

220-1202 Dumps

CompTIA A+ Certification Exam: Core 2

<https://www.certleader.com/220-1202-dumps.html>



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

Recently, the number of users sharing smartphone passcodes has increased. The management team wants a technician to deploy a more secure screen lock method. Which of the following technologies should the technician use?

- A. Pattern lock
- B. Facial recognition
- C. Device encryption
- D. Multifactor authentication

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Facial recognition is a biometric authentication method that ties access to a unique physical feature of the user. Unlike passcodes or pattern locks—which can be easily shared—facial recognition provides a more secure and non-transferable form of access. It also enhances user convenience and is widely supported by modern smartphones.

* A. Pattern locks can still be shared and are less secure.

* C. Device encryption protects data but does not prevent screen access if a passcode is shared.

* D. Multifactor authentication typically applies to app or account access, not basic phone unlocking.

Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and authentication technologies.

Study Guide Section: Biometric screen lock technologies (e.g., facial recognition, fingerprint)

=====

NEW QUESTION 3

SIMULATION

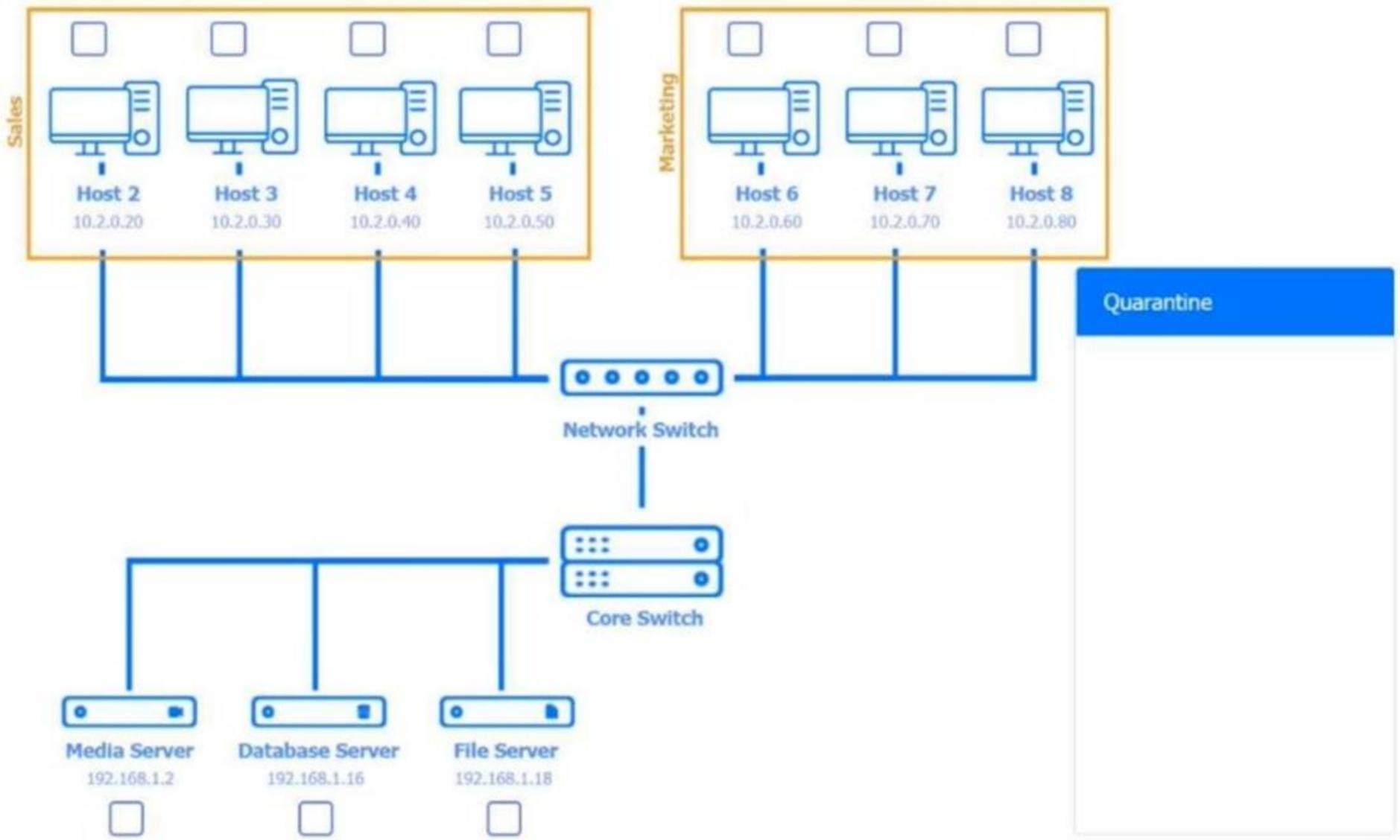
Multiple users are reporting audio issues as well as performance issues after downloading unauthorized software. You have been dispatched to identify and resolve any issues on the network using best practice procedures.

