CompTIA

Exam Questions 220-1202

CompTIA A+ Certification Exam: Core 2

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

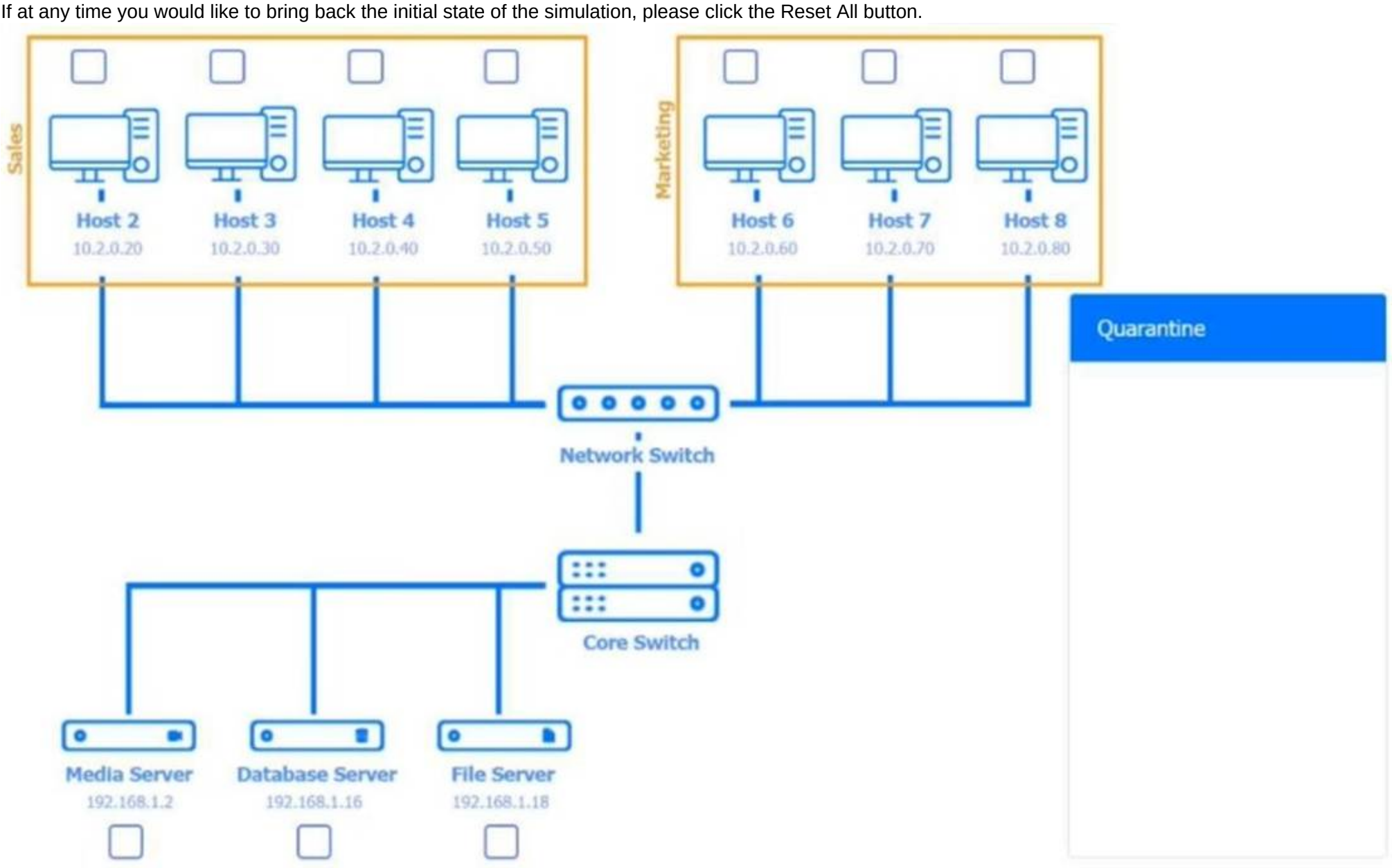
NEW QUESTION 1
Recently, the number of users sharing smartphone passcodes has increased. The management team wants a technician to deploy a more secure screen lock method. Which of the following technologies should the technician use?

