



CertsMania

Free Questions for 220-1201

Shared by **Hugh** on **Dec 2, 2025**

For More Free Questions and Preparation Resources

Check the Links on Last Page



CertsMania

Questions # 1:

Which of the following storage options would a technician most likely recommend to have large amounts of affordable capacity without concern for read times on a desktop computer?

Options:

A.

750GB NVMe M.2 SSD

B.

2x 1TB PCIe SSD in RAID 1

C.

2TB SATA 3.5" 5,400rpm HDD

D.

4TB SAS 2.5" 15,000rpm HDD



CertsMania

Answer

C

Explanation

If performance is not a primary concern and the user requires large, cost-effective storage, a 2TB 5400rpm SATA HDD is ideal. It offers high capacity at a lower price point than SSDs and faster HDDs.

Option A: NVMe drives offer exceptional speed but are significantly more expensive per GB and not necessary when read/write speed is not a concern.

Option B: RAID 1 improves redundancy but cuts usable capacity in half and uses expensive SSDs.

Option D: SAS drives are fast and reliable but are enterprise-grade and expensive overkill for desktop use.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.3: Given a scenario, install and configure storage devices.

Questions # 2:

A help desk technician needs to work on a high-volume printer. Users have reported occasional paper jams and smudges appearing on printed documents. Which of the following steps should the technician do next to address these issues?

Options:

A.

Perform a full factory reset.

B.

Check and clean the rollers.

C.

Change all the ink or toner cartridges.

D.

Replace the fuser.

Answer

B

Explanation

Paper jams and smudging in high-volume printers are often caused by dirty or worn rollers. Rollers are responsible for feeding the paper through the printer. Over time, they accumulate dust, toner residue, or wear out, resulting in misfeeds or jams. Cleaning or replacing them typically resolves this issue.

Option A (Factory reset): A full reset does not directly address mechanical issues like dirty rollers or smudging. It's a last resort and more relevant to configuration or software-related issues.

Option C (Change toner cartridges): While toner quality can affect print quality, it won't usually cause jams or widespread smudging unless the cartridge is leaking which is less likely across multiple users.

Option D (Replace the fuser): A damaged fuser could cause smudging, but this is typically after extensive use and is not the first thing to check. Fuser issues also usually present more persistent, uniform smudges.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.7: Given a scenario, troubleshoot common printer problems.

Questions # 3:

A user prints a spreadsheet in duplex mode. The spreadsheet is difficult to read because some of the columns spill onto the second side of the page. Which of the following should the user do to prevent the issue but still print on both sides of the page?

Options:

A.

Turn off duplex printing.

B.

Try a smaller font size in the spreadsheet.

C.

Change the page orientation.

D.

Use a different print driver.

Answer

C

Explanation

Changing the page orientation (e.g., from portrait to landscape) allows wider columns to fit on one side of the page. This maintains readability while continuing to use duplex printing.

Option A: Disabling duplex defeats the goal of printing on both sides.

Option B: May help, but could make the document harder to read if the font is too small.

Option D: Unlikely to resolve formatting issues related to layout and dimensions.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.7: Given a scenario, troubleshoot common printer problems.

Questions # 4:

A user reports that their desktop PC does not turn on. Which of the following components would most likely cause the issue?

Options:

A.

PSU

B.

GPU

C.

RAM

D.

CPU



CertsMania

Answer

A

Explanation

If a desktop fails to power on entirely, the most probable cause is a faulty Power Supply Unit (PSU). If there are no lights, fans, or POST beeps, the PSU may have failed, cutting off all power to the motherboard and components.

Option B (GPU): Could prevent video output, but the system would still power on and beep.

Option C (RAM): Missing or faulty RAM would cause POST errors but not prevent startup entirely.

Option D (CPU): A bad CPU may cause POST failure, but the system would usually at least power on.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.5: Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.

=====

Questions # 5:

Which of the following provides electricity to devices through network cables?

Options:

A.

Edge router

B.

PoE switch

C.

Access point

D.

Patch panel



CertsMania

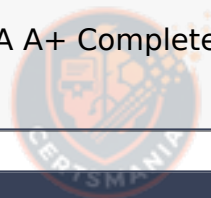
Answer

B

Explanation

A PoE (Power over Ethernet) switch transmits both data and electrical power over Ethernet cables to devices like wireless access points or VoIP phones. This is especially useful in areas where separate power sources are not available.

[Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter - Chapter 5, pages 319-321., , , , , ,]



CertsMania

Questions # 6:

A technician is setting up a new SOHO wireless router. According to security best practices, which of the following should the technician do first?

Options:

A.

Enable encryption.

B.

Assign a static IP.

C.

Change the default password.

D.

Reset the router.



CertsMania

Answer

C

Explanation

The first security step after deploying a new router is to change the default administrative password. Default credentials are well known and pose a security risk if left unchanged.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.3 - Secure a wireless network:

“Always change default administrative credentials before further configuration to prevent unauthorized access.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Wireless Security

CompTIA Exam Objectives 220-1101, Domain 2.3

=====



CertsMania

Questions # 7:

A help desk technician inspects a laptop keyboard because a single key has stopped working. The technician checks the keyboard for debris. Which of the following actions should the technician do next to troubleshoot the issue cost-effectively?

Options:

A.

Replace the keyboard.

B.

Replace the key switch

C.

Replace the circuit board.

D.

Replace the keycap



CertsMania

Answer

B

Explanation

If only one key is not functioning and debris has been checked, replacing the individual keycap is the most cost-effective next step. It's a simple, low-cost option before considering more extensive repairs like replacing the entire keyboard.

[Reference: "CompTIA A+ Complete Practice Tests" by Jeff T. Parker – Chapter 1, Question 10, page 8., , , ,]

Questions # 8:

Which of the following cable types can be used to transfer data and video?

Options:

A.

USB-C

B.

HDMI

C.

DisplayPort

D.



CertsMania

VGA

Answer

A

Explanation

USB-C is a versatile connector capable of transmitting data, video, audio, and power. With standards like DisplayPort over USB-C or Thunderbolt 3/4, it can be used for external displays, file transfers, charging, and more all through one cable.

Option B (HDMI): Supports video and audio but not general data transfer.

Option C (DisplayPort): Similar to HDMI supports video/audio but not general file transfer.

Option D (VGA): Legacy analog video only no data or audio support.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.1: Identify common connector types.

Questions # 9:

A company wants to have fast read speeds for its locally stored data. Which of the following configurations has the lowest cost to fulfill this requirement?