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

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

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

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

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

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

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

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

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

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

A company would like to deploy baseline images to new computers as they are started up on the network. Which of the following boot processes should the company use for this task?

- A. ISO
- B. Secure
- C. USB
- D. PXE

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
PXE (Preboot Execution Environment) allows workstations to boot over the network and download an OS image from a server. It is ideal for automating mass deployments using baseline images across many machines without the need for physical media.
* A. An ISO is a disk image file but requires mounting or physical media.
* B. Secure Boot is a security feature, not a method of deploying OS images.
* C. USB requires manual installation and is not suitable for automated deployment at scale. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Remote installation methods — PXE boot deployment
=====

NEW QUESTION 5

A technician is using a credential manager to safeguard a large number of credentials. Which of the following is important for using this application?

- A. Restricted log-in times
- B. Secure master password
- C. TPM module
- D. Windows lock screen

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
Credential managers or password vaults (e.g., Windows Credential Manager, KeePass, or LastPass) store passwords securely. The integrity of such tools heavily depends on the strength of the master password protecting the vault. If compromised, all saved credentials could be exposed. Therefore, setting a secure master password is crucial.
* A. Login time restrictions are general user account settings, not specific to credential managers.
* C. TPM is used more commonly for full disk encryption, not specifically required for password managers.
* D. The lock screen protects general access but does not protect stored credentials alone. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast authentication technologies and secure credential storage.
Study Guide Section: Password management and protection best practices
=====

NEW QUESTION 6

Which of the following is the quickest way to move from Windows 10 to Windows 11 without losing data?

- A. Using gpupdate
- B. Image deployment
- C. Clean install
- D. In-place upgrade

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
An in-place upgrade is the fastest and most efficient way to upgrade from Windows 10 to Windows 11 while keeping all user data, applications, and settings intact. This method is often used when the hardware meets Windows 11 requirements and no system reconfiguration is necessary.
* A. gpupdate is used to refresh Group Policy settings — unrelated to OS upgrades.
* B. Image deployment typically replaces the current OS and may not retain user data unless specifically customized.
* C. A clean install requires formatting the drive and starting fresh, which removes all data. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: In-place upgrade vs. clean install methods
=====

NEW QUESTION 7

Which of the following is the best way to distribute custom images to 800 devices that include four device vendor classes with two types of user groups?

- A. Use xcopy to clone the hard drives from one to another
- B. Use robocopy to move the files to each device
- C. Use a local image deployment tool for each device
- D. Use a network-based remote installation tool

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
In enterprise environments, network-based deployment solutions (such as Windows Deployment Services or SCCM) allow administrators to push images across the network to hundreds of devices efficiently. These tools support hardware-specific drivers (for different vendor classes) and can accommodate user-group configurations using task sequences or answer files.
A and B (xcopy and robocopy) are file-level tools and not designed for full OS image deployment.
* C. Using local tools per device is inefficient for large-scale rollouts (800 devices).
* D. Network-based deployment is the industry standard for this scale. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, use appropriate Microsoft operating system installation methods.
Study Guide Section: Deployment methods (including PXE boot, image deployment)
=====

NEW QUESTION 8

Which of the following is the best reason for a network engineering team to provide a help desk technician with IP addressing information to use on workstations being deployed in a secure network segment?

- A. Only specific DNS servers are allowed outbound access.
- B. The network allow list is set to a specific address.
- C. DHCP services are not enabled for this subnet.
- D. NAC servers only allow for security updates to be installed.

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
In secure or isolated network segments, DHCP may be disabled to reduce the risk of unauthorized device connections or to maintain strict IP assignment control. In such cases, the help desk technician must manually configure IP settings (including IP address, subnet mask, gateway, and DNS servers). This ensures the workstation communicates properly within that segment.
* A. DNS server restriction is unrelated to manual IP configuration.
* B. Allow lists refer to traffic access, but manual IP assignment is due to lack of DHCP, not allow lists.
* D. NAC servers control access but don't replace the need for IP addressing. Reference:
CompTIA A+ 220-1102 Objective 1.7: Given a scenario, troubleshoot common operating system and network issues.
Study Guide Section: IP configuration and DHCP-related deployment scenarios
=====

NEW QUESTION 9

A user has been adding data to the same spreadsheet for several years. After adding a significant amount of data, they are now unable to open the file. Which of the following should a technician do to resolve the issue?

- A. Revert the spreadsheet to the last restore point.
- B. Increase the amount of RAM.
- C. Defragment the storage drive.
- D. Upgrade the network connection speed.

