CompTIA

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

NEW QUESTION 1
The screen of a previously working computer repeatedly displays an OS Not Found error message when the computer is started. Only a USB drive, a keyboard, and a mouse are plugged into the computer. Which of the following should a technician do first?

A. Run data recovery tools on the disk
B. Partition the disk using the GPT format
C. Check boot options
D. Switch from UEFI to BIOS

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An "OS Not Found" error typically indicates that the computer is attempting to boot from a drive that doesn't contain a valid operating system or bootable partition. The presence of a USB drive might be confusing the boot order. Therefore, the first step a technician should take is to verify and adjust the boot sequence in the system??s firmware (BIOS or UEFI). It's possible that the USB drive is being prioritized over the internal hard drive, which may cause the system to miss the OS entirely.
* A. Running data recovery tools is premature before confirming boot order.
* B. Repartitioning the disk would destroy existing data—this should not be done until confirmed the OS is actually missing.
* D. Switching between UEFI and BIOS (legacy mode) might help in rare cases, but it is not the first step in standard OS boot issue troubleshooting.
Reference:
CompTIA A+ 220-1102 Objective 1.7: Troubleshoot common operating system problems. Study Guide Section: Boot process and boot order configuration.
==========

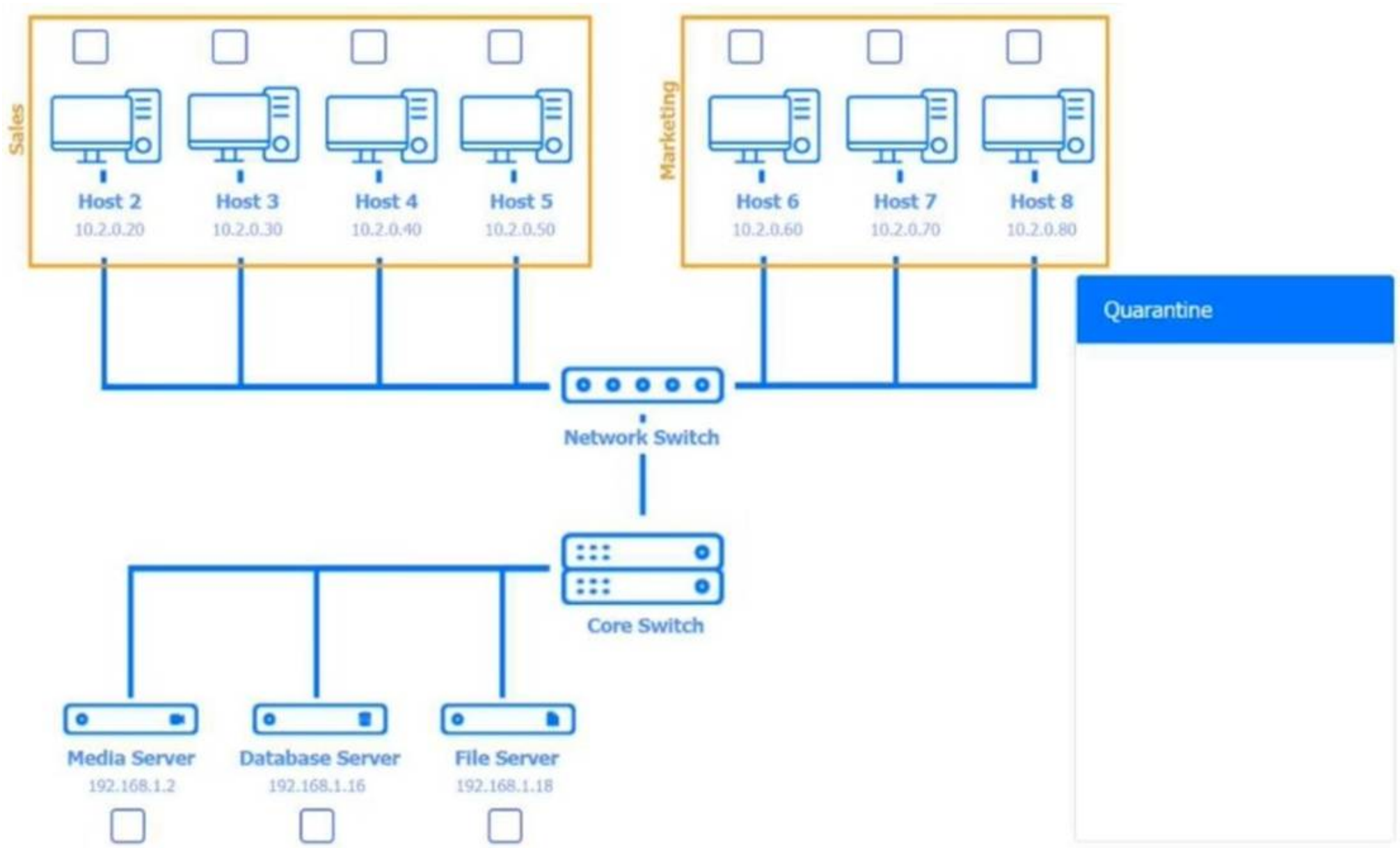
NEW QUESTION 2
Recently, the number of users sharing smartphone passcodes has increased. The management team wants a technician to deploy a more secure screen lock method. Which of the following technologies should the technician use?