Options:

A.

RAID 0

B.

RAID 1

C.

RAID 5

D.

RAID 10



CertsMania

Answer

A

Explanation

RAID 0 (striping) provides the fastest read (and write) speeds at the lowest cost, as all disk capacity is used for storage and performance. However, it offers no redundancy.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.4 - RAID types:

"RAID 0 stripes data across multiple disks, offering the best performance and lowest cost but no fault tolerance."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: RAID Levels

CompTIA Exam Objectives 220-1101, Domain 3.4

Questions # 10:

A new directive mandates the use of a security component to securely allow users to authenticate to systems, access sensitive data, and enter the office. The component must provide an additional factor of authentication alongside user accounts and cannot be something the user owns. Which of the following components best meets these requirements?

Options:

- A.
Fingerprint reader
- B.
Smart card
- C.
Secure token
- D.
NFC scanner



CertsMania

Answer

B

Explanation

A smart card provides an additional factor of authentication by storing secure credentials, such as certificates, that cannot be guessed or replicated. It complements user accounts and is "something you have".

Why Not A (Fingerprint reader): This is "something you are", but the scenario specifically requires a physical token.

Why Not C (Secure token): Secure tokens are also valid but may not integrate as seamlessly into multi-factor authentication for physical and system access.

Why Not D (NFC scanner): An NFC scanner is a device and not a token itself; it reads cards or other credentials.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.5, access controls.

Questions # 11:

A user brings a laptop to work every morning, correctly seats it in the docking station and then opens the laptop to begin work with no issues. After the user left the laptop at home during a two-week vacation the laptop is no longer working. Upon returning to the office, the user reports that the keyboard and display are no longer working. Which of the following should the technician ask the user to do first?

Options:

A.

Ensure the docking station is plugged in.

B.

Press and release the laptop power button.

C.

Plug the laptop in and let it charge overnight.

D.

Connect the laptop directly to the network.

Answer

B

Explanation

Reasoning: Many docking stations provide power and functionality only when the laptop is properly powered on. If the laptop was powered off (e.g., during the vacation), docking it will not automatically turn it on. The technician should first ensure the laptop is powered on by pressing the power button.

This is a common troubleshooting step when laptops in docking stations appear non-functional.

Relevance to CompTIA A+ Core 1: This falls under Objective 5.2, which covers diagnosing and resolving common laptop and mobile device issues.

Why the Other Options Are Incorrect:

A. Ensure the docking station is plugged in:

While ensuring power to the docking station is important, the scenario specifies that the issue occurred after a vacation. The likelihood of the docking station losing power coincidentally during the vacation is low. Verifying the laptop's power state should be the first step.

C. Plug the laptop in and let it charge overnight:

There is no indication the laptop's battery is drained. While charging could resolve a dead battery, the user is more likely experiencing an issue where the laptop is powered off but docked, so charging overnight is not the best first step.

D. Connect the laptop directly to the network:

A network connection will not resolve the primary issue of the keyboard and display not working. Addressing the laptop's power state is a higher priority.

Practical Example:

If a user returns from a vacation and places a powered-off laptop into a docking station, it may not automatically power on. Pressing the power button ensures the laptop is operational and communicating with the docking station.

CompTIA A+ Exam Objective Alignment:

Objective 5.2: Troubleshooting common laptop issues, including power, display, and peripheral connectivity.

Questions # 12:

Users working with large files back up the files to external hard drives. One user's files take longer to back up than other users' files. The user has tried backing up the files to other users' drives with the same results. Which of the following steps should the technician take first to correct this issue?

Options:

- A.
Replace the hard drive's USB cable.
- B.
Defragment the user's external hard drive.
- C.
Update the storage drivers on the user's system.
- D.
Instruct the user to compress the files.

Answer

B

Explanation

If a hard drive is heavily fragmented, file read/write operations can take significantly longer, causing slow backup speeds. Defragmenting the drive organizes the data for more efficient access.

Why Not A (Replace the hard drive's USB cable): A faulty cable would typically cause disconnections or errors, not just slower speeds.

Why Not C (Update the storage drivers): This might help if the issue is with system drivers, but the described symptoms point to a fragmentation issue.

Why Not D (Compress the files): Compression reduces file size but does not address the root cause of the slow backups.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 3.1, storage troubleshooting.

Questions # 13:

A user returns from a trip and discovers a computer that is connected to the LAN times out intermittently. Upon investigation, a technician finds the RJ45 pin is not properly terminated. Which of the following networking tools is most appropriate to fix the issue?

Options:

A.

Toner probe

B.

Cable tester

C.

Punchdown

D.

Crimper



CertsMania

Answer

D

Explanation

D. Crimper:

A crimper is used to terminate an RJ45 cable properly by attaching the connector to the twisted-pair wires.

If the termination is not done correctly, the connection will be intermittent or fail entirely.

Incorrect Options:

A. Toner probe: Used to locate cables or trace their path, not for terminating RJ45 connectors.

B. Cable tester: Useful for testing connectivity but does not fix termination issues.

C. Punchdown: Used to connect wires to a patch panel or keystone jack, not for RJ45 connectors.

Key Takeaway: A crimper is the proper tool for fixing an improperly terminated RJ45

connection.

[Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 2.8 – Using appropriate tools for network troubleshooting., , , , ,]

Questions # 14:

A user is unable to access secure applications on their tablet when working from home a couple days per week, but the applications work when in the office. Which of the following services most likely needs to be reconfigured to allow for remote work?

Options:

A.

Global Positioning System

B.

Mobile device management

C.

Wi-Fi Protected Access

D.

Near-field communication

Answer

B

Explanation

Mobile Device Management (MDM) software often controls access to corporate resources based on location, network, or VPN status. If the MDM is not configured to allow access from outside the office or via home networks, the apps may be blocked. This is the most probable cause if apps work only on-premises.

Option A: GPS is used for location services, not access control.

Option C: WPA is a Wi-Fi security protocol, not related to access restrictions.

Option D: NFC enables close-range communication irrelevant to app access.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.6: Given a scenario, configure basic mobile device network connectivity and application support.

Questions # 15:

A technician is troubleshooting a workstation that repeatedly shuts down within ten minutes of being turned on. The technician notices a loud clicking sound coming from inside the case. Which of the following components should the technician check first?

Options:

A.

Exhaust fan

B.

Capacitors

C.

CPU fan

D.

Intake fan

Answer

C

Explanation

A failing CPU fan may make unusual noises (including clicking) and, if it is not cooling the CPU, the system will quickly overheat and shut down to prevent damage.