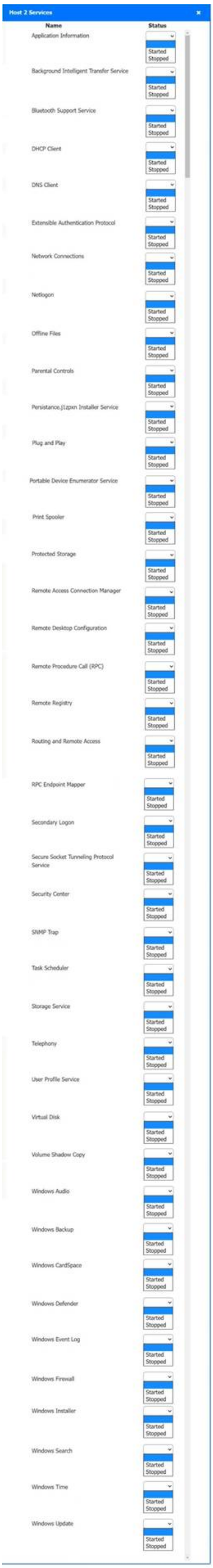
A. Pattern lock
B. Facial recognition
C. Device encryption
D. Multifactor authentication

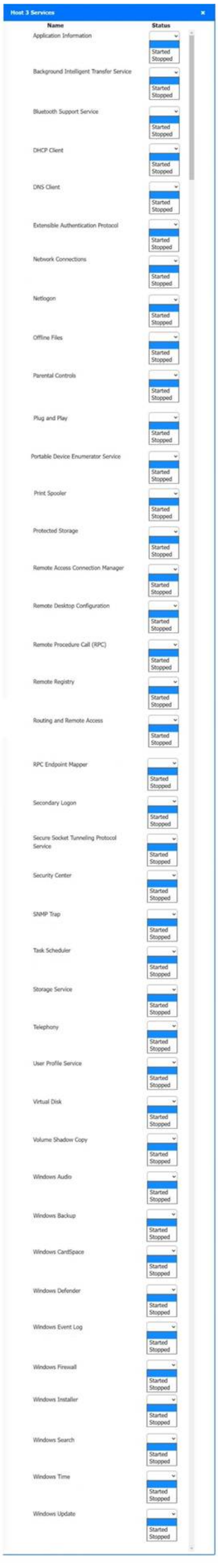
Answer: B

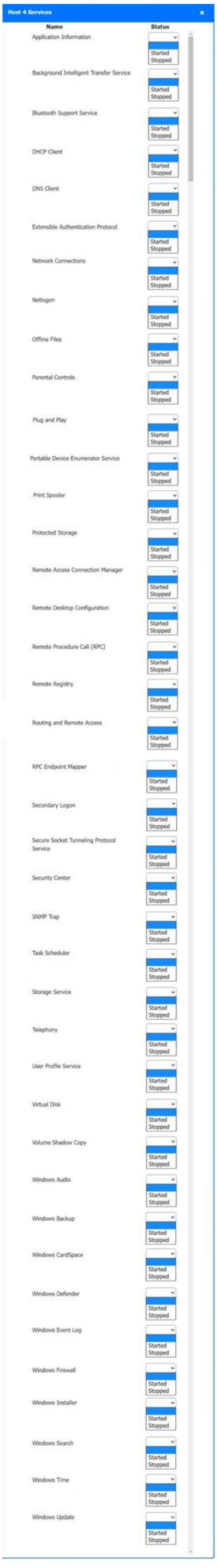
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Facial recognition is a biometric authentication method that ties access to a unique physical feature of the user. Unlike passcodes or pattern locks—which can be easily shared—facial recognition provides a more secure and non-transferable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

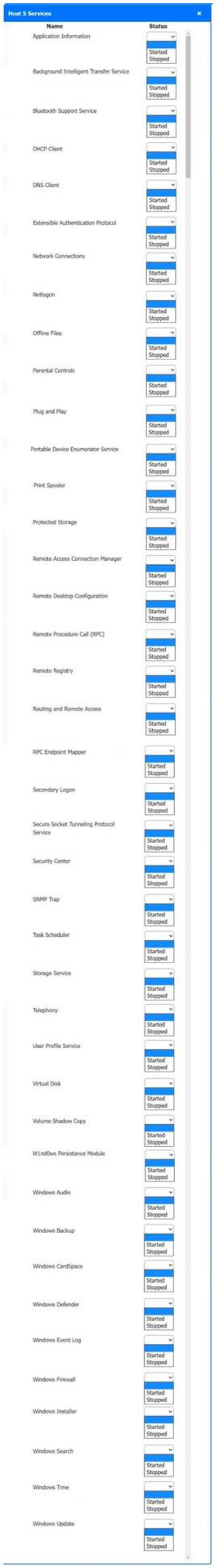
NEW QUESTION 2
SIMULATION
Multiple users are reporting audio issues as well as performance issues after downloading unauthorized software. You have been dispatched to identify and resolve any issues on the network using best practice procedures.
INSTRUCTIONS
Quarantine and configure the appropriate device(s) 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.

