● Change the fan speed setting to "Cool" mode to increase fan activity and reduce system temperature. ✓ Correct

○ Adjust the boot order to prioritize the SSD, reducing the time the system spends booting and thus lowering heat generation.

○ Enable Secure Boot to ensure that only trusted software runs, preventing overheating.

Explanation

By analyzing the current fan speed setting, you can determine that the "Quiet" mode is likely contributing to the overheating issue. Changing the setting to "Cool" mode will increase fan activity, enhancing cooling and reducing system temperature during intensive tasks.

Secure Boot is a security feature that does not affect system temperature or fan operation. It ensures that only trusted software is loaded during boot but does not address overheating issues.

Adjusting the boot order does not impact the system's temperature during intensive tasks. Boot order settings determine the sequence of boot devices and do not influence heat generation or cooling.

Disabling USB ports may slightly reduce power consumption, but it is unlikely to have a significant impact on the overall system temperature during intensive tasks. The primary issue is related to fan speed settings, not USB port activity.

Related Content

4.1.5 Fan Considerations

resources\questions\q_fan_considerations_and_temperature_monitoring_05.question.xml

Question 11 ✓ Correct

A user reports that their computer is not booting from a newly installed SSD, even though it is properly connected.

Upon checking the system firmware settings, you find that the boot option sequence is set to prioritize the optical drive first, followed by a USB drive, and then the network.

Which of the following actions should you take to analyze and resolve the boot issue?

● Change the boot option sequence to prioritize the SSD as the first boot device. ✓ Correct

○ Enable Secure Boot in the UEFI setup to ensure the SSD is recognized as a trusted device.

○ Update the system firmware to the latest version to ensure compatibility with the SSD.

○ Disconnect the optical drive and USB drive to force the system to boot from the SSD.

Explanation

Analyzing the boot option sequence reveals that the SSD is not prioritized, which is why the system is not booting from it. By changing the sequence to prioritize the SSD, you ensure that the system firmware searches the SSD first for a boot manager, resolving the issue.

While disconnecting other boot devices might force the system to boot from the SSD, it is not an efficient or practical solution. It does not address the root cause of the issue, which is the incorrect boot option sequence.

Enabling Secure Boot is a security measure and does not influence the boot order or resolve issues related to boot device prioritization. It ensures that only trusted software is loaded but does not affect the SSD's boot priority.

While updating the firmware can be beneficial for compatibility, it is not necessary in this scenario. The issue is related to the boot option sequence, not firmware compatibility. Prioritizing the SSD in the boot sequence is the correct action to resolve the issue.

Related Content

- 4.1.1 BIOS and UEFI
- 4.1.3 Boot and Device Options

- 4.1.4 USB Permissions
- 4.1.5 Fan Considerations
- 4.1.6 Boot Passwords and Secure Boot
- 4.1.8 Trusted Platform Modules
- 4.1.11 Lesson Review

resources\questions\q_boot_and_device_options_05.question.xml

Question 12 ✓ Correct

You are a technician tasked with setting up a new computer system for a client who wants to install an operating system from a USB drive. However, the system is currently configured to boot from the internal hard drive first.

Which of the following actions should you take to ensure the system boots from the USB drive?

○ Disable the internal hard drive in the UEFI setup program to force the system to boot from the USB drive.

○ Format the internal hard drive to remove any existing boot managers.

● Access the UEFI setup program and change the boot option sequence to prioritize the USB drive over the internal hard drive. ✓ Correct

○ Connect the USB drive and restart the computer without making any changes to the boot order.

Explanation

By accessing the UEFI setup program and adjusting the boot option sequence, you can ensure that the system checks the USB drive for a boot manager before the internal hard drive. This is the appropriate action to take to boot from the USB drive.

Simply connecting the USB drive and restarting the computer will not change the boot order. The system will continue to boot from the internal hard drive as it is currently prioritized in the boot sequence.

Formatting the internal hard drive is unnecessary and could result in data loss. It does not address the need to change the boot order to prioritize the USB drive.

Disabling the internal hard drive is an extreme measure that is not required. Adjusting the boot order is sufficient to achieve the desired outcome without disabling hardware components.