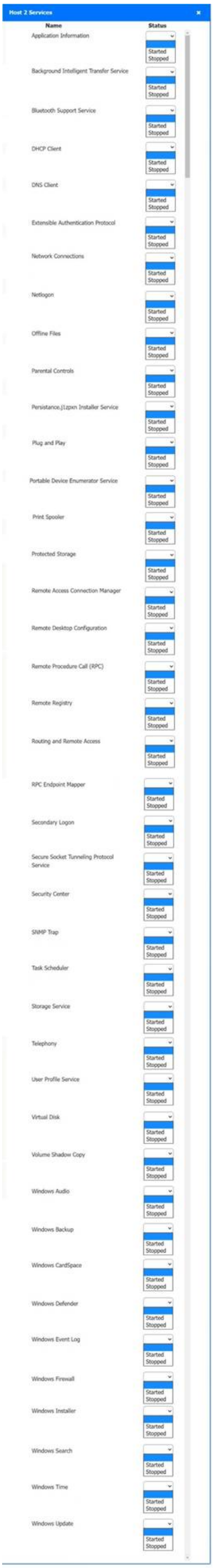
A. Pattern lock
B. Facial recognition
C. Device encryption
D. Multifactor authentication

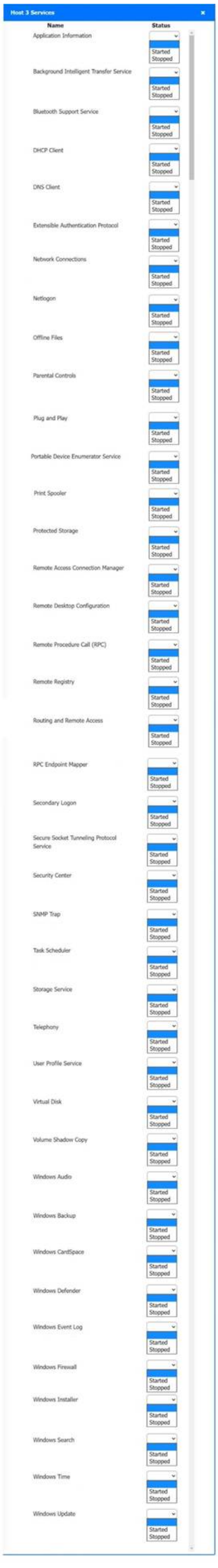
Answer: B

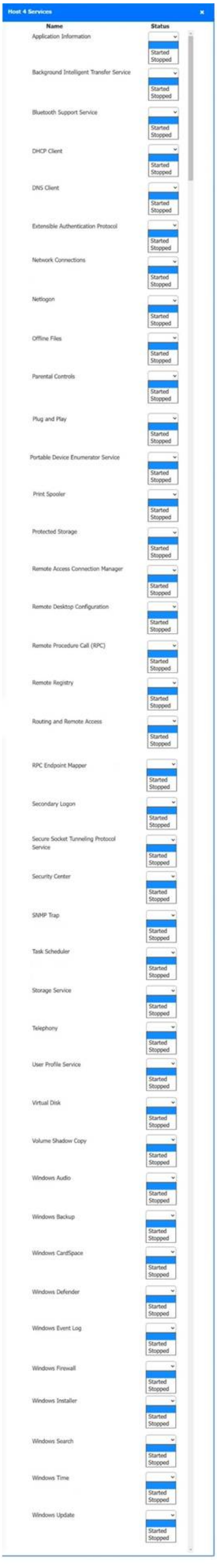
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Facial recognition is a biometric authentication method that ties access to a unique physical feature of the user. Unlike passcodes or pattern locks—which can be easily shared—facial recognition provides a more secure and non-transferable 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)
==========

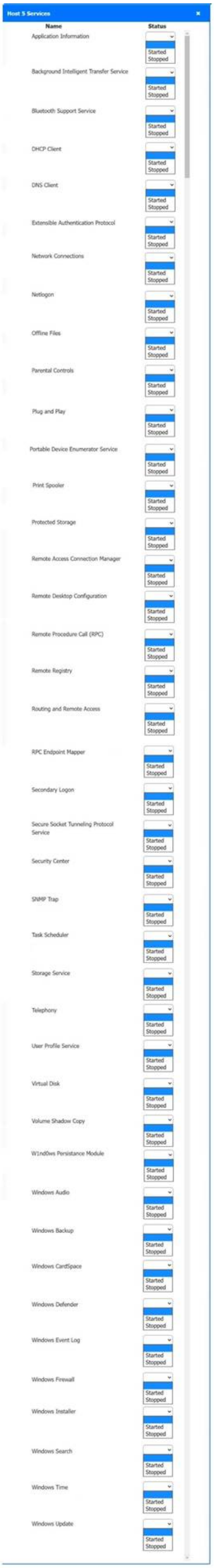
NEW QUESTION 3
SIMULATION
Multiple users are reporting audio issues as well as performance issues after downloading unauthorized software. You have been dispatched to identify and resolve any issues on the network using best practice procedures.
INSTRUCTIONS
Quarantine and configure the appropriate device(s) 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.