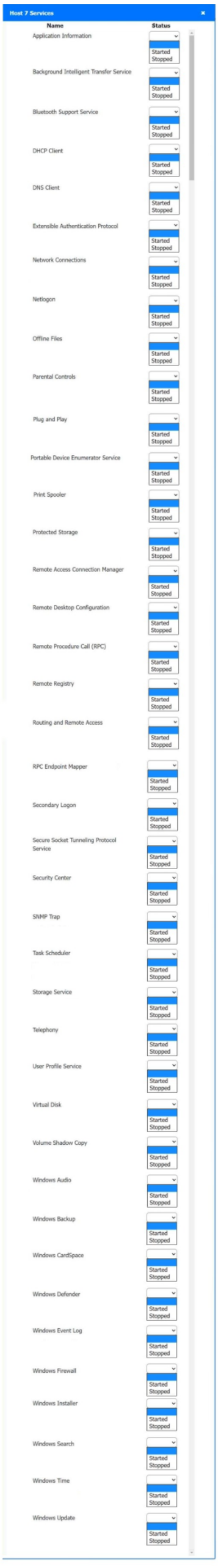


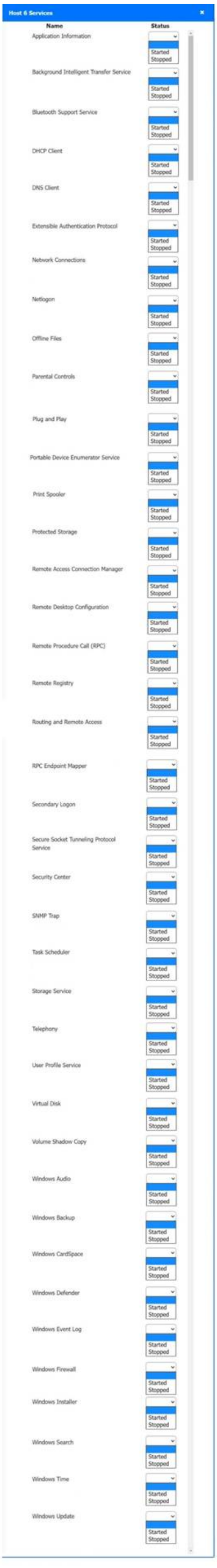

Host 2 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Persistance.j1zpxn Installer Service
Plug and Play
Portable Device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

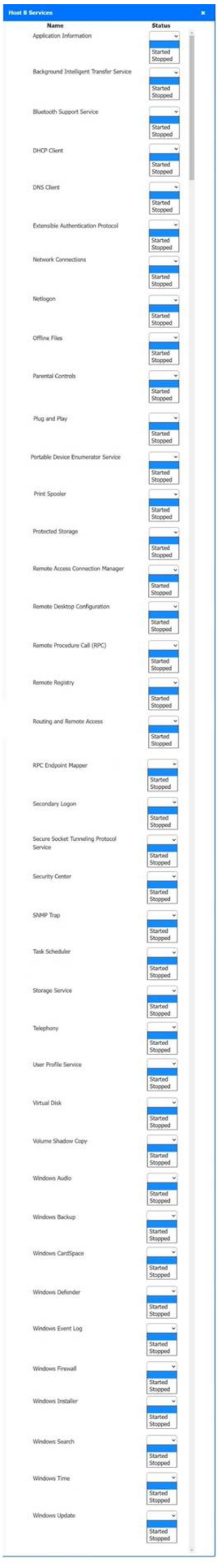

Host 3 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected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

