CompTIA

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

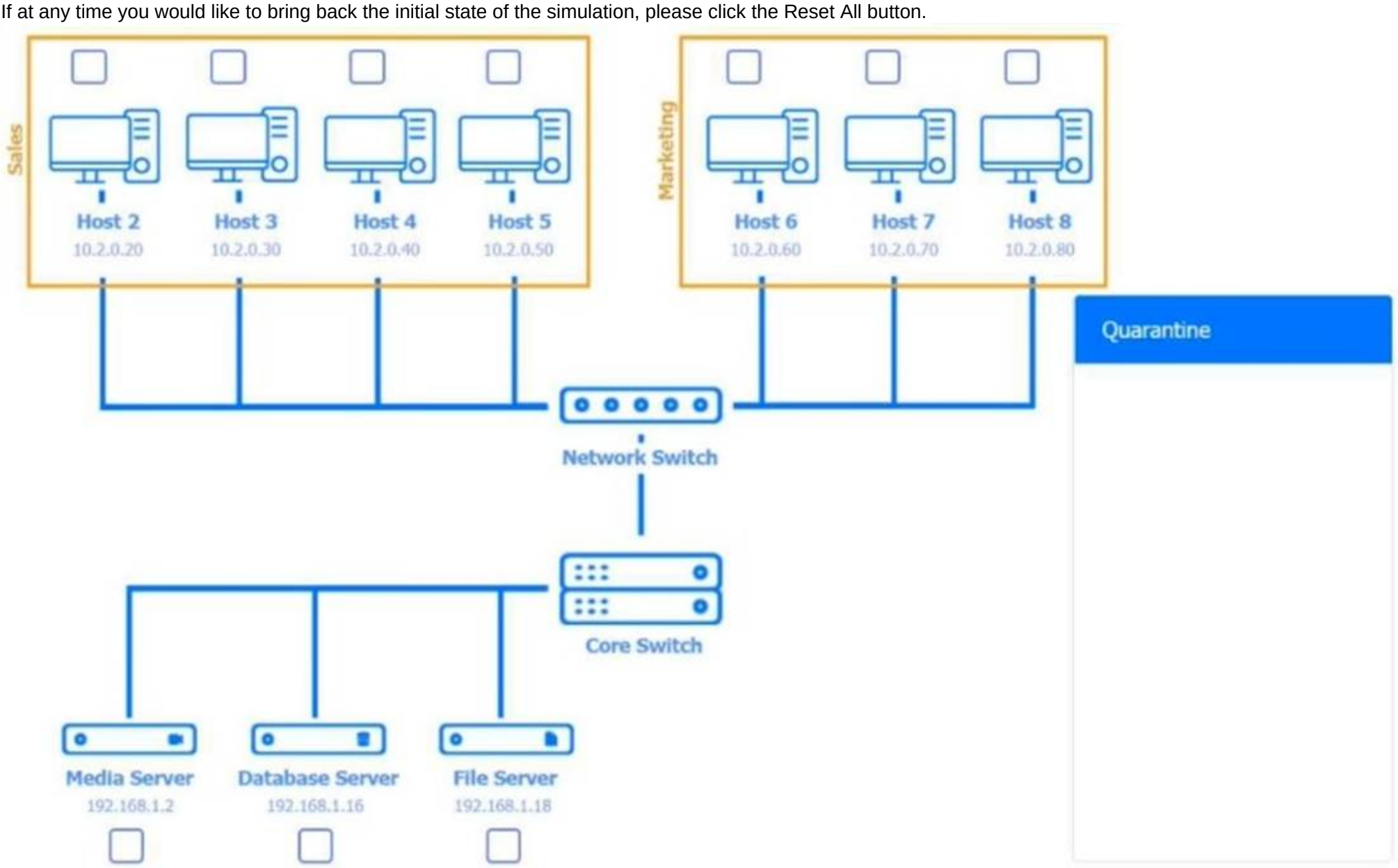
NEW QUESTION 1
Every time a user loads a specific spreadsheet, their computer is temporarily unresponsive. The user also notices that the title bar indicates the application is not responding. Which of the following would a technician most likely inspect?