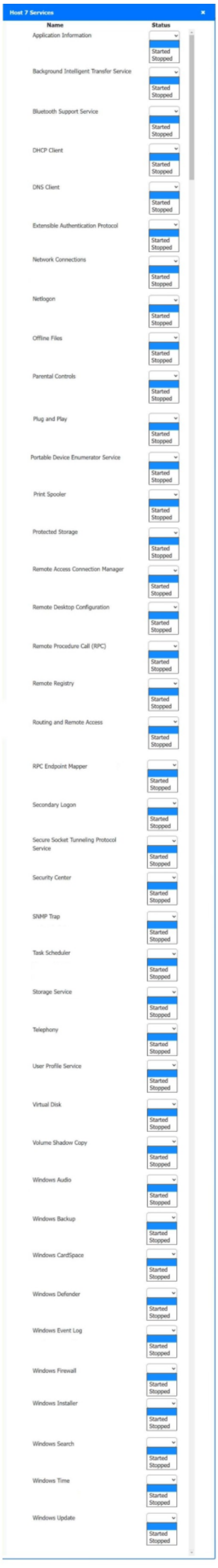

Sales
Host 2
10.2.0.20
Host 3
10.2.0.30
Host 4
10.2.0.40
Host 5
10.2.0.50
Marketing
Host 6
10.2.0.60
Host 7
10.2.0.70
Host 8
10.2.0.80
Quarantine
Network Switch
Core Switch
Media Server
192.168.1.2
Database Server
192.168.1.16
File Server
192.168.1.18

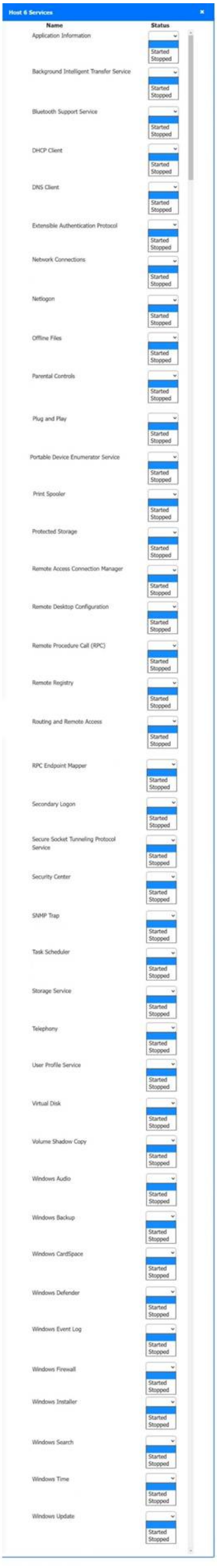

Host 2 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Persistance.j1zpxn Installer Service
Plug and Play
Portable Device 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

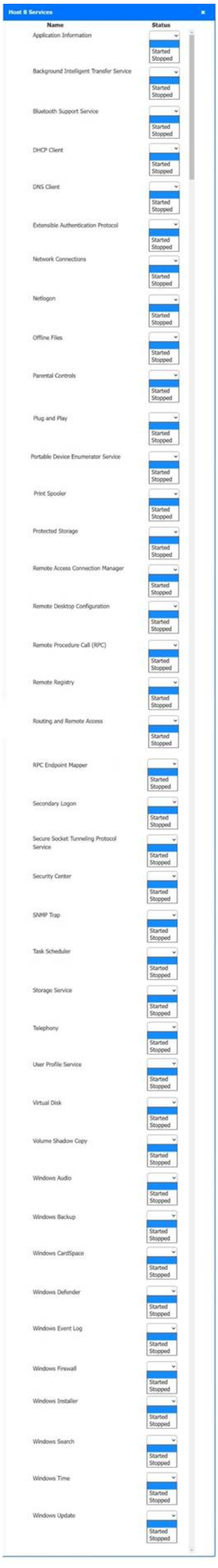

Host 3 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected 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

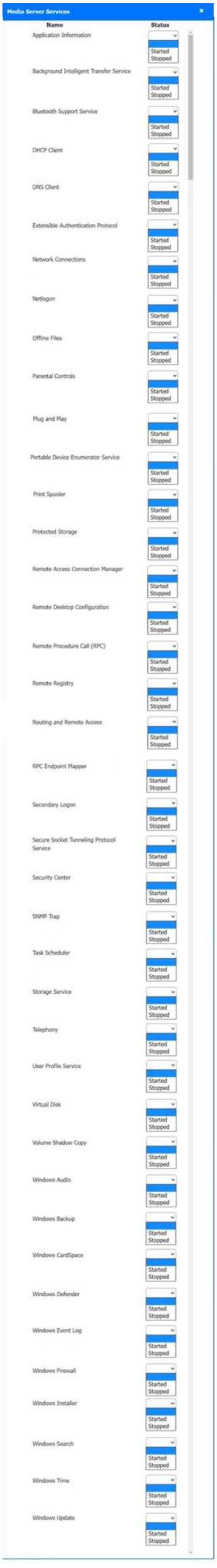

Host 4 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected 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

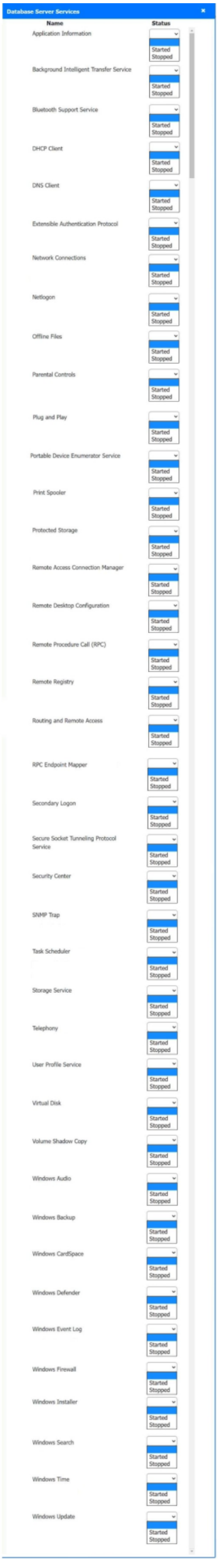

Host 5 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected 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