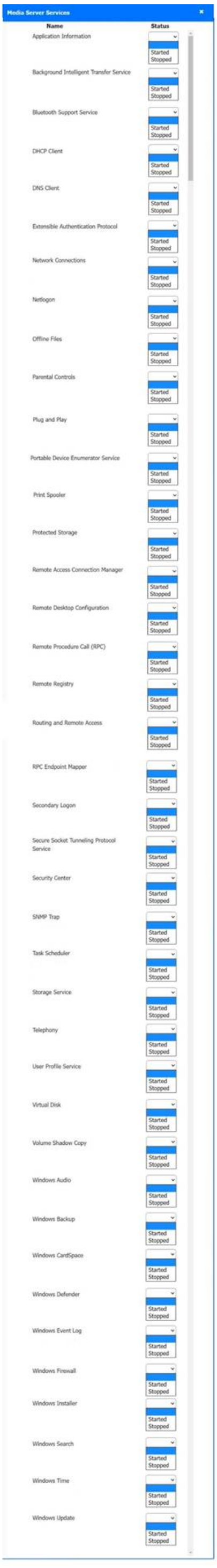

Host 4 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected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

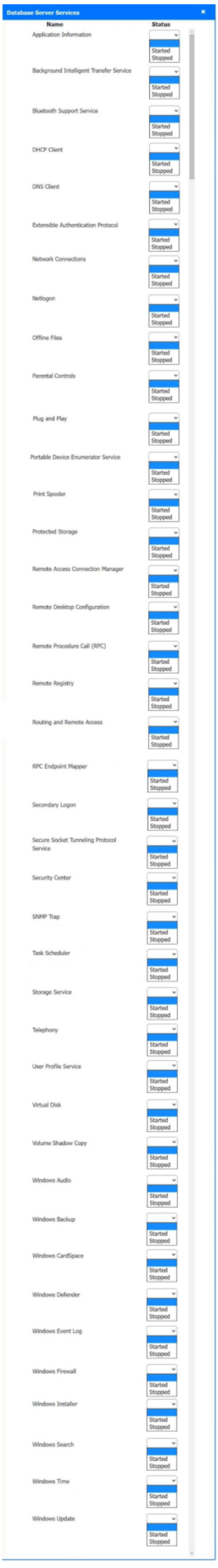

Host S Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected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

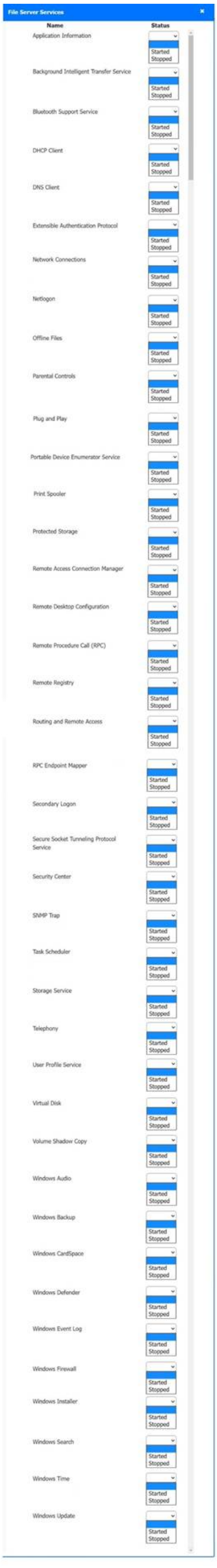

Host 7 Services
Name
Status
Application Information
Background Intelligent Transfer Service
Bluetooth Support Service
DHCP Client
DNS Client
Extensible Authentication Protocol
Network Connections
Netlogon
Offline Files
Parental Controls
Plug and Play
Portable Device Enumerator Service
Print Spooler
Protected 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
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 4
Which of the following methods involves requesting a user's approval via a push notification to verify the user's identity?

A. Call
B. Authenticator
C. Hardware token
D. SMS

Answer: B

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Authenticator apps (e.g., Microsoft Authenticator, Google Authenticator, Duo) often support push notifications. When the user logs in, the app sends a push to their mobile device, prompting the user to approve or deny the authentication request — a common and user- friendly form of multi-factor authentication (MFA).
* A. Phone call verification is a separate method involving voice-based confirmation.
* C. Hardware tokens generate one-time codes but do not send push notifications.
* D. SMS sends a text message with a code — again, no push mechanism. Reference:
CompTIA A+ 220-1102 Objective 2.2: Compare and contrast multi-factor authentication methods.
Study Guide Section: Authentication apps and push notification verification
==========