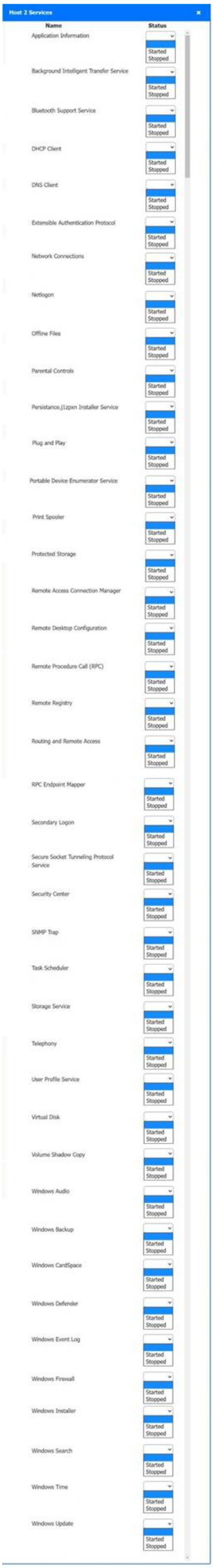
A. Anti-malware logs
B. Workstation repair options
C. Bandwidth status as reported in the Task Manager
D. File size and related memory utilization

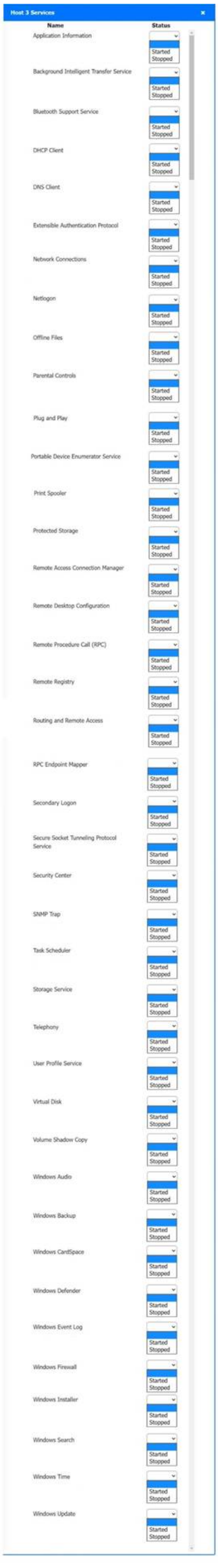
Answer: D

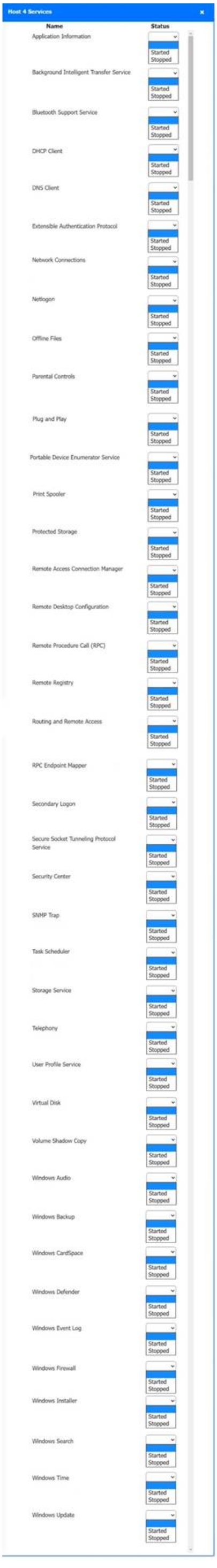
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
If a system becomes unresponsive while opening a specific spreadsheet, the issue is likely tied to the file??s size or the complexity of its content (e.g., embedded formulas, macros, or graphics). High memory utilization caused by the file can lead to temporary freezing or application "Not Responding" messages. Checking the spreadsheet's file size and monitoring system memory in Task Manager will help isolate performance bottlenecks.
* A. Anti-malware logs are important for security troubleshooting but less likely relevant to spreadsheet-related performance issues.
* B. Workstation repair is for system-wide problems and not necessary for a single-file issue.
* C. Bandwidth relates to network usage and wouldn??t impact opening a local file. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common application issues.
Study Guide Section: Troubleshooting application slowness and performance using Task Manager and resource monitoring tools
==========

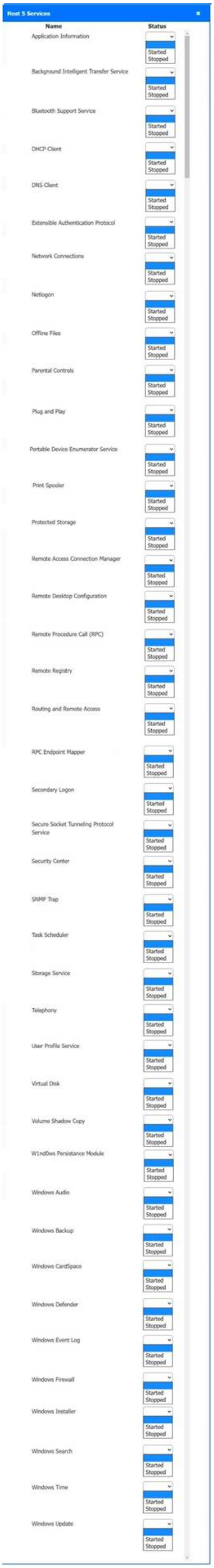
NEW QUESTION 2
SIMULATION
Multiple users are reporting audio issues as well as performance issues after downloading unauthorized software. You have been dispatched to identify and resolve any issues on the network using best practice procedures.
INSTRUCTIONS
Quarantine and configure the appropriate device(s) so that the users?? audio issues are resolved using best practice procedures.
Multiple devices may be selected for quarantine. Click on a host or server to configure services.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