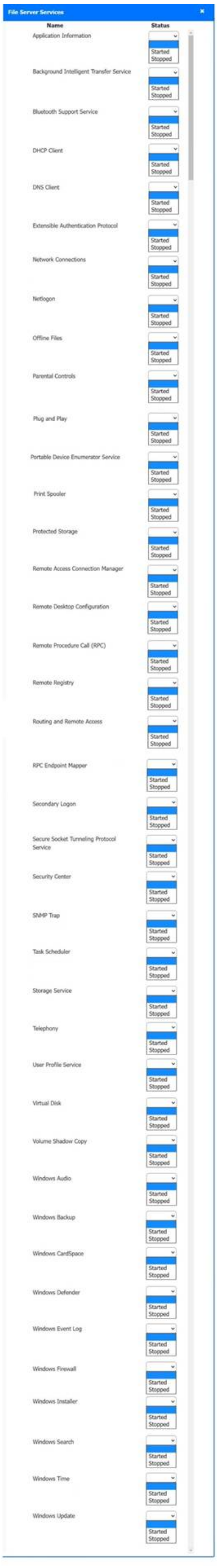

Host 7 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected 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 4
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 5
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 6
A technician is attempting to join a workstation to a domain but is receiving an error message stating the domain cannot be found. However, the technician is able to ping the server and access the internet. Given the following information:
? IP Address – 192.168.1.210
? Subnet Mask – 255.255.255.0
? Gateway – 192.168.1.1
? DNS1 – 8.8.8.8
? DNS2 – 1.1.1.1
? Server – 192.168.1.10
Which of the following should the technician do to fix the issue?

A. Change the DNS settings.
B. Assign a static IP address.
C. Configure a subnet mask.
D. Update the default gateway.

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The issue described—??domain cannot be found?? despite the ability to ping the server and access the internet—indicates aDNS resolution problem, not a network connectivity issue. The workstation is currently usingpublic DNS servers (8.8.8.8 and 1.1.1.1)which cannot resolve internal domain names, such as the ones used

in Active Directory environments. To resolve this, the technician needs tochange the DNS settings to point to the internal DNS server, which in most domain setups is thedomain controller itself (likely 192.168.1.10 in this case).
Here??s the breakdown of the incorrect options:
? B. Assign a static IP address: The IP is already assigned and functioning; the
device can ping and reach the network and internet.
? C. Configure a subnet mask: The subnet mask is appropriate for the network range (Class C /24).
? D. Update the default gateway: The gateway is valid and allows internet access; this is not the issue.
CompTIA A+ 220-1102 Core 2 Objective Reference:
Objective 1.8 – Given a scenario, use features and tools of the operating system. Under this objective, candidates must know how to troubleshoot OS-based network configurations, includingproper DNS settings in domain environments.

NEW QUESTION 7
A company wants to use a single operating system for its workstations and servers and avoid licensing fees. Which of the following operating systems would the company most likely select?

A. Linux
B. Windows
C. macOS
D. Chrome OS

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Linux is an open-source operating system that is freely available and does not require traditional licensing fees. It is highly versatile and scalable, making it suitable for both workstations and servers. Many enterprise environments use Linux to reduce software costs and benefit from robust server features.
* B. Windows requires per-device or per-user licensing for both workstation and server editions.
* C. macOS is proprietary and limited to Apple hardware with licensing restrictions.
* D. Chrome OS is designed for lightweight devices and lacks server functionality. Reference:
CompTIA A+ 220-1102 Objective 1.8 & 1.9: Identify common features and tools of the Linux client/desktop OS.
Study Guide Section: Open-source operating systems and licensing considerations
==========

NEW QUESTION 8
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 9
Which of the following is used in addition to a password to implement MFA?

A. Sending a code to the user's phone
B. Verifying the user's date of birth
C. Prompting the user to solve a simple math problem
D. Requiring the user to enter a PIN

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) requires at least two different types of authentication factors:
? Something you know (e.g., password or PIN)
? Something you have (e.g., smartphone or hardware token)
? Something you are (e.g., fingerprint or facial recognition)
Option A, sending a code to the user??s phone, is an example of "something you have" — a physical device that receives a one-time passcode. Combined with a password, this forms a proper MFA implementation.
* B. Date of birth is another knowledge-based factor (like a password), not a second factor type.
* C. Solving a math problem is not a recognized authentication factor.
* D. A PIN is also "something you know" and does not count as a distinct MFA factor when paired with a password.
Reference:

CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and authentication technologies.
Study Guide Section: Authentication factors — password, biometrics, tokens, MFA
==========

NEW QUESTION 10
A technician installs VPN client software that has a software bug from the vendor. After the vendor releases an update to the software, the technician attempts to reinstall the software but keeps getting an error message that the network adapter for the VPN already exists. Which of the following should the technician do next to mitigate this issue?

A. Run the latest OS security updates.
B. Map the network adapter to the new software.
C. Update the network adapter's firmware.
D. Delete hidden network adapters.

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
VPN clients often create virtual network adapters. If the software wasn't uninstalled properly or crashed during install, leftover (often hidden) virtual adapters can prevent reinstallation. The proper solution is to delete hidden network adapters using Device Manager (with ??Show hidden devices?? enabled).
* A. OS updates won??t fix a leftover driver or adapter issue.
* B. Mapping an adapter to the software is not a standard or viable solution.
* C. Firmware updates apply to physical adapters, not virtual VPN adapters. Reference:
CompTIA A+ 220-1102 Objective 3.1: Troubleshoot common Windows OS and network issues.
Study Guide Section: Troubleshooting network adapter conflicts and VPN client errors

NEW QUESTION 10
A help desk team was alerted that a company-owned cell phone has an unrecognized password-cracking application. Which of the following should the help desk team do to prevent further unauthorized installations from occurring?