NEW QUESTION 5
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)
==========

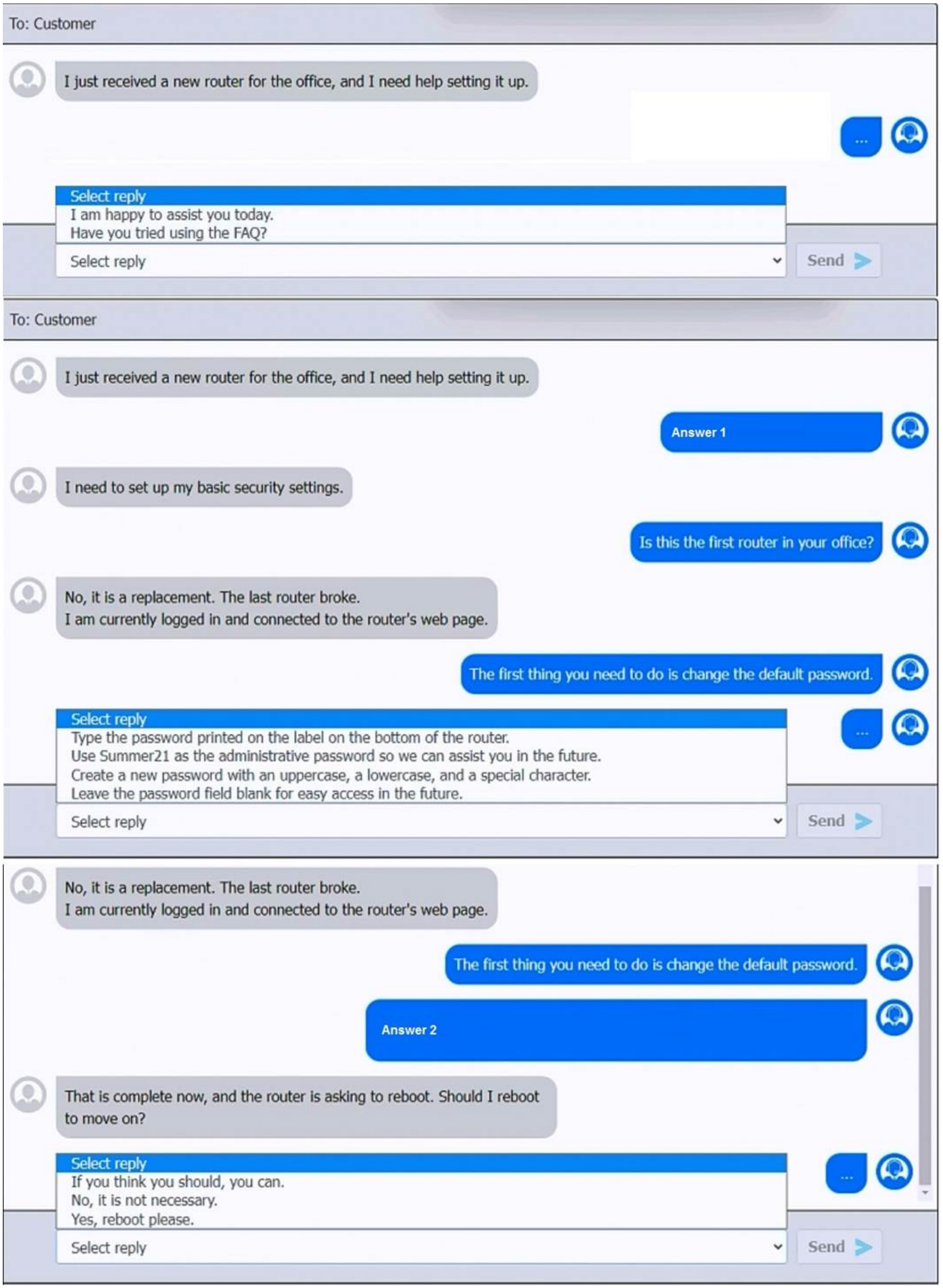
NEW QUESTION 6
A company recently transitioned to a cloud-based productivity suite and wants to secure the environment from external threat actors. Which of the following is the most effective method?

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 7
SIMULATION
You have been contacted through the help desk chat application. A user is setting up a replacement SOHO router. Assist the user with setting up the router.
INSTRUCTIONS
Select the most appropriate statement for each response. Click the send button after each response to continue the chat.
If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.