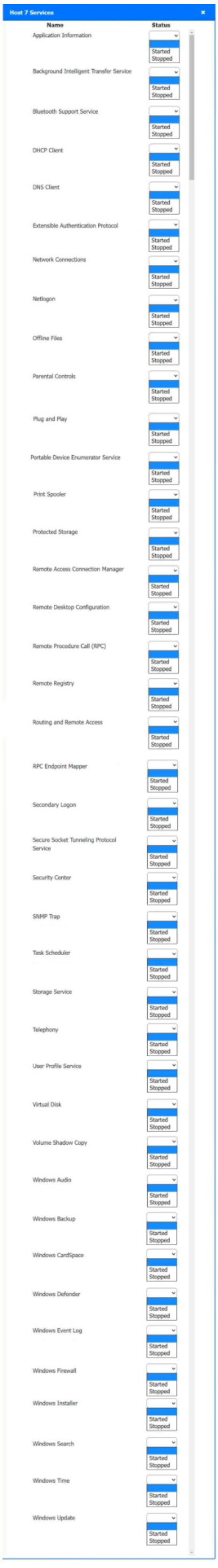


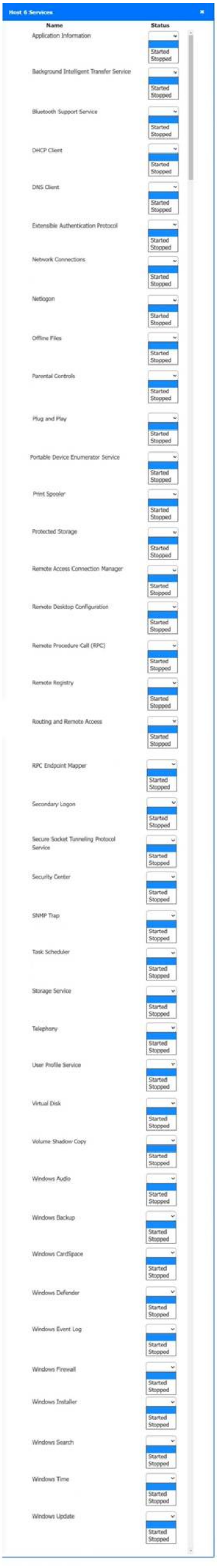

Host 2 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Persistance.j1zpxn Installer Service
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped

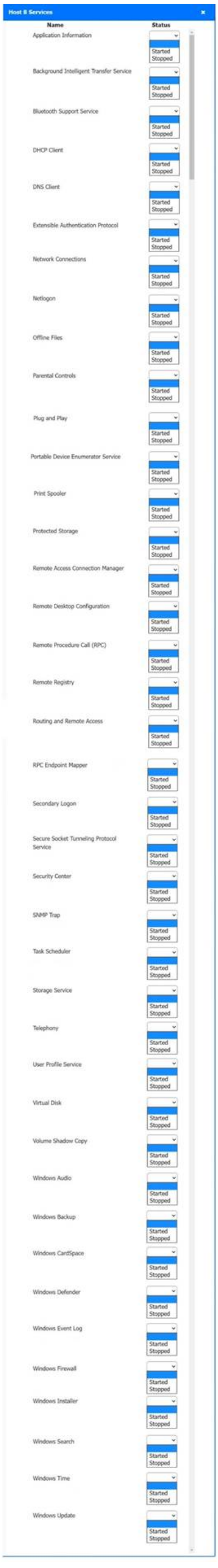

Host 3 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped

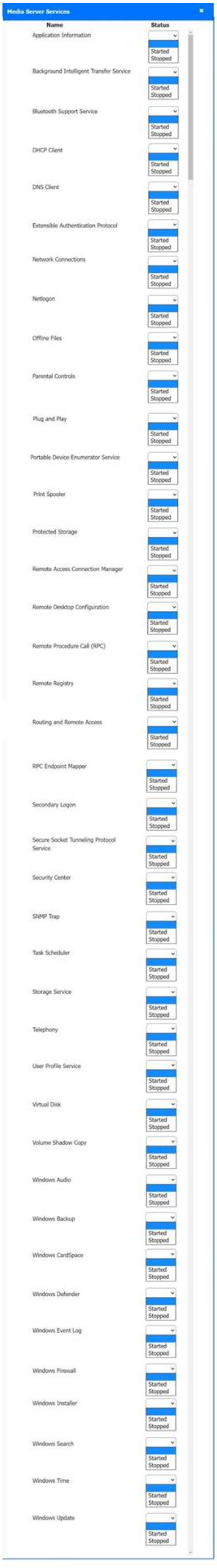

Host 4 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped

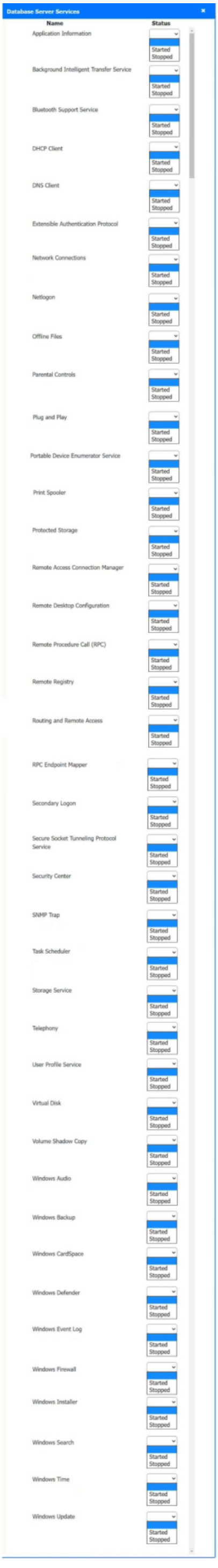

Host 5 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
W1nd0ws Persistance Module
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped

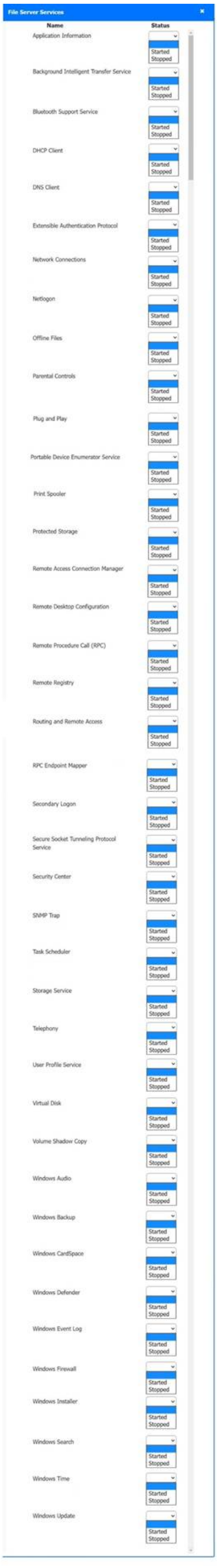

Host 7 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped


Host 6 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped


Host 8 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped


Media Server Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped


Database Server Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped


File Server Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected Storage
Remote Access Connection Manager
Remote Desktop Configuration
Remote Procedure Call (RPC)
Remote Registry
Routing and Remote Access
RPC Endpoint Mapper
Secondary Logon
Secure Socket Tunneling Protocol Service
Security Center
SNMP Trap
Task Scheduler
Storage Service
Telephony
User Profile Service
Virtual Disk
Volume Shadow Copy
Windows Audio
Windows Backup
Windows CardSpace
Windows Defender
Windows Event Log
Windows Firewall
Windows Installer
Windows Search
Windows Time
Windows Update
Started
Stopped

A. Mastered
B. Not Mastered

Answer: A

Explanation:
Host 2, Host 3, Host 4 , Host 5 ,Host 6, Host 7, Host 8 , Media Server - Stop All unwanted and malicious service (Persistance.j1zpxn Installer Service) from all the listed host and Media servers
Refer screenshot below on the required service started/stopped on host2, same service to be started and stopped across all host servers.

NEW QUESTION 3
After a recent mobile OS upgrade to a smartphone, a user attempts to access their corporate email, but the application does not open. A technician restarts the smartphone, but the issue persists. Which of the following is the most likely way to resolve the issue?

A. Updating the failed software
B. Registering the smartphone with an MDM solution
C. Installing a third-party client
D. Clearing the cache partition

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Mobile OS updates can sometimes cause compatibility issues with specific apps, including corporate email clients. The most likely resolution is to check for and apply an update to the affected application, especially if it hasn??t been updated to support the latest OS version.
* B. Registering with MDM might be required for access but wouldn??t address app crashes due to incompatibility.
* C. A third-party client might help, but it??s not the best first step if the default app is expected to work.
* D. Clearing the cache can help resolve some minor issues, but updating the app directly addresses compatibility concerns.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot mobile OS and application issues. Study Guide Section: App compatibility and mobile software updates
==========

NEW QUESTION 4
A technician uses AI to draft a proposal about the benefits of new software. When reading the draft, the technician notices that the draft contains factually incorrect information. Which of the following best describes this scenario?