A. Configure Group Policy.
B. Implement PAM.
C. Install anti-malware software.
D. Deploy MDM.

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Mobile Device Management (MDM) is used to control, monitor, and enforce policies on mobile devices. It allows IT teams to restrict app installations, push approved apps, and monitor device compliance. Deploying MDM would prevent unauthorized applications, such as password crackers, from being installed on company-managed devices.
* A. Group Policy is for managing Windows environments and not applicable to smartphones.
* B. PAM (Privileged Access Management) controls administrative access, not app installation.
* C. Anti-malware can help detect malicious apps but doesn??t prevent their installation proactively.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast common security measures and tools.
Study Guide Section: Mobile Device Management (MDM) capabilities — app control, security enforcement

NEW QUESTION 15
Which of the following is used to apply corporate restrictions on an Apple device?

A. App Store
B. VPN configuration
C. Apple ID
D. Management profile

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A management profile is used to enforce corporate policies on Apple devices. These profiles are installed via an MDM (Mobile Device Management) solution and control access, restrictions,Wi-Fi settings, app installations, and more. They??re critical for managing devices in a business environment.
* A. The App Store allows software downloads but doesn??t control policies.
* B. VPN configuration is used for secure remote connections, not enforcement of restrictions.
* C. Apple ID is for personal account access to Apple services, not corporate device management.
Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast security tools and MDM features.
Study Guide Section: Mobile device management and configuration profiles (Apple/iOS)
==========

NEW QUESTION 16
Which of the following file types would a desktop support technician most likely use to automate tasks for a Windows user log-in?

A. .bat
B. .sh
C. .py
D. .js

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
* A .bat file (batch file) is a script file in DOS, OS/2, and Microsoft Windows. It contains a series of commands that are executed by the command-line interpreter. In Windows environments, batch files are commonly used to automate log-in tasks, such as mapping network drives, launching applications, or setting environment variables during the user's logon process.
* B. .sh is a shell script used in Linux/Unix environments.
* C. .py is a Python script, which can be used for automation but is not commonly run directly at user logon in standard Windows environments.
* D. .js is JavaScript, used mainly in web development and not for system-level scripting in Windows logon automation.
Reference:
CompTIA A+ 220-1102 Objective 1.3: Use appropriate Microsoft operating system features and tools.
Study Guide Section: Scripting basics and file types for automation — .bat for Windows
==========

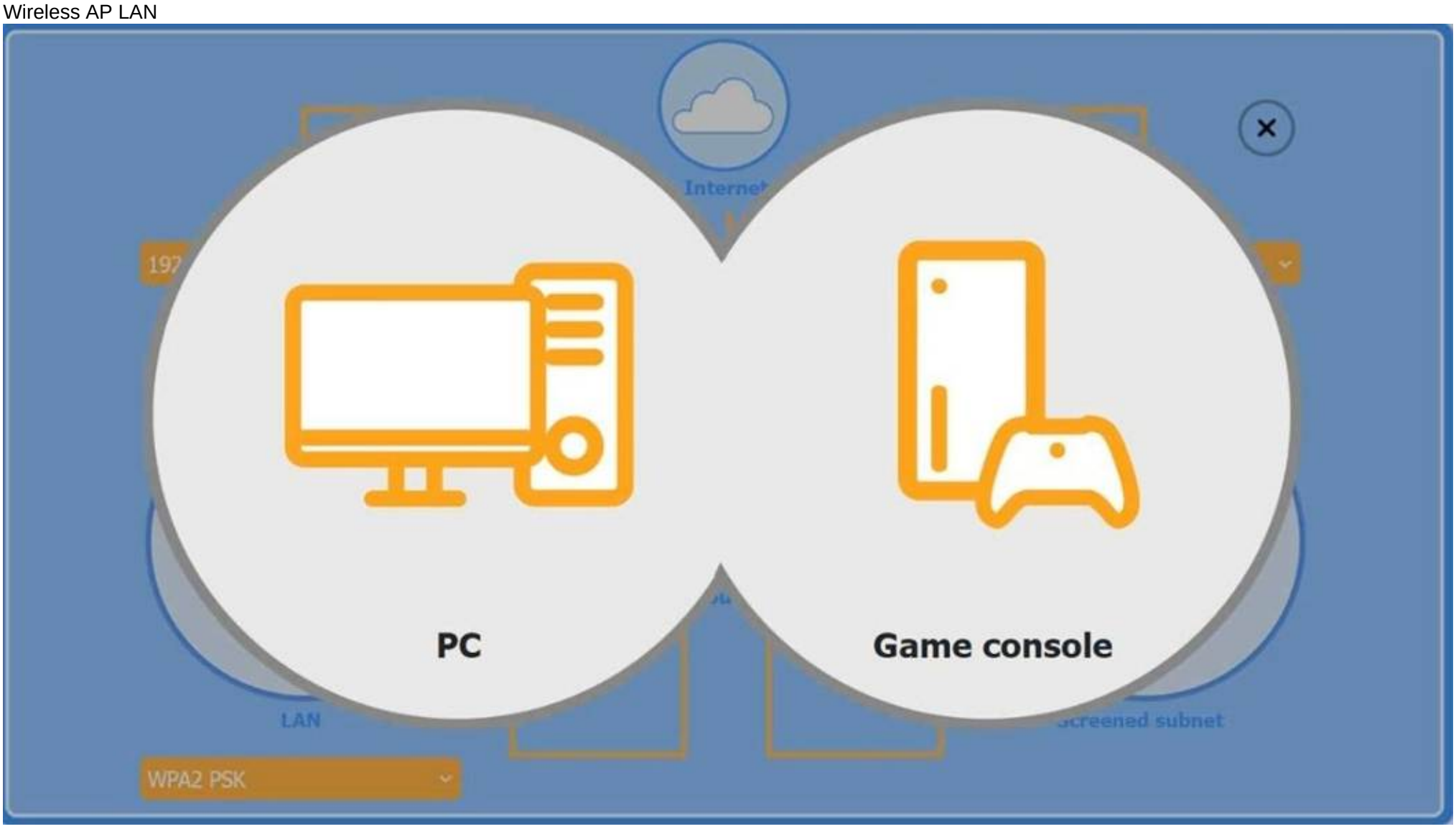
NEW QUESTION 18
A user is experiencing issues with outdated images while browsing websites. Which of the following settings should a technician use to correct this issue?