From CompTIA A+ 220-1101 Official Study Guide, Objective 4.1 – Troubleshooting hardware problems:

“Overheating due to a failed or obstructed CPU fan can cause frequent shutdowns. Loud noises are a sign the fan should be checked first.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: PC Hardware Troubleshooting

=====

Questions # 16:

Which of the following devices has ACL capabilities?

Options:

- A.
PoE injector
- B.
DSL
- C.
Firewall
- D.
Unmanaged switch

Answer

C

Explanation

Firewalls are specifically designed to monitor, filter, and control network traffic using Access Control Lists (ACLs). ACLs define which traffic is allowed or denied based on parameters like IP address, protocol, or port.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.2 - Networking hardware and security:

“Firewalls use access control lists (ACLs) to allow or deny traffic based on rules. Unmanaged switches and PoE injectors do not support ACLs.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Networking Security Devices

=====

Questions # 17:

A technician is installing a new high-end graphics card that uses a 12VHPWR connector. Which of the following is the maximum wattage supported by this power connector?

Options:

- A.
400W
- B.
MOW
- C.
600W
- D.
700W

Answer

C

Explanation

The 12VHPWR connector can supply up to 600 watts of power, designed for high-end graphics cards.

Why Not A (400W): This is less than the connector's maximum capability.

Why Not B (MOW): This is an invalid option.

Why Not D (700W): The maximum supported power is 600W.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.4, power supply and connectors.

Questions # 18:

A technician is troubleshooting an all-in-one laser printer that prints a vertical line when making copies and scans. When users print or receive faxes, the output from the printer is correct. Which of the following should the technician examine to determine the cause of the issue?

Options:

- A.
The pickup rollers
- B.
The corona wire
- C.
The document feeder
- D.
The drum assembly



CertsMania

Answer

C

Explanation

Since the issue only occurs during scanning and copying (not printing or faxing), the problem is isolated to the document feeder. A vertical line is typically caused by debris or damage on the glass under the ADF (Automatic Document Feeder), not on components related to printing.

[Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter - Chapter 4, page 261.,.,.,.,.]

Questions # 19:

A user is testing a new OS that is contained on a USB drive. The user wants the new OS to load automatically when the computer is turned on. Which of the following should the user configure?

Options:

- A.
BIOS password
- B.
Trusted Platform Module
- C.
USB permissions
- D.
Boot options



CertsMania

Answer

D

Explanation

To boot from a USB drive, the user must configure the boot order in the system BIOS/UEFI to prioritize the USB device. This setting tells the computer to load the operating system from the USB device on startup.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.5 – Configure BIOS/UEFI settings:

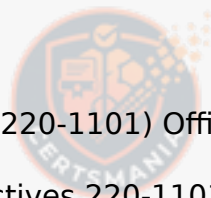
“The boot order determines the sequence in which the system firmware attempts to find an OS to boot. Setting USB as the first boot device allows the computer to boot from a USB drive.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: BIOS/UEFI Configuration

CompTIA Exam Objectives 220-1101, Domain 3.5

=====



CertsMania

Questions # 20:

A developer wants to protect critical data from hard drive failure. Their workstation has two hard drives. Which RAID level should they use?

Options:

A.

RAID 0

B.

RAID 1

C.

RAID 5

D.

RAID 10



CertsMania

Answer

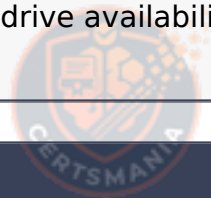
B

Explanation

RAID 1, also known as disk mirroring, duplicates data identically to two drives, ensuring full redundancy if one drive fails. Because the workstation only has two drives, RAID 1 is the only RAID level that provides fault tolerance under this constraint, exactly as described in the CompTIA A+ study guide.

RAID 0 offers no redundancy, RAID 5 requires at least three drives, and RAID 10 requires at least four drives.

RAID 1 is the recommended configuration for small environments or workstations that rely on data integrity and quick recovery, matching CompTIA's guidance for redundancy in systems with limited drive availability.



CertsMania

Questions # 21:

Which of the following DNS records would an administrator change to redirect email flow?

Options:

A.

MX

- B.
TXT
- C.
SPF
- D.
CNAME



CertsMania

Answer

A

Explanation

AnMX (Mail Exchange) record defines which mail servers are responsible for receiving email for a domain. If you want to change or redirect email traffic, theMX record must be updated with the correct server information.

Option B (TXT): Stores text-based info used for SPF, DKIM, etc.

Option C (SPF): Part of email authentication stored in a TXT record; doesn't redirect traffic.

Option D (CNAME): Alias for another domain name not used for email routing.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 2.4: Compare and contrast common networking hardware.

=====

Questions # 22:



CertsMania

A user can connect their laptop to the internet in the main office. However, when the user places the laptop on top of a motor on the factory floor, there is no internet connectivity. Which of the following is the most likely cause of this issue?

Options:

- A.
Jitter

B.

Insufficient power levels

C.

External interference

D.

High latency



CertsMania

Answer

C

Explanation

Large electrical motors can emit electromagnetic interference (EMI), which can disrupt wireless signals and prevent connectivity.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.4 - Wireless troubleshooting:

“Sources of external interference such as motors or other electrical equipment can disrupt wireless network connectivity.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Networking Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 2.4

=====



CertsMania

Questions # 23:

Which of the following can carry data and electricity to network devices? (Select two).

Options:

A.

Router

- B.
Injector
- C.
Cable modem
- D.
Access point
- E.
PoE
- F.
Unmanaged switch



CertsMania

Answer

B, E

Explanation

PoE (Power over Ethernet) allows both data and electrical power to be delivered over the same Ethernet cable. A PoE injector adds power to Ethernet cables for devices that need it.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.2 - Networking hardware:

“Power over Ethernet (PoE) technology and PoE injectors enable both power and data transmission to compatible network devices like access points and IP cameras.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Network Hardware

CompTIA Exam Objectives 220-1101, Domain 2.2

=====

Questions # 24:

Which of the following involves installing an application on a server so several users can run the application concurrently without the need for local installation?

Options:

A.

Client virtualization

B.

Software as a service

C.

Sandboxing

D.

Embedded software



CertsMania

Answer

A

Explanation

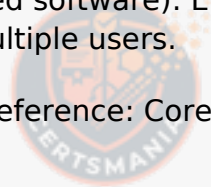
Client virtualization involves installing an application on a server and enabling multiple users to run the application simultaneously via virtualized sessions. This eliminates the need for individual installations on local machines.