A. Data privacy
B. Hallucinations
C. Appropriate use
D. Plagiarism

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
In the context of artificial intelligence, "hallucinations" refer to instances where an AI system generates information that is plausible-sounding but factually incorrect or entirely fabricated. This is a known limitation of large language models, including generative AI tools.
* A. Data privacy refers to the protection of personal or sensitive data, not content accuracy.
* C. Appropriate use relates to ethical and policy-based concerns, not factual correctness.
* D. Plagiarism involves presenting someone else's work as your own — this situation is about accuracy, not ownership.
Reference:
CompTIA A+ 220-1102 Objective 4.4: Identify basic concepts of scripting and automation. Study Guide Section: AI tools and responsible usage — hallucinations and fact-checking outputs
==========

NEW QUESTION 5
A small office reported a phishing attack that resulted in a malware infection. A technician is investigating the incident and has verified the following:
All endpoints are updated and have the newest EDR signatures.
Logs confirm that the malware was quarantined by EDR on one system. The potentially infected machine was reimaged.
Which of the following actions should the technician take next?

A. Install network security tools to prevent downloading infected files from the internet
B. Discuss the cause of the issue and educate the end user about security hygiene
C. Flash the firmware of the router to ensure the integrity of network traffic
D. Suggest alternate preventative controls that would include more advanced security software

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
After containment and remediation, one of the final steps in incident response is user education. Since the root cause was a phishing attack, it is essential to educate users about identifying phishing attempts, safe browsing practices, and how to handle suspicious communications. This improves overall security posture and helps prevent future incidents.
* A. Installing additional tools may be helpful but is a long-term step.
* C. Flashing router firmware is not warranted unless the network hardware is known to be compromised.
* D. Suggesting more advanced tools might be excessive given that the EDR successfully contained the incident.
Reference:

CompTIA A+ 220-1102 Objective 2.5: Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.
Study Guide Section: Incident response and user education after a security event

NEW QUESTION 6
A technician needs to map a shared drive from a command-line interface. Which of the following commands should the technician use?

A. pathping
B. nslookup
C. net use
D. tracert

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The net use command in Windows is used to map (assign) a shared drive from the command line. The syntax typically looks like: net use X: \server\share where X is the drive letter and \server\share is the network path.
* A. pathping tests network latency and packet loss.
* B. nslookup is used for DNS troubleshooting.
* D. tracert shows the route packets take to reach a destination — not for drive mapping. Reference:
CompTIA A+ 220-1102 Objective 1.7: Given a scenario, troubleshoot common operating system problems.
Study Guide Section: Command-line tools — net use for drive mapping
==========

NEW QUESTION 7
Which of the following prevents forced entry into a building?

A. PIV card
B. Motion-activated lighting
C. Video surveillance
D. Bollard

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A bollard is a sturdy physical barrier—often a steel or concrete post—designed to prevent
vehicles or unauthorized individuals from ramming into or entering secure areas of a building. It provides physical security and is commonly used outside entrances to prevent forced entry.
* A. PIV (Personal Identity Verification) cards are used for identity access control, not physical blocking.
* B. Motion lighting may deter activity but doesn??t physically prevent entry.
* C. Surveillance records activity but cannot stop a forced entry. Reference:
CompTIA A+ 220-1102 Objective 2.4: Compare and contrast physical security measures. Study Guide Section: Physical security devices — barriers, bollards, and deterrents

NEW QUESTION 8
Which of the following is found in an MSDS sheet for a battery backup?

A. Installation instructions
B. Emergency procedures
C. Configuration steps
D. Voltage specifications

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An MSDS (Material Safety Data Sheet), now commonly referred to as SDS (Safety Data Sheet), is a document that provides detailed information on the properties of a particular substance. It includes safety guidelines and emergency procedures related to handling, exposure, fire hazards, and first aid—not installation or configuration instructions.
For a battery backup (UPS device), the MSDS would include emergency procedures such as what to do in case of a chemical spill, exposure to battery acid, or fire hazard due to overheating or chemical leakage. This ensures the safety of personnel and complies with hazardous materials handling regulations.
Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information management.
Study Guide Section: MSDS/SDS usage and safety documentation

NEW QUESTION 9
A technician is deploying mobile devices and needs to prevent access to sensitive data if the devices are lost. Which of the following is the best way to prevent unauthorized access if the user is unaware that the phone is lost?

A. Encryption
B. Remote wipe
C. Geofencing
D. Facial recognition

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:

Remote wipe is the best option to prevent unauthorized access to data when a mobile device is lost or stolen—especially if the user is unaware of the loss. It allows administrators or mobile device management (MDM) systems to remotely erase all data on the device, rendering it unusable for unauthorized users.
* A. Encryption protects the data, but if the device remains powered and logged in, it may still be accessible.
* C. Geofencing can restrict features based on location but does not erase data.
* D. Facial recognition helps secure access but can be bypassed in some cases or fail in practical situations.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools. Study Guide Section: Mobile device security (remote wipe, lockout, MDM tools)

NEW QUESTION 10
A customer is unable to open some files on their system. Each time the customer attempts to open a file, the customer receives a message that the file is encrypted. Which of the following best describes this issue?