A. Administrative Tools
B. Windows Defender Firewall
C. Internet Options
D. Ease of Access

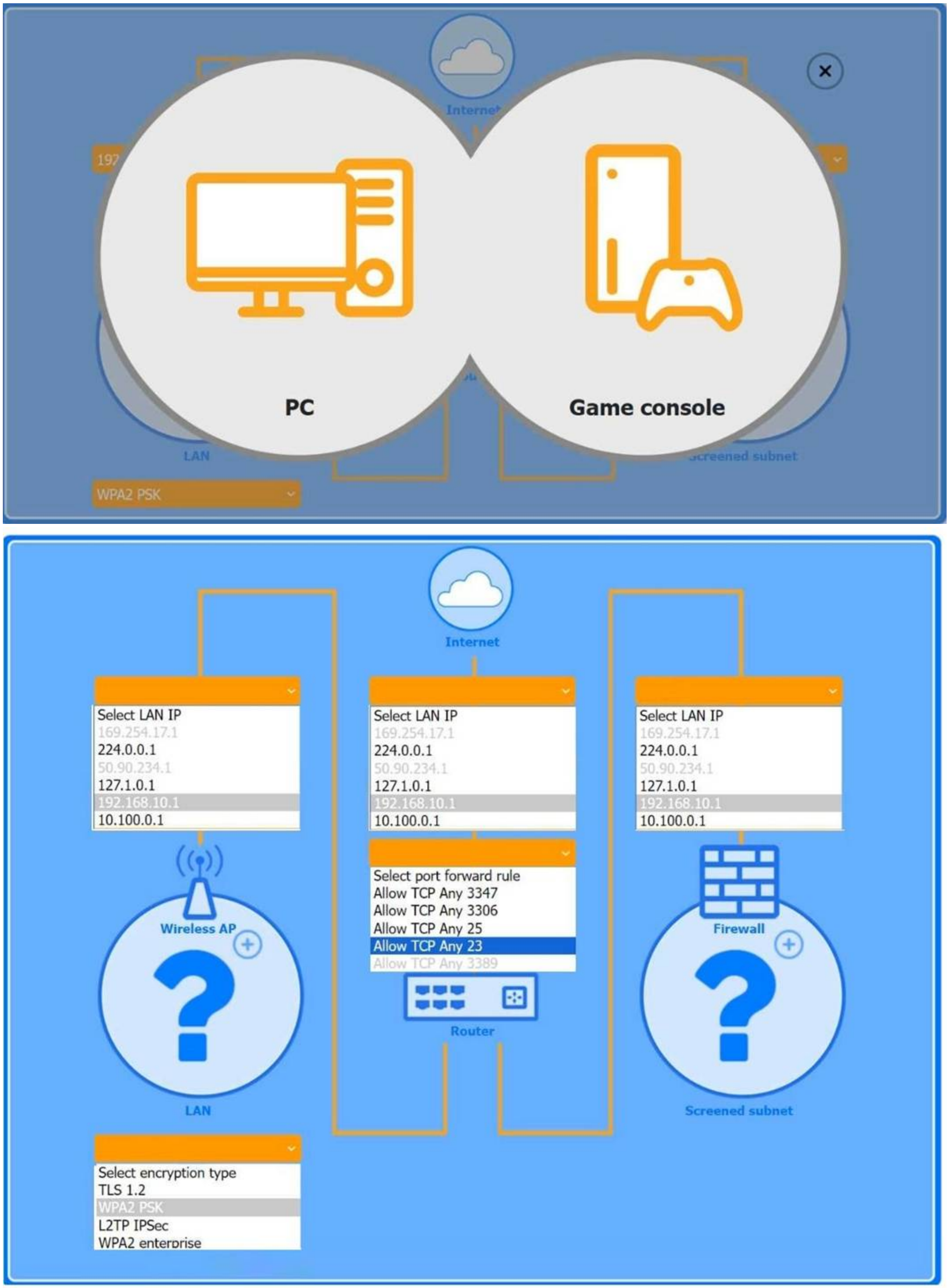
Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract: Outdated images and website data often result from cached files in the browser. The Internet Options panel in Windows (specifically under the General tab) allows users to clear browsing history, including cached images and files, which forces the browser to load the most current versions of web content.
* A. Administrative Tools is used for advanced system management, not browser settings.
* B. Windows Defender Firewall controls network traffic and security rules, not caching.
* D. Ease of Access provides accessibility features for users with disabilities — unrelated to web browsing issues.
Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common software and application issues.
Study Guide Section: Internet Options and browser cache clearing for display issues