Why Not B (Software as a Service): SaaS delivers software over the internet and does not require local installations but is managed by a third party, not the organization itself.

Why Not C (Sandboxing): Sandboxing is for isolating applications for security testing, not for concurrent user access.

Why Not D (Embedded software): Embedded software is installed on hardware devices, not shared across multiple users.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 4.2, virtualization concepts.



CertsMania

Questions # 25:

An end user's domain password expires while they are working from home. The end user tries to reset the password using Ctrl+Alt+Delete and then receives the following message:

Configuration information could not be read from the domain controller, either because the machine is unavailable or because access is denied.

Which of the following will resolve this issue?

Options:

A.

Restart the computer.

B.

Connect to the VPN.

C.

Reset the account in Active Directory.

D.

Join the Wi-Fi network.



CertsMania

Answer

B

Explanation

To change a domain password from a remote location, the system must communicate with the domain controller. Since the user is working from home, they need to connect to the corporate VPN to establish that secure connection. Without it, the password change cannot be authenticated.

Option A: Restarting will not resolve the lack of connection to the domain controller.

Option C: Resetting the password in AD could help, but doesn't let the user reset it themselves.

Option D: The user may already be on Wi-Fi; the issue is with connecting to the corporate network, not local.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.6: Given a scenario, configure basic mobile device network connectivity and application support.

=====

A technician observes slow startup times on a laptop. Which of the following is most likely causing the issue?

Options:

- A.
HDD
- B.
RAM
- C.
NIC
- D.
BIOS



CertsMania

Answer

A

Explanation

A hard disk drive (HDD), especially if it's older or nearly full, is the most common cause of slow startup times in laptops. HDDs are much slower than SSDs and can significantly bottleneck the boot process.

From CompTIA A+ 220-1101 Official Study Guide, Objective 4.1 – Troubleshoot common hardware problems:

“A slow startup or sluggish system performance is commonly due to a failing or fragmented hard disk drive (HDD). Replacing with an SSD can greatly improve boot times and overall system responsiveness.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Troubleshooting PC Hardware

CompTIA Exam Objectives 220-1101, Domain 4.1

=====

Questions # 27:

Which of the following is an advantage of using a hybrid cloud instead of a public cloud?

Options:

- A.
Ability to reduce management overhead
- B.
Ability to use cross-platform virtualization
- C.
Ability to meet data residency requirements
- D.
Ability to leverage IaaS and PaaS

Answer

C

Explanation

A hybrid cloud combines on-premises infrastructure with public cloud services. One significant advantage is that it allows organizations to keep sensitive data in a private environment to meet regulatory or data residency requirements, while still utilizing the scalability and cost-efficiency of the public cloud for other workloads. This ensures compliance with legal mandates about data location.

[Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter - Chapter 8, "Virtualization and Cloud Computing", page 488. Also supported in CompTIA A+ Exam Objectives 220-1201 under section 4.1., , , ,]

Questions # 28:

Which of the following DNS record types is used to direct email to a mail server?

Options:

A.

CNAME

B.

SRV

C.

MX

D.

SOA



CertsMania

Answer

C

Explanation

An MX (Mail Exchange) record specifies the mail server responsible for receiving email for a domain.

Why Not A (CNAME): CNAME is used for domain aliasing, not for email delivery.

Why Not B (SRV): SRV records are used to locate specific services, not mail servers.

Why Not D (SOA): SOA records provide domain information but do not handle email.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.6, DNS record types.



CertsMania

Questions # 29:

A user reports that the print quality of their desk printer is poor. A technician replaces the ink cartridge, but this does not resolve the issue. Which of the following should the technician do next?

Options:

A.

Replace the pickup rollers

B.

Clean the printheads

C.

Switch the paper type

D.

Change the ribbon



CertsMania

Answer

B

Explanation

If print quality remains poor after replacing the ink cartridge, the next step is to clean the printheads. Printheads can become clogged with dried ink, especially in inkjet printers, causing streaks or faded output.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 4.3 – Troubleshoot printing problems:

“Poor print quality after replacing cartridges is commonly caused by clogged or dirty printheads. Use the printer's cleaning cycle or manually clean the printheads as needed.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Printer Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 4.3

=====



CertsMania

Questions # 30:

A customer needs to install a new printer in their network. The customer reports that users had intermittent connectivity issues with previous printers. Which of the following should the technician configure on the new printer to prevent this issue?

Options:

A.

Gateway IP address

B.

DHCP IP address

C.

Static IP address

D.

Public IP address



CertsMania

Answer

C

Explanation

Intermittent connectivity issues with network printers are commonly caused by changing IP addresses when using DHCP. Assigning a static IP address ensures that the printer is always reachable at the same IP address by client machines.

[Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter - Chapter 4, "Printers and Multifunction Devices", page 241., , , ,]

Questions # 31:

A technician wants to upgrade a computer to a new Windows version. The Windows Upgrade Advisor states that the computer is not compatible with the new Windows version due to a lack of TPM 2.0 support. Which of the following should the technician do next?

Options:

A.

Enable the module in the UEFI BIOS.

B.

Install an HSM in the computer.

C.

Perform a clean Install of the new Windows version.



CertsMania

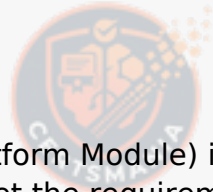
D.

Implement BitLocker on the computer.

Answer

A

Explanation



CertsMania

TPM 2.0 (Trusted Platform Module) is often disabled by default in the UEFI BIOS. Enabling it is necessary to meet the requirements for certain Windows installations, including Windows 11.

Why Not B (Install an HSM): A Hardware Security Module (HSM) is a separate device used for cryptographic functions and is not related to TPM on the motherboard.

Why Not C (Perform a clean install): A clean installation will not bypass the TPM 2.0 requirement.

Why Not D (Implement BitLocker): BitLocker requires TPM but does not resolve its absence or lack of activation.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.4, BIOS/UEFI configuration.

Questions # 32:

A user reports slow internet browsing. The technician finds high CPU and memory usage, and pop-ups occur every minute. Which of the following should the technician do next?

Options:

A.

Escalate to the network team to check end-to-end connectivity.

B.

Download and install the latest drivers.

C.

Update the anti-malware signatures and scan the system.

D.



CertsMania

Check the wireless settings and validate the DHCP configuration.