A. Keylogger
B. Ransomware
C. Phishing
D. Cryptominer

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Ransomware is a type of malware that encrypts the user's files and demands a payment (ransom) for the decryption key. When a user receives a message stating that their files are encrypted and cannot be accessed, ransomware is the most likely cause. The attacker??s goal is to hold the data hostage until the victim pays to restore access.
* A. Keylogger records keystrokes and doesn??t encrypt files.
* C. Phishing is a social engineering tactic to gather credentials, not to encrypt data.
* D. Cryptominer uses system resources to mine cryptocurrency, not encrypt files. Reference:
CompTIA A+ 220-1102 Objective 2.3: Compare and contrast common types of malware and threats.
Study Guide Section: Ransomware behavior and user impact
==========

NEW QUESTION 10
A company recently transitioned to a cloud-based productivity suite and wants to secure the environment from external threat actors. Which of the following is the most effective method?

A. Multifactor authentication
B. Encryption
C. Backups
D. Strong passwords

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multifactor authentication (MFA) is considered one of the most effective security measures for cloud environments. It requires users to verify their identity using two or more factors (e.g., password + phone app code), making it significantly harder for external attackers to gain access, even if the primary password is compromised.
* B. Encryption is important for data protection but doesn??t prevent unauthorized logins.
* C. Backups protect against data loss but don??t stop breaches.
* D. Strong passwords are helpful but can still be phished or cracked — MFA adds a critical
extra layer. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication technologies. Study Guide Section: Cloud security best practices — MFA and access control

NEW QUESTION 15
Which of the following filesystem types does the Linux OS use?

A. exFAT
B. APFS
C. ext4
D. NTFS

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The ext4 (Fourth Extended Filesystem) is the most widely used default filesystem in modern Linux distributions. It is designed for high performance, scalability, and reliability, and is supported by all mainstream Linux kernels.
* A. exFAT is used for cross-platform external drives, not native Linux systems.
* B. APFS is Apple's proprietary filesystem for macOS and iOS.
* D. NTFS is the default filesystem for Windows, not Linux. Reference:
CompTIA A+ 220-1102 Objective 1.9: Identify common features and tools of the Linux client/desktop OS.
Study Guide Section: Filesystem types in Linux — ext3, ext4, and their characteristics

NEW QUESTION 19
A company executive is currently attending a major music festival with a large number of attendees and is having trouble accessing a work email account. The email application is not downloading emails and also appears to become stuck during connection attempts. Which of the following is most likely causing the disruption?

A. The phone has no storage space available.
B. Company firewalls are configured to block remote access to email resources.
C. Too many devices in the same area are trying to connect to the mobile network.
D. The festival organizer prohibits internet usage during the event and has blocked the internet signal

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
At large events such as music festivals, cellular towers may become congested due to the high volume of users attempting to connect simultaneously. This congestion causes slow or failed data connections, which explains the email application being unable to sync or connect. This is a common real-world mobile connectivity issue in crowded areas.
* A. Lack of storage would prevent saving attachments, not prevent connection attempts.
* B. Company firewalls usually don??t affect mobile access unless specific device restrictions are enforced.
* D. Organizers do not have the ability to block the internet signal; only carriers manage mobile bandwidth.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot mobile OS and connectivity issues. Study Guide Section: Mobile network limitations — signal congestion and bandwidth issues
==========

NEW QUESTION 21
An employee is using a photo editing program. Certain features are disabled and require a log-in, which the employee does not have. Which of the following is a way to resolve this issue?

A. License assignment
B. VPN connection
C. Application repair
D. Program reinstallation

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Many modern commercial software applications (including photo editors like Adobe Photoshop) offer tiered features based on user subscriptions or license levels. If certain features are locked and prompt for a login, the issue is likely due to a missing or unassigned software license. Assigning the correct license through a centralized license management system (such as Adobe Admin Console or Microsoft 365 portal) will enable those features.
* B. VPN connection does not affect local software licensing.
* C. Repairing the application does not resolve license entitlement.
* D. Reinstalling the software won??t help unless the license is assigned. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software and application issues.
Study Guide Section: Troubleshooting licensing and access control for applications
==========

NEW QUESTION 23
A user receives a new personal computer but is unable to run an application. An error displays saying that .NET Framework 3.5 is required and not found. Which of the following actions is the best way to resolve this issue?