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:
When a spreadsheet becomes very large, opening and processing it requires more memory (RAM). If the system doesn't have sufficient memory, it may fail to load the file properly. Upgrading or increasing the available RAM can resolve performance and loading issues with very large files.
* A. Restore points roll back system settings, not individual file content.
* C. Defragmentation optimizes disk performance but won't help with memory issues.
* D. Network speed has no effect if the file is stored and opened locally. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common application and performance issues.
Study Guide Section: Troubleshooting large-file performance and system resource limitations
=====

NEW QUESTION 10

A computer technician is implementing a solution to support a new internet browsing policy for a customer's business. The policy prohibits users from accessing unauthorized websites based on categorization. Which of the following should the technician configure on the SOHO router?

- A. Secure management access
- B. Group Policy Editor
- C. Content filtering
- D. Firewall

Answer: C

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Content filtering allows administrators to block or allow access to websites based on categories (e.g., social media, adult content, streaming). On a SOHO (Small Office/Home Office) router, this is often built-in or available via DNS-level filtering, and is the most appropriate method for enforcing browsing policies without needing to touch each individual device.

* A. Secure management access protects router admin interfaces but doesn't control user browsing.

* B. Group Policy Editor is a Windows tool, not used on routers.

* D. A firewall can block specific IPs or ports, but it doesn't categorize web content. Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security measures and tools. Study Guide Section: SOHO router security features — content filtering, parental controls

NEW QUESTION 10

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 15

Which of the following types of social engineering attacks sends an unsolicited text message to a user's mobile device?

A. Impersonation

B. Vishing

C. Spear phishing

D. Smishing

Answer: D

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Smishing (SMS phishing) is a type of social engineering attack where attackers send fraudulent text messages to trick users into revealing sensitive information or downloading malware. These messages often impersonate banks, delivery services, or official institutions to lure the victim into clicking malicious links.

* A. Impersonation is an in-person or voice-based tactic.

* B. Vishing refers to voice phishing over phone calls.

* C. Spear phishing is a targeted email-based phishing method. Reference:

CompTIA A+ 220-1102 Objective 2.3: Compare and contrast social engineering techniques.

Study Guide Section: Smishing as a type of phishing via SMS or mobile messaging.

NEW QUESTION 16

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 20

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 22

A customer wants to be able to work from home but does not want to be responsible for bringing company equipment back and forth. Which of the following would allow the user to remotely access and use a Windows PC at the main office? (Choose two.)

- A. SPICE
- B. SSH
- C. RDP
- D. VPN
- E. RMM
- F. WinRM

Answer: CD

Explanation:

Comprehensive and Detailed Explanation From Exact Extract: To work remotely without physically transporting a workstation, the user needs:

? C. RDP (Remote Desktop Protocol): Allows graphical remote access to a Windows PC at the office.

? D. VPN (Virtual Private Network): Establishes a secure tunnel to access the corporate network remotely, making the internal PC reachable.

* A. SPICE is used in virtual machine environments and is not typically used for end-user remote desktop access.

* B. SSH is a text-based remote access tool used mostly for Linux systems.

* E. RMM (Remote Monitoring and Management) is used by IT administrators for support — not end-user remote access.

* F. WinRM is used for Windows remote management via PowerShell, not for full desktop access.

Reference:

CompTIA A+ 220-1102 Objectives 2.2 & 4.4: Compare and contrast security tools and remote access methods.

Study Guide Section: Remote access tools — RDP and VPN for secure remote work

NEW QUESTION 24

A user reports some single sign-on errors to a help desk technician. Currently, the user is able to sign in to the company's application portal but cannot access a specific SaaS-based tool. Which of the following would the technician most likely suggest as a next step?

- A. Reenroll the user's mobile device to be used as an MFA token
- B. Use a private browsing window to avoid local session conflicts
- C. Bypass single sign-on by directly authenticating to the application
- D. Reset the device being used to factory defaults

Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

SSO issues are often related to cached session data, cookies, or browser artifacts. The fact that the user can access the company portal but not one specific SaaS tool suggests a session or token problem. Using a private/incognito browsing window allows a clean session to be initiated, which often resolves SSO conflicts.

* A. Reenrolling MFA is not related unless access issues stem from failed multifactor authentication.

* C. Bypassing SSO may not be possible depending on the SaaS tool and company policies.

* D. Factory resetting a device is a last resort and unnecessary in this case. Reference:

CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software, application, and OS security issues.

Study Guide Section: Troubleshooting login and authentication issues, especially with SSO services.

=====

NEW QUESTION 28

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 220-1202 Exam with Our Prep Materials Via below:

<https://www.certleader.com/220-1202-dumps.html>