Answer

C

Explanation

High resource usage along with frequent pop-ups are strong signs of a malware infection. The next logical step is to update anti-malware definitions and run a full scan to detect and remove threats.

Option A: Network performance is likely not the root cause as local system behavior points to malware.

Option B: Drivers affect hardware functionality; they don't resolve malware-related slowness.

Option D: DHCP issues usually cause IP conflicts or no network access, not CPU spikes or pop-ups.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 4.2: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.

Questions # 33:

An SAS RAID array has severely degraded and gone offline. A systems administrator examines the syslog, and the point of failure is not obvious. Which of the following techniques should the administrator use to identify the issue (Select two).

Options:

A.

Run a magnet over each drive.

B.

Check if one of the drives is not level

C.

Listen for clicking and grinding noises

D.

Check the OS logs

E.

Update the RAID controller firmware.

F.

Check the historical SMART data



CertsMania

Answer

C, F

Explanation

Clicking and grinding noises indicate mechanical drive failure.

SMART data provides insights into the health and status of drives, helping identify failing components in the RAID array.

Why Not A (Run a magnet): This would damage drives.

Why Not B (Check if one drive is not level): Physical leveling is irrelevant.

Why Not D (Check OS logs): OS logs may provide limited information for RAID arrays.

Why Not E (Update RAID controller firmware): While important, it does not diagnose drive failure.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 3.3, storage troubleshooting.

Questions # 34:



CertsMania

A user reports that a software application functioned as expected the previous day, but this morning, the user is unable to launch the application. Which of the following describe what the technician should do next?

Options:

A.

Research the symptoms

B.

Identify any changes the user has made

C.

Determine which steps need to be performed.

D.

Check the vendor's website for guidance.



CertsMania

Answer

B

Explanation

Identifying changes made to the system is the next step to troubleshoot why an application no longer launches, as recent changes often cause such issues.

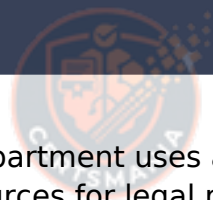
Why Not A (Research the symptoms): Research is broader and should come after identifying changes.

Why Not C (Determine which steps need to be performed): This comes after identifying the issue.

Why Not D (Check the vendor's website): This is a later step if further guidance is needed.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 3.1, troubleshooting methodology.

Questions # 35:



CertsMania

A human resources department uses a network shared with other departments to produce a variety of printed resources for legal retention. The human resources department only wants its members to have access to these materials. Which of the following should the technician implement?

Options:

A.

Security groups

B.

Audit logs

C.

Time-of-day access

D.

Print server

Answer

A

Explanation

Security groups are used to manage access permissions to network resources, ensuring only authorized HR department members can access the shared materials.

Why Not B (Audit logs): Audit logs monitor activity but do not restrict access.

Why Not C (Time-of-day access): Time-of-day access limits when users can access resources but doesn't specify user permissions.

Why Not D (Print server): A print server manages print jobs but does not control file access.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.5, access control and permissions.

Questions # 36:

When turning on a workstation, a technician observes the following message:

"Bootable device not found."

The technician verifies the correct boot order in the BIOS. Which of the following steps should the technician take next?

Options:

A.

Reformat the HDD.

B.

Run HDD diagnostics.

C.

Reseat the RAM.

D.

Replace the HDD.



CertsMania

Answer

B

Explanation

If the system reports “Bootable device not found”, and the BIOS is configured correctly, the next step is to run diagnostics on the hard drive to check for physical or logical failure. It could be a sign of a failing drive or corrupt boot sector.

Option A: Reformatting the drive would erase data not a diagnostic step.

Option C: RAM does not affect whether a drive is bootable.

Option D: Replacing the drive should only be done after diagnostics confirm failure.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.5: Given a scenario, troubleshoot problems related to storage devices.

Questions # 37:

A company is testing the latest model of a laptop. After turning on the laptop, there is a noticeable burning smell. Which of the following steps should a technician take to troubleshoot the laptop issue? (Select two).

Options:

A.

Turn it off and disconnect all power sources.

B.

Submit an emergency request to the local facilities manager.

C.

Check for foreign objects, liquid spills, and internal damage.

D.

Contact the vendor and submit a return request.

E.

Remove the device from the MDM.

F.

Try an alternate AC adapter.



CertsMania

Answer

A, C

Explanation

When a technician encounters a burning smell, it is a critical safety issue. The first response must be to immediately power down and disconnect the device from all power sources to prevent electric shock, fire, or further hardware damage.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 4.1 – Troubleshoot common hardware problems:

"Signs of electrical issues such as burning smells, smoke, or sparks require an immediate shutdown of the system and disconnection from any power source."

After ensuring safety, the technician should inspect the hardware for visible signs of damage:

From the same Objective (4.1):

"Inspect for foreign objects, liquid damage, or burnt components. These can cause short circuits or thermal events that may damage the motherboard or other internal components."

These steps are standard practice in the industry to ensure safe and accurate diagnosis of faulty devices. Trying a different adapter (Option F) may make the problem worse, and contacting vendors (Option D) comes after initial safety and inspection.

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Troubleshooting Hardware Problems

CompTIA Exam Objectives 220-1101, Domain 4.0 – Hardware and Network

Questions # 38:

A user keeps getting an error message when trying to print a letter. The printer is normally used to print cards and invitations. The user tries printing from a different computer, but the issue persists. Which of the following should the user do to resolve the issue?

Options:

A.

Print fewer pages.

B.

Print on card stock

C.

Replace the rollers.

D.

Change the paper tray setting.

Answer

D

Explanation

If a printer is set to use a special tray (for cards/invitations) but a different type of print job is attempted (like a letter), a paper tray setting mismatch can cause errors. Changing the tray setting to match the print media resolves the issue.

From CompTIA A+ 220-1101 Official Study Guide, Objective 4.3 – Troubleshooting printers:

“If print jobs fail when media type changes, verify and adjust the paper tray settings to match the required output.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 4: Printer Troubleshooting

CompTIA Exam Objectives 220-1101, Domain 4.3

=====

Questions # 39:

Which of the following has the best penetration through physical objects, such as walls?

Options:

A.

2.4GHz

B.

5GHz

C.

6GHz

D.

NFC

Answer

A

Explanation

2.4GHz Wi-Fi signals have better penetration through walls and other obstacles compared to 5GHz and 6GHz. Lower frequency waves (like 2.4GHz) travel farther and are less absorbed by physical barriers.