NEW QUESTION 19
SIMULATION
You are configuring a home network for a customer. The customer has requested the ability to access a Windows PC remotely, and needs all chat and optional functions to work in their game console.
INSTRUCTIONS
Use the drop-down menus to complete the network configuration for the customer. Each option may only be used once, and not all options will be used.
Then, click the + sign to place each device in its appropriate location.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.
Wireless AP LAN



Firewall Screened Subnet



A. Mastered
B. Not Mastered

Answer: A

Explanation:
The completed configuration:
* 1. Wireless AP (LAN side) 1. LAN IP: 192.168.10.1
* 2. Encryption: WPA2 PSK
* 2. Router (port-forward rule)
* 1. Allow TCP Any 3389
This forwards inbound RDP traffic (TCP/3389) from the Internet to the Windows PC, enabling Remote Desktop access.
* 3. Firewall (screened subnet side) 1. LAN IP: 10.100.0.1
* 4. Device placement
* 1. PC: place behind the router (where the port-forward rule points).
* 2. Game console: place on the Wireless AP (so it can use chat and extra services over WPA2 PSK).
* 3. Firewall: place in front of the screened subnet (with its 10.100.0.1 IP facing that subnet).
? The Windows PC is placed in the screened subnet (behind the firewall) for enhanced security. Remote access to this PC requires port forwarding of TCP port 3389 (RDP), which is correctly configured through the router.
? The Game Console is placed on the Wireless AP LAN, using WPA2 PSK for a secure wireless connection. Game consoles typically use peer-to-peer chat and online services that require open access without firewall restrictions, which is why the console is not placed behind the firewall.
CompTIA A+ 220-1102 Reference Points:
? Objective 3.4: Given a scenario, implement best practices associated with data and device security.
? Objective 2.4: Given a scenario, use appropriate tools to support and configure network settings.
? Study Guide Reference: CompTIA A+ Core 2 guides recommend using screened subnets (a type of DMZ) for systems needing controlled external access, such as remote desktops, while placing gaming and media devices on less restricted networks for full functionality.

NEW QUESTION 22
A technician is troubleshooting an issue in which a service runs momentarily and stops at certain points in the process. The technician needs to determine the root cause of this issue. Which of the following tools should the technician use?

A. Event Viewer
B. Task Manager
C. Internet Options
D. Process Explorer

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the best tool to analyze the root cause of service failures in Windows. It provides detailed logs from system processes, including errors, warnings, and crash reports related to services and applications. When a service starts and stops unexpectedly, Event Viewer will often record the cause, such as dependency failures or access violations.
* B. Task Manager shows active processes but doesn't retain logs or causes of failure.
* C. Internet Options is used for configuring browser settings, not troubleshooting services.
* D. Process Explorer is powerful but more suited for live monitoring and detailed process trees, not post-failure log analysis.
Reference:
CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.
Study Guide Section: Log file analysis using Event Viewer
==========

NEW QUESTION 24
An end user's laptop is having network drive connectivity issues in the office. The end user submits a help desk ticket, and a support technician is able to establish a remote connection and fix the issue. The following day, however, the network drive is disconnected again. Which of the following should the technician do next?

A. Connect remotely to the user's computer to see whether the network drive is still connected.
B. Send documentation about how to fix the issue in case it reoccurs.
C. Escalate the ticket to the next level.
D. Keep the ticket open until next day, then close the ticket.

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Since the issue has recurred after a temporary fix, it is likely a deeper or persistent configuration or server issue. Escalating the ticket to the next tier of support (e.g., network or system administrator) ensures further investigation and permanent resolution. Escalation is part of the standard support protocol when issues reoccur despite initial troubleshooting.
* A. Rechecking remotely may confirm the issue, but doesn??t resolve it long term.
* B. Providing documentation helps the user but doesn??t solve the root cause.
* D. Keeping the ticket open is passive and doesn??t address the recurring issue. Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information.
Study Guide Section: Escalation procedures and ticket management
==========

NEW QUESTION 27
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 31
Which of the following provides information to employees, such as permitted activities when using the organization's resources?

A. AUP
B. MNDA
C. DRM
D. EULA

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An Acceptable Use Policy (AUP) outlines the rules and guidelines for employees or users regarding the appropriate use of company systems, resources, and internet access. It defines permitted and prohibited activities, helping to mitigate security risks and establish clear behavioral expectations.
* B. MNDA (Mutual Non-Disclosure Agreement) deals with confidentiality, not usage guidelines.
* C. DRM (Digital Rights Management) controls access to copyrighted content.
* D. EULA (End User License Agreement) pertains to software licensing, not internal policies.
Reference:
CompTIA A+ 220-1102 Objective 4.3: Explain common safety and environmental impacts and procedures.
Study Guide Section: Organizational policies — AUP, security best practices
==========

NEW QUESTION 36
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 40
A network technician notices that most of the company's network switches are now end-of- life and need to be upgraded. Which of the following should the technician do first?

A. Implement the change
B. Approve the change
C. Propose the change
D. Schedule the change

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The first step in the IT change management process is to identify and propose the change. In this case, the technician notices a need (end-of-life network switches), so the
appropriate action is toformally propose a change. This proposal would be documented and submitted for approval before any planning or implementation occurs.
According to the CompTIA A+ 220-1102 objectives under Operational Procedures (Domain 4.0), the change management process follows these typical steps:
? Submit a change request (Propose the change)
? Review and approval (Approve the change)
? Planning and scheduling (Schedule the change)
? Implementation
? Documentation and review
Therefore, proposing the change is the correct first step in accordance with standard ITIL- based change management practices.
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: Change Management Process
==========

NEW QUESTION 44
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 45
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 49
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 50
An application's performance is degrading over time. The application is slowing, but it never gives an error and does not crash. Which of the following tools should a technician use to start troubleshooting?