Related Content

- 4.1.1 BIOS and UEFI
- 4.1.3 Boot and Device Options
- 4.1.4 USB Permissions

4.1.5 Fan Considerations

4.1.6 Boot Passwords and Secure Boot

4.1.8 Trusted Platform Modules

4.1.11 Lesson Review

resources\questions\q_boot_and_device_options_03.question.xml

Question 13 ✓ Correct

A technician is implementing a feature that will compare hashes of key system state data during the boot process to ensure that nobody has tampered with the system firmware, boot loader, and OS kernel.

What feature is this?

○ Encryption

● TPM ✓ Correct

○ HSM

○ Boot password

Explanation

The technician is implementing the trusted platform module (TPM), which, during the boot process, compares hashes of key system state data to ensure they have not been tampered with.

A hardware security module (HSM) is a secure USB key or thumb drive used to store cryptographic material where a user must authenticate before they can access the keys stored on the module.

Encryption products make data secure by scrambling it in such a way that only a user with the correct decryption key can subsequently read it.

A boot password requires the user to authenticate before the operating system is loaded. There are usually at least two passwords, though some systems may allow for more.

Related Content

- 4.1.1 BIOS and UEFI
- 4.1.3 Boot and Device Options
- 4.1.4 USB Permissions
- 4.1.5 Fan Considerations
- 4.1.6 Boot Passwords and Secure Boot
- 4.1.8 Trusted Platform Modules

4.1.11 Lesson Review
resources\questions\q_bios_and_uefi_01.question.xml

Question 14 Correct

A company is planning to implement a secure method for storing cryptographic keys used in their data encryption processes. They have several computers that do not support Trusted Platform Module (TPM) technology.

The IT manager is considering using a Hardware Security Module (HSM) for this purpose.

Which of the following reasons BEST justifies the use of an HSM in this scenario?

○ An HSM can be used to enhance the overall network bandwidth of the company.

○ An HSM can be used to improve the processing speed of encryption algorithms.

● An HSM provides a secure way to store cryptographic keys, especially for computers lacking TPM support. ✓ Correct

○ An HSM can be used to back up all company data to prevent data loss.

Explanation

A Hardware Security Module (HSM) is used to securely store cryptographic keys. It is particularly useful for computers that do not support TPM, providing a secure alternative for key storage and recovery.

An HSM is focused on secure storage of cryptographic keys, not on network performance.

The purpose of an HSM is specifically for securely storing cryptographic keys, not for general data backup.

An HSM is used for secure storage of cryptographic keys, which is unrelated to the speed of encryption processes.

Related Content

4.1.8 Trusted Platform Modules
resources\questions\q_trusted_platform_modules_06.question.xml

Question 15 ✓ Correct

You are a system administrator tasked with optimizing the cooling system of a high-performance workstation used for video editing. The workstation frequently overheats, causing performance issues.

Based on the system's UEFI settings, which of the following actions should you take to ensure the workstation operates efficiently without overheating?

- ● Configure the duty cycle settings to a higher percentage to increase the fan speed and improve cooling efficiency. ✓ Correct
- ○ Disable all USB ports to reduce power consumption and indirectly lower system temperature.
- ○ Use third-party applications to manually monitor the temperature and adjust fan settings as needed.
- ○ Set the cooling option to "Quiet" to reduce fan noise and allow the system to run at higher temperatures.

Explanation

Increasing the duty cycle settings will make the fans run faster, enhancing cooling efficiency and helping to prevent the workstation from overheating. This action directly addresses the overheating issue by improving airflow and heat dissipation.

While this option reduces fan noise, it allows the system to run at higher temperatures, which is not ideal for a workstation that is already experiencing overheating issues. This setting prioritizes noise reduction over cooling efficiency.

Disabling USB ports may slightly reduce power consumption, but it is unlikely to have a significant impact on the system's overall temperature. This action does not directly address the cooling needs of the workstation.

While third-party applications can provide valuable temperature monitoring, they do not directly adjust fan settings through UEFI. The question specifically asks for actions within the UEFI settings, making this option less relevant to the scenario.

Related Content

4.1.5 Fan Considerations

resources\questions\q_fan_considerations_and_temperature_monitoring_03.question.xml

Copyright © CompTIA, Inc. All rights reserved.