From the CompTIA A+ 220-1101 Official Study Guide, Objective 2.5 - Compare and contrast wireless networking protocols:

“The 2.4GHz frequency band offers greater range and better penetration through walls and obstacles than higher frequencies like 5GHz and 6GHz. Higher frequencies provide faster speeds but are more easily absorbed by walls.”

NFC (Near Field Communication) is not a Wi-Fi technology and works only over very short distances (a few centimeters).

Verified Source:

=====

Questions # 40:

Which of the following is a benefit of using a VLAN?

Options:

A.

It minimizes collision domains.

B.

It provides private access to cloud resources.

C.

It increases network address space.

D.

It enables secure network segmentation.

Answer

D

Explanation

A VLAN (Virtual Local Area Network) segments a physical network into separate logical networks, enhancing security by isolating traffic.

Why Not A (Minimizes collision domains): VLANs manage broadcast domains, not collision domains.

Why Not B (Provides private access to cloud resources): VLANs operate within a local network, not cloud-specific.

Why Not C (Increases network address space): VLANs do not affect address space.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 2.6, VLAN concepts.

Questions # 41:

A technician has discovered that some users are connected to a network that is not available on the user interface. Which of the following is the most effective tool the technician can use to identify networks that are not broadcasting SSIDs?

Options:

A.

Cable tester

B.

Toner probe

C.

Wi-Fi analyzer

D.

Loopback plug

Answer

C

Explanation

Comprehensive and Detailed Step-by-Step Explanation:

Wi-Fi Analyzer:

A Wi-Fi analyzer is a tool used to detect and analyze wireless networks, even those that are not broadcasting their SSIDs (hidden networks).

It provides detailed information about nearby networks, including signal strength, channel usage, and security protocols.

In this case, the Wi-Fi analyzer can identify the hidden networks that users are connected to, which are not visible on the standard user interface.

Incorrect Options:

A. Cable tester: A cable tester is used to test the integrity of physical network cables. It

does not detect wireless networks or SSIDs.

B. Toner probe: A toner probe is used to trace and identify cables within a wiring system. It is not applicable to wireless network analysis.

D. Loopback plug: A loopback plug is used to test the functionality of a network port or NIC. It is unrelated to identifying hidden wireless networks.

Key Takeaway:

The most effective tool for identifying hidden wireless networks is a Wi-Fi analyzer, as it can detect networks that are not broadcasting their SSIDs.

[Reference: CompTIA A+ Core 1 Exam Objectives (220-1201), Domain 2.5 – Explain basic wired and wireless networking concepts, including Wi-Fi tools and protocols., , , , , ,]

Questions # 42:

Which of the following statements best summarize managed vs unmanaged switches? (Select two).

Options:

A.

Unmanaged switches are generally more expensive

B.

Unmanaged switches have more security capabilities

C.

Unmanaged switches start working as soon as they are plugged in to the network

D.

Managed switches have more features

E.

Managed switches require no configuration

F.

Managed switches consume less power

Answer

C, D

Explanation

Unmanaged switches require no configuration they simply need to be plugged in and start working immediately, making them ideal for simple network setups.

Managed switches provide advanced features such as VLANs, SNMP monitoring, port security, and traffic management, but require configuration.

From CompTIA A+ 220-1101 Official Study Guide, Objective 2.2 – Compare and contrast common networking hardware:

“Unmanaged switches operate out of the box with no configuration and are designed for simple connectivity. Managed switches allow for configuration, monitoring, and management of network traffic and security.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 2: Networking Hardware

CompTIA Exam Objectives 220-1101, Domain 2.2

=====

Questions # 43:

An IT support specialist needs to configure several laptops to access local resources wherever the employees are while in the office. Which of the following would best meet this requirement?

Options:

A.

Configure cellular location services to facilitate device identification

B.

Set up a Wi-Fi connection with a common SSID

C.

Enable Bluetooth connectivity in all laptops

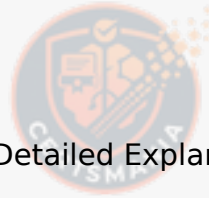
D.

Create roaming profiles for each laptop

Answer

B

Explanation



CertsMania

Comprehensive and Detailed Explanation (From CompTIA A+ 220-1201 Concepts):

A consistent Wi-Fi SSID across all APs allows users to roam throughout the office while maintaining access to local resources without reconnecting manually.

CompTIA Core 1 Study Guide Concept Reference:

Wireless networking configuration

SSID broadcast and roaming

WLAN infrastructure

The study guide explains that a common SSID enables seamless roaming and uninterrupted access to network resources.

Questions # 44:

An administrator is helping a new employee configure email on a smartphone. The employee also needs access to a shared mailbox. Which is the best email client for this situation?



CertsMania

Options:

A.

Open-source

B.

Built-in

C.

Corporate

D.

Employee preferred

Answer

C

Explanation



CertsMania

A corporate-provided email client is designed to integrate with enterprise services such as shared mailboxes, MDM policies, and enterprise authentication. CompTIA A+ states that corporate clients support additional management features, secure authentication protocols (such as OAuth or Kerberos), and policy-enforced access control essential for accessing shared or departmental mailboxes.

Open-source clients (Option A) may lack compatibility with enterprise environments. Built-in smartphone clients (Option B) often don't support complex mailbox structures such as shared mailboxes. Employee-preferred apps (Option D) are discouraged because they may not meet security requirements.

Corporate clients ensure full compatibility with organizational mail servers, shared folders, calendars, and enterprise security features, making corporate email clients the correct choice according to CompTIA's mobile device email configuration standards.

Questions # 45:

A network administrator must ensure that a printer will still be assigned a specific IP address even if all addresses are depleted. Which of the following network configuration concepts is this describing?

Options:

A.

VLAN

B.

Lease

C.

Reservation

D.



CertsMania

Exclusion

Answer

C

Explanation

A DHCP reservation binds a specific MAC address to an IP address so the device always receives the same IP from the DHCP server. This ensures network devices like printers maintain consistent connectivity and availability even when the IP pool is low.

[Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter - Chapter 18, page 1252., , , , ,]

Questions # 46:

A company uses vital legacy software that does not run in the current OS version Which of the following will best support the software while keeping the OS current?

Options:

A.

Shared resources

B.

System sandbox

C.

Test development

D.

Application virtualization

Answer

D

Explanation

Application virtualization allows legacy software to run in a virtualized environment while

the operating system remains current. It isolates the application from the OS, ensuring compatibility without downgrading the OS.

Why Not A (Shared resources): This relates to resource sharing, not application compatibility.