A. Resolve the dependency through the 'Turn Windows features on or off' menu.
B. Download the dependency via a third-party repository.
C. Ignore the dependency and install the latest version 4 instead.
D. Forward the trouble ticket to the SOC team because the issue poses a great security risk.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
NET Framework versions are often required for applications to run. If an older app requires
.NET Framework 3.5, it must be explicitly installed as it is not included by default in newer versions of Windows. The best method to do this safely is through the built-in "Turn Windows features on or off" utility, which downloads and installs it via official Microsoft services.
* B. Using third-party repositories is unsafe and not recommended.
* C. Installing .NET 4 does not include 3.5; versions are not fully backward compatible.
* D. The issue is technical, not a security incident for the SOC team. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.
Study Guide Section: Managing application dependencies (e.g., .NET Framework, Java)
==========

NEW QUESTION 28
Users are reporting that an unsecured network is broadcasting with the same name as the
normal wireless network. They are able to access the internet but cannot connect to the file share servers. Which of the following best describes this issue?

A. Unreachable DNS server
B. Virtual local area network misconfiguration
C. Incorrect IP address
D. Rogue wireless access point

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
This scenario describes a rogue access point — a malicious or unauthorized wireless access point that uses the same SSID as the legitimate network. Users may

connect to it unknowingly, which can result in limited network access, data interception, or redirection of traffic. The inability to reach internal file servers supports this being an unauthorized AP with no connection to internal resources.
* A. A DNS issue would impact name resolution, not connectivity to file servers directly.
* B. VLAN issues generally affect segmentation, not mimic SSID problems.
* C. An incorrect IP address could cause connectivity issues, but not in the presence of a malicious AP broadcasting the same SSID.
Reference:
CompTIA A+ 220-1102 Objective 2.4: Compare and contrast wireless and physical security threats.
Study Guide Section: Rogue access points and their detection
==========

NEW QUESTION 29
A technician is preparing to replace the batteries in a rack-mounted UPS system. After ensuring the power is turned off and the batteries are fully discharged, the technician needs to remove the battery modules from the bottom of the rack. Which of the following steps should the technician take?

A. Ensure the fire suppression system is ready to be activated.
B. Use appropriate lifting techniques and guidelines.
C. Place the removed batteries in an antistatic bag.
D. Wear a face mask to filter out any harmful fumes.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
UPS batteries are heavy and often located at the bottom of racks to maintain balance. Safe removal requires the use of correct lifting techniques to avoid injury. OSHA and workplace safety standards emphasize ergonomic handling when dealing with heavy equipment.
* A. Fire suppression readiness is important for fire safety but not specifically relevant to battery removal.
* C. Antistatic bags are for electronic components, not heavy battery modules.
* D. A face mask is not generally necessary unless there is a chemical leak, which is not indicated here.
Reference:
CompTIA A+ 220-1102 Objective 4.3: Explain common safety and environmental impacts and procedures.
Study Guide Section: Safe handling procedures — lifting techniques, battery handling
==========

NEW QUESTION 31
An administrator received an email stating that the OS they are currently supporting will no longer be issued security updates and patches. Which of the following is most likely the reason the administrator received this message?

A. Support from the computer's manufacturer is expiring
B. The OS will be considered end of life
C. The built-in security software is being removed from the next OS version
D. A new version of the OS will be released soon

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Operating systems periodically reach a status known as "end of life" (EOL), at which point the developer (e.g., Microsoft, Apple) ceases to provide security updates, patches, or technical support. When this happens, the OS becomes vulnerable and non-compliant with security best practices, which is why organizations typically receive advance notifications from vendors or support teams.
* A. Manufacturer support expiration only applies to hardware, not OS patching.
* C. Security software may be upgraded or removed, but that does not affect patching the OS itself.
* D. The release of a new version doesn??t automatically stop updates for the current version. Reference:
CompTIA A+ 220-1102 Objective 1.3: Given a scenario, use appropriate Microsoft operating system features and tools.
Study Guide Section: OS lifecycle management and vendor support phases (e.g., EOL)
==========

NEW QUESTION 34
Which of the following is used to detect and record access to restricted areas?

A. Bollards
B. Video surveillance
C. Badge readers
D. Fence

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Badge readers are electronic access control systems that require authorized users to scan a badge (e.g., RFID or magnetic strip cards) to gain access to restricted physical locations. These systemstypically log all access attempts—successful or denied—providing both detection and recording of access events.
* A. Bollards are physical barriers to prevent vehicle access.
* B. Video surveillance can record access visually but does not track identity unless integrated with access control systems.
* D. A fence restricts access but doesn't detect or record who entered. Reference:
CompTIA A+ 220-1102 Objective 2.4: Compare and contrast physical security measures.
Study Guide Section: Physical access controls (e.g., badge readers, mantraps)

NEW QUESTION 39
An organization is experiencing an increased number of issues. A technician notices applications that are not installed by default. Users are reporting an increased

number of system prompts for software licensing. Which of the following would the security team most likely do to remediate the root cause?