A. Reliability history
B. Computer management
C. Resource monitor
D. Disk

Answer: C

Explanation:
Comprehensive and Detailed Explanation From Exact Extract: Resource Monitor provides real-time monitoring of system performance and resource usage, including CPU, memory, disk, and network usage. It helps technicians identify
performance bottlenecks (e.g., high memory or CPU usage) that can cause slowdowns in applications over time without producing crash errors.
* A. Reliability history logs application crashes or errors — not helpful if the app doesn??t crash.
* B. Computer Management is a broad utility with limited real-time monitoring capability.
* D. Disk is too vague — tools like CHKDSK can help with disk errors but not general performance degradation.
Reference:
CompTIA A+ 220-1102 Objective 3.2: Given a scenario, troubleshoot common personal computer issues.
Study Guide Section: System performance tools — Resource Monitor, Task Manager
==========

NEW QUESTION 51
Which of the following is a Linux command that is used for administrative purposes?

A. runas
B. cmcl
C. net user
D. su

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The su (substitute user) command is used in Linux to switch to another user account, most commonly to escalate privileges by switching to the root (administrator) account. It allows administrative tasks to be performed in a terminal session.
* A. runas is a Windows command for executing a program under another user's context.
* B. cmcl is not a valid Linux or administrative command.
* C. net user is a Windows command for managing local user accounts.
Reference:
CompTIA A+ 220-1102 Objective 1.9: Identify common features and tools of the Linux client/desktop OS.
Study Guide Section: Linux command-line tools — su, sudo
==========

NEW QUESTION 56
A user recently installed an application that accesses a database from a local server. When launching the application, it does not populate any information. Which of the following command-line tools is the best to troubleshoot the issue?

A. ipconfig
B. nslookup
C. netstat
D. curl

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The scenario involves an application that should retrieve data from a local database server but is failing to do so. This likely indicates a problem in communication between the application and the database server (such as a network issue, port misconfiguration, or service unavailability). The correct troubleshooting approach involves testing the network/service connectivity between the client and the database.
Let??s examine the options:
? A. ipconfig:This command displays IP configuration details for Windows systems, such as IP address, subnet mask, and default gateway. While useful for diagnosing general networkissues, it does not test service connectivity or the availability of a specific application port/service.
? B. nslookup:Used to query DNS servers to resolve domain names to IP addresses.
However, since the question references a local server (likely accessed via IP or static hostname), DNS is probably not involved. Also, it does not test application/service availability.
? C. netstat:Displays active TCP connections, listening ports, and routing tables. It
helps determine whether the local system is listening for or maintaining any network connections, but it does not initiate a connection to test availability. It??s diagnostic but not interactive for service testing.
? D. curl:This is the most appropriate tool for this scenario. curl is used to test
connectivity to services over protocols like HTTP, HTTPS, FTP, and more. If the application retrieves data via a web interface or API (common in database-driven applications), curl can be used to test if the application can successfully reach and retrieve data from the server. It provides immediate, testable feedback on whether the server and service are available and responsive.
Example usage: curlhttp://localhost:8080/api/data
This command would test whether a local server's application programming interface (API) is available and responding on port 8080.
CompTIA A+ 220-1102 Reference Points:
? Objective 2.4: Given a scenario, use appropriate tools to troubleshoot and support Windows OS issues.
? Objective 3.3: Use appropriate tools to troubleshoot and resolve issues.
? The CompTIA A+ Core 2 study guide references curl as a useful command-line utility for testing connectivity and troubleshooting application access to services.
==========

NEW QUESTION 58
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 59
A user's new smartphone is not staying charged throughout the day. The smartphone charges fully every night. Which of the following should a technician review first to troubleshoot the issue?

A. Storage usage
B. End of software support
C. Charger wattage
D. Background applications

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract: Background applications can significantly drain a smartphone??s battery, even when the device is idle. A technician should first review which apps are running in the background
and consuming power through the battery usage section of the OS. Disabling or restricting power-hungry apps often resolves poor battery life.
* A. Storage usage doesn??t significantly affect battery life.
* B. End of software support is unrelated to battery performance unless it's causing inefficient processes, which would still be secondary.
* C. Charger wattage affects charging speed, not battery life after charging. Reference:
CompTIA A+ 220-1102 Objective 3.3: Troubleshoot common mobile OS and application issues.
Study Guide Section: Diagnosing battery and app performance issues on mobile devices

NEW QUESTION 64
A support specialist needs to decide whether to install a 32-bit or 64-bit OS architecture on a new computer. Which of the following specifications will help the specialist determine which OS architecture to use?

A. 16GB RAM
B. Intel i7 CPU
C. 500GB HDD
D. 1Gbps Ethernet

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The amount of installed RAM is the key factor in determining whether a 64-bit OS is needed. A 32-bit operating system cannot effectively address more than 4GB of RAM. Since this system has 16GB of RAM, a 64-bit OS is required to utilize the full memory.
* B. An Intel i7 CPU supports both 32-bit and 64-bit OS installations, so it alone doesn??t determine the need.
* C. HDD size does not influence OS architecture selection.
* D. Ethernet speed is a network consideration and not related to OS architecture. Reference:
CompTIA A+ 220-1102 Objective 1.4: Given a scenario, choose the appropriate Microsoft OS installation methods and configurations.
Study Guide Section: 32-bit vs. 64-bit system requirements and memory limitations
==========

NEW QUESTION 67
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 70

.....

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

100% Actual & Verified — Instant Download, Please Click
Order The 220-1202 Practice Test Here