Why Not B (System sandbox): Sandboxes isolate applications for security testing, not compatibility.

Why Not C (Test development): Test environments are used for development, not running legacy applications.

CompTIA A+ Exam Reference: Core 1 (220-1201), Section 4.2, virtualization concepts.

Questions # 47:

Which of the following can a user utilize to share their mobile phone connection with their laptop?

Options:

A.

IR

B.

NFC

C.

Wi-Fi Direct

D.

Tethering

Answer

D

Explanation

Tethering refers to sharing a mobile phone's internet connection with another device, such as a laptop, either through USB, Bluetooth, or Wi-Fi. Tethering effectively turns the mobile phone into a personal hotspot for internet access.

Option A (IR): Incorrect. Infrared (IR) is used for short-range communication, such as remote controls, but it does not support internet sharing.

Option B (NFC): Incorrect. Near-field communication (NFC) is used for close-proximity data transfer, not for internet sharing.

Option C (Wi-Fi Direct): Incorrect. Wi-Fi Direct enables device-to-device communication but does not inherently provide internet sharing.

[References:, CompTIA A+ Core 1 Objectives: 1.4 (Configure basic mobile-device network connectivity), , , , , , ,]

Questions # 48:

A user wants to print files from an overseas office using a shared network folder. The user's laptop has no public-facing internet connectivity. Which of the following can be used to print from the shared network folder?

Options:

A.

ADF

B.

USB

C.

PCL

D.

SMB

Answer

D

Explanation

SMB (Server Message Block) is a protocol used to access files and printers over a network, including across shared network folders. It enables the user to access and print files stored remotely on a shared directory.

Option A (ADF): Automatic Document Feeder hardware, not a network protocol.

Option B (USB):Used for direct physical connections, not for printing over networks.

Option C (PCL):Printer Command Language relates to printer drivers, not file sharing or access.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.4: Given a scenario, install and configure printers.

Questions # 49:

A salesperson is unable to use a personal device to access emails and calendar features at a client site but was able to use the device while at the office. Which of the following policies has been enforced on the salesperson's mobile device?

Options:

A.

MOW

B.

MAN

C.

MFA

D.

MAM

Answer

D

Explanation

Mobile Application Management (MAM) enforces policies restricting access to apps and services based on location, ensuring security at external sites.

Why Not A (MOW): "Mobile Only Workplace" (MOW) is not a recognized term in this context.

Why Not B (MAN): Metropolitan Area Network (MAN) is unrelated to mobile device policies.

Why Not C (MFA): Multi-Factor Authentication secures user accounts but does not enforce app restrictions.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.7, mobile device security policies.

Questions # 50:

Which of the following virtualization technologies is best suited for running microservices?

Options:

A.

Containers

B.

VDI

C.

Type 2 hypervisors

D.

Type 1 hypervisors

Answer

A

Explanation

Containers provide lightweight virtualization, ideal for deploying microservices because they are isolated, portable, and require fewer resources than traditional VMs.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.7 - Virtualization and cloud computing:

“Containers package applications and their dependencies, making them ideal for running microservices efficiently and independently.”

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: Cloud and Virtualization

=====

Questions # 51:

A customer reports that a workstation has no internet connectivity. A technician confirms the port is disabled. Which of the following is most likely responsible for the issue?

Options:

- A.
Patch panel
- B.
Physical NIC
- C.
Managed switch
- D.
Stand-alone firewall

Answer

C

Explanation

A managed switch allows an administrator to enable or disable individual ports as part of network security and management. If a port on a managed switch has been disabled, the device connected to that port will lose connectivity, which matches the scenario described.

[Reference: CompTIA A+ Certification Exam Core 1 Objectives - Domain 2.0 Networking - Objective 2.2: Compare and contrast common networking hardware devices., , ,]

Questions # 52:

A student configures a wireless SOHO network to connect four laptops and one multifunction printer. All laptops must have internet access and be able to use the printer. Which of the following settings ensures the printer is always available?

Options:

A.

Configure dynamic IPs for the laptops and a static IP for the printer on the same subnet.

B.

Manually assign IP addresses to the laptops and printer based on the public IP from the ISP.

C.

Use APIPA for laptops and connect the printer to the ISP router.

D.

Use dynamic IP addresses from the ISP router for all the devices.

Answer

A

Explanation

Comprehensive and Detailed Explanation (100–150+ Words):

CompTIA A+ stresses that printers must use static IP addresses to remain consistently reachable on a LAN. When using DHCP, the printer's IP address may change, causing laptops to lose access. By assigning a static IP within the same subnet, the printer becomes a stable, discoverable network resource for all laptops.

Using dynamic IPs for the laptops is perfectly acceptable in SOHO environments, because clients don't require permanent IPs. Assigning public IPs (Option B) is incorrect and unsafe. APIPA (169.254.x.x) does not route and cannot reach the internet or a standard printer. Using dynamic ISP-assigned IPs for all devices (Option D) is also incorrect because ISP routers typically give only one public IP, not multiple internal ones.

Therefore, to ensure the printer is always reachable, the correct configuration is: DHCP for laptops, static IP for printer a best practice detailed in CompTIA's networking and SOHO setup guidelines.

A technician needs to troubleshoot a user's smartphone that will not connect to its wireless provider's service. Which of the following should the technician check first?

Options:

- A.
SIM card
- B.
Network settings
- C.
Subscription plan
- D.
Bluetooth connection



CertsMania

Answer

C

Questions # 54:

A group of friends is gathering in a room to play video games. One of the friends has a game server. Which of the following network types should the group use so they can all connect to the same server and the internet?

Options:

- A.
SAN
- B.
MAN
- C.
LAN



CertsMania

D.

PAN

Answer

C

Explanation



CertsMania

The appropriate network type for this scenario is a Local Area Network (LAN), which is designed for small, localized networks, such as within a single building or room. LANs are ideal for gaming because they provide high-speed, low-latency connections.

Option A (SAN): Incorrect. A Storage Area Network is used for data storage, not for gaming or general networking.

Option B (MAN): Incorrect. A Metropolitan Area Network covers a city or campus, far exceeding the scope needed for a gaming setup in a single room.

Option D (PAN): Incorrect. A Personal Area Network is designed for a single user, such as Bluetooth devices, and would not support multiple devices connecting to a game server.

[References:, CompTIA A+ Core 1 Objectives: 2.7 (Compare and contrast network types and features), , , , , ,]

Questions # 55:

A network operations analyst receives an automated alert regarding a server with an array. The analyst walks over to the server and sees a blinking orange light at the hard disk bay. The server is configured for RAID 1. Which of the following should the analyst do to resolve this issue?