A. Deploy an internal PKI to filter encrypted web traffic.
B. Remove users from the local admin group.
C. Implement stronger controls to block suspicious websites.
D. Enable stricter UAC settings on Windows.

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
If unauthorized or non-standard applications are appearing on systems and users are receiving licensing prompts, it??s likely users are installing software themselves. Removing users from the local administrators group will prevent them from installing software without approval and reduce the likelihood of introducing unapproved or malicious programs.
* A. Deploying a PKI helps with secure communications but doesn??t address user software installation rights.
* C. Blocking suspicious websites is helpful but doesn??t prevent local installations.
* D. Stricter UAC may add prompts but can still be bypassed by admin users. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast access control methods and user privilege settings.
Study Guide Section: Principle of least privilege and managing local admin rights
==========

NEW QUESTION 42
A technician is setting up a surveillance system for a customer. The customer wants access to the system's web interface on the LAN via the system??s IP address. Which of the following should the technician use to prevent external log-in attempts from the internet?

A. Port mapping
B. Subnetting
C. Static IP
D. Content filtering

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
To prevent external access, the technician should avoid exposing the surveillance system??s port to the public internet. Port mapping (also known as port forwarding) is the method used to control which internal devices and ports are accessible from the outside. By not configuring port forwarding for the device, external login attempts are effectively blocked.
* B. Subnetting organizes IP addresses but doesn't directly restrict access.
* C. A static IP ensures consistent addressing but does not secure access.
* D. Content filtering is used to restrict web content, not to block access to a web interface. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools. Study Guide Section: SOHO router security — port forwarding and blocking external
access
==========

NEW QUESTION 44
A technician needs to install an operating system on a large number of workstations. Which of the following is the fastest method?

A. Physical media
B. Mountable ISO
C. Manual installation
D. Image deployment

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Image deployment is the fastest and most efficient method for installing operating systems on multiple machines. It involves creating a pre-configured image of an OS and deploying it across systems using tools like Windows Deployment Services (WDS) or third-party imaging solutions. This method saves time and ensures consistency across all devices.
* A. Physical media is slow and not scalable.
* B. Mountable ISOs are useful but still require manual installation.
* C. Manual installation is time-consuming and not suitable for large-scale deployment. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Deployment methods — image deployment, automation

NEW QUESTION 47
A customer??s computer does not have an active connection to the network. A technician goes through a few troubleshooting steps but is unable to resolve the issue. The technician has exhausted their knowledge. The customer expresses frustration at the time taken to resolve this issue. Which of the following should the technician do?

A. Escalate the issue to a senior team member and provide next steps to the customer.
B. Dismiss the customer and reschedule another troubleshooting session at a later date.
C. Interrupt the customer and express that troubleshooting support tickets can take time.
D. Maintain a positive attitude and continue to ask questions regarding the scope of the issue.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:

When a technician exhausts all troubleshooting steps within their knowledge and the issue remains unresolved, the best practice is to escalate the issue to a higher-level technician or team. Additionally, the technician should clearly communicate the next steps to the customer to maintain transparency and reduce frustration. This ensures continuity of support and upholds customer satisfaction.
* B. Dismissing the customer is unprofessional and violates proper customer service
protocols.
* C. Interrupting the customer and providing excuses escalates the tension and is inappropriate.
* D. Continuing to ask questions without new troubleshooting steps wastes time and increases frustration.
Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information.
Study Guide Section: Customer service best practices — escalation and communication
==========

NEW QUESTION 48
MFA for a custom web application on a user's smartphone is no longer working. The last time the user remembered it working was before taking a vacation to another country. Which of the following should the technician do first?

A. Verify the date and time settings
B. Apply mobile OS patches
C. Uninstall and reinstall the application
D. Escalate to the website developer

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) apps, especially time-based one-time password (TOTP) apps (e.g., Google Authenticator, Authy), rely on accurate time synchronization between the device and the authentication server. If the user recently traveled internationally, the device may have incorrect date/time settings due to time zone changes or failed synchronization, leading to MFA failure.
The most logical and non-intrusive first step is to verify and correct the date and time settings. This aligns with basic troubleshooting principles—start with the simplest and most likely cause before taking more drastic action.
Reference:
CompTIA A+ 220-1102 Objective 2.6: Given a scenario, apply cybersecurity best practices to secure a workstation.
Study Guide Section: Authentication technologies and MFA troubleshooting
==========

NEW QUESTION 49
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

220-1202 Practice Exam Features:

* 220-1202 Questions and Answers Updated Frequently

* 220-1202 Practice Questions Verified by Expert Senior Certified Staff

* 220-1202 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 220-1202 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year