CertsMania

Options:

A.

Change the array to RAID 0.

B.

Undo the array and create a new one.

C.

Update RAID card firmware.

D.

Replace the hard disk and rebuild the array.

Answer

D

Explanation



CertsMania

A blinking orange light typically indicates a failed hard drive in the RAID array. In RAID 1 (mirroring), you can replace the failed drive and rebuild the array without data loss.

From CompTIA A+ 220-1101 Official Study Guide, Objective 3.4 – RAID configuration and troubleshooting:

"In the event of a hard drive failure in RAID 1, replace the failed disk and allow the array to rebuild using the remaining mirrored disk."

Verified Source:

CompTIA A+ Core 1 (220-1101) Official Study Guide, Chapter 3: RAID and Storage

CompTIA Exam Objectives 220-1101, Domain 3.4

=====

Questions # 56:

A user is receiving many unsolicited emails. Which of the following controls can be configured to best reduce these types of emails?

Options:

A.

Load balancer

B.

Spam gateway

C.

Mail forwarding



CertsMania

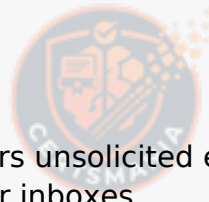
D.

Proxy servers

Answer

B

Explanation



CertsMania

A spam gateway filters unsolicited emails at the server level, significantly reducing spam before it reaches user inboxes.

Why Not A (Load balancer): Load balancers distribute traffic but don't filter spam.

Why Not C (Mail forwarding): Forwarding doesn't filter spam.

Why Not D (Proxy servers): Proxies control web traffic, not email filtering.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.10, email security controls.

Questions # 57:

A thief stole a company phone and successfully extracted confidential company information from the device. Which of the following should have been used to prevent the extraction?

Options:

A.

GPS

B.

EPS

C.

eSIM

D.

MDM



CertsMania

Answer

D

Explanation

Comprehensive and Detailed Explanation From Exact Extract:

MDM (Mobile Device Management) enforces security policies, such as encryption, remote wipe, and access control. It could have remotely wiped the device or locked it down to prevent data theft.

[Reference: CompTIA A+ Core 1 220-1201 Official Study Guide, Section: Mobile Device Security MDM tools provide remote wipe and security policy enforcement, essential for protecting mobile data., , ,]

Questions # 58:

A security team wants to implement compliance controls that only permits the installation of company-approved software on user laptops. Which of the following should the IT department deploy?

Options:

A.

EDR

B.

VPN

C.

MDM

D.

SaaS

Answer

C

Explanation

Mobile Device Management (MDM) allows IT departments to enforce compliance controls,

such as restricting the installation of unapproved software, on laptops and mobile devices.

Why Not A (EDR): Endpoint Detection and Response focuses on detecting and mitigating security threats, not compliance controls.

Why Not B (VPN): Virtual Private Networks provide secure connections but do not enforce software installation policies.

Why Not D (SaaS): Software as a Service refers to software delivery models and does not enforce compliance controls.

CompTIA A+ Exam Reference: Core 2 (220-1102), Section 2.7, device management and security.

Questions # 59:

A company deploys server machines in a public cloud. Which of the following cloud service models is this an example of?

Options:

A.

Platform as a service

B.

Anything as a service

C.

Infrastructure as a service

D.

Software as a service

Answer

C

Explanation

Infrastructure as a Service (IaaS) provides virtualized computing resources over the internet. This includes virtual servers, storage, and networking. Deploying server machines falls under IaaS since the organization is responsible for managing the OS and

applications on top of the infrastructure.

[Reference: "CompTIA A+ Complete Study Guide" by Quentin Docter - Chapter 8, "Virtualization and Cloud Computing", page 488-490. Also found in the 220-1201 objectives, section 4.1., , , , , ,]

Questions # 60:

A technician needs to select PC components with a minimal number of visible internal cables. Which of the following should the technician use?

Options:

A.

SATA drive connections

B.

Liquid cooling

C.

Modular power supply

D.

Wireless NIC

Answer

C

Explanation

A modular power supply allows a technician to connect only the power cables that are needed, reducing clutter and improving airflow. This is ideal when aiming for a clean build with minimal visible internal cables.

Option A (SATA drive connections): Still require both power and data cables, adding to cable count.

Option B (Liquid cooling): May reduce some bulk from large air coolers, but adds tubing and still needs cabling.

Option D (Wireless NIC): Adds wireless capability but has no relation to internal cabling cleanliness.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 3.3: Given a scenario, apply the appropriate PC configuration.

Questions # 61:

Which of the following technologies best allows a phone to connect to a point-of-sale terminal for wireless payments?

Options:

A.

Bluetooth

B.

NFC

C.

Wi-Fi

D.

Cellular

Answer

B

Explanation

Near-field communication (NFC) is a short-distance wireless communication method widely used in mobile payment systems like Apple Pay and Google Pay. Simply placing the device near a compatible terminal initiates the payment process.

[Reference: "Mike Meyers' CompTIA A+ Certification All-in-One Exam Guide" - Chapter 24, page 1022., , , , ,]

Questions # 62:

A technician is troubleshooting stylus issues on identical, company-provided tablets. Users can

purchase their own accessories. Some users have no issues, but others report that their styluses charge intermittently and die frequently. Which of the following is the most likely cause of this issue?

Options:

A.

Certain cases are causing charging issues.

B.

The tablets need to be updated.

C.

Some of the tablets have manufacturing defects.

D.

The malfunctioning styluses need firmware updates.

Answer

A

Explanation

The most likely cause is third-party or ill-fitting cases obstructing the contact between the stylus and the tablet charging mechanism. Some cases may not be designed with stylus charging in mind, particularly if users are purchasing their own accessories.

Option B: A software update might fix OS-related issues, but would not typically affect physical charging.

Option C: If some devices had defects, the issue would likely be consistent, not isolated to some users.

Option D: Firmware issues could be a factor but are less likely than physical obstructions when users are using different accessories.

CompTIA A+ Core 1 Exam Objective Reference:

Objective 1.4: Given a scenario, configure settings and use cases for laptops and mobile devices.

To Get Premium Files for 220-1201 Visit

<https://www.certsmania.com/comptia/220-1201-practice>

For More Free Questions Visit

<https://www.certsmania.com/comptia/pdf/220-1201>



CertsMania