A. Mastered
B. Not Mastered

Answer: A

Explanation:
First Chat Response:When the user mentions setting up a new router, the best initial response to maintain a helpful and professional tone is:
>Select reply:"I am happy to assist you today."
Second Chat Response:When the user states that they need to set up basic security settings:
>Select reply:"Is this the first router in your office?"
Third Chat Response:After learning it's a replacement router and the user is logged into the router's web page:
>Select reply:"The first thing you need to do is change the default password."
Fourth Chat Response:For the response about password settings:
>Select reply:"Create a new password with an uppercase, a lowercase, and a special character."
Fifth Chat Response:When the router prompts to reboot:
>Select reply:"Yes, reboot please."
Study Guide Reference: The CompTIA A+ Core 2 guide highlights the importance of changing default credentials and using strong password policies, particularly in SOHO environments where routers are often targeted.

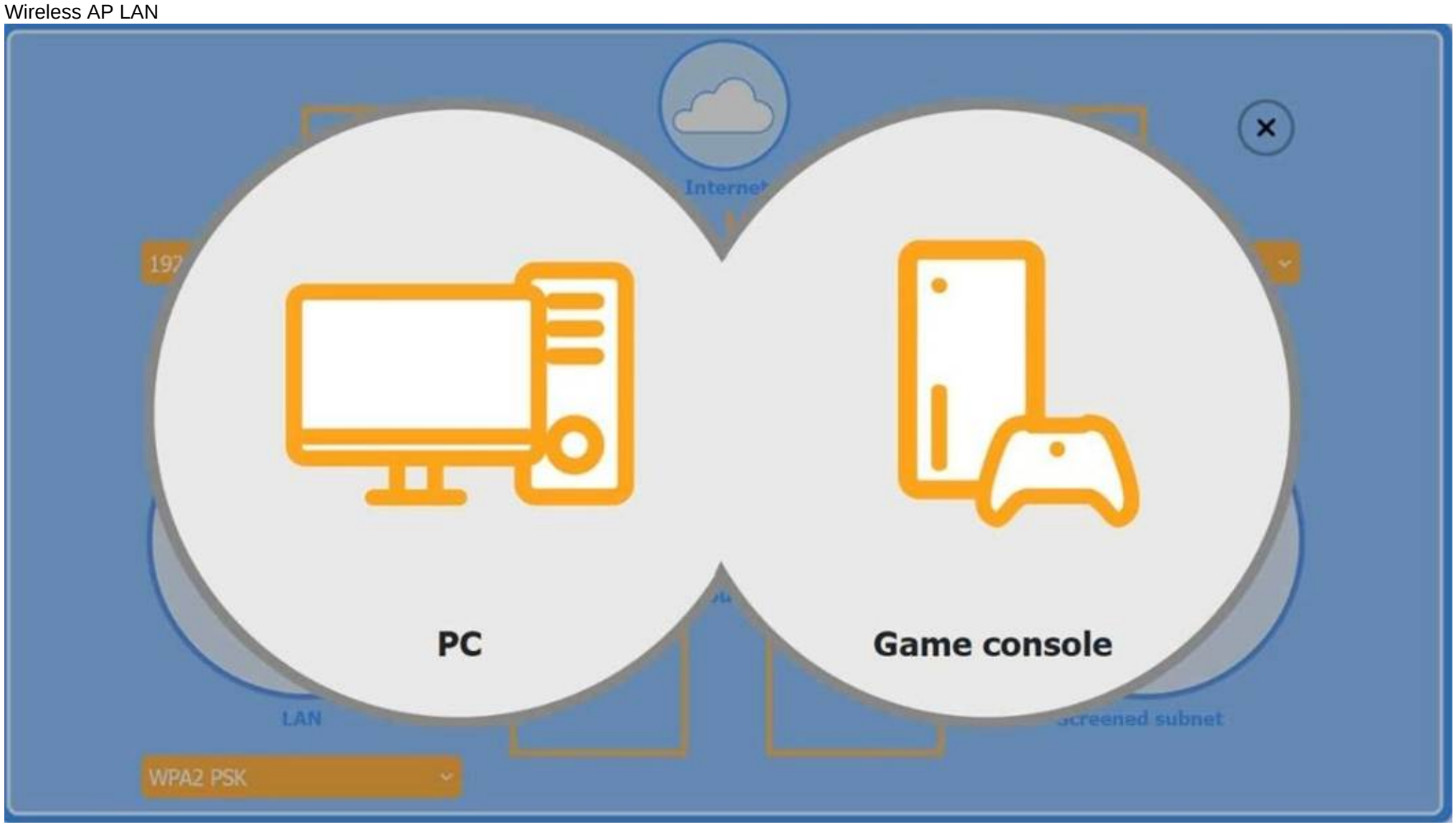
NEW QUESTION 8
A user is experiencing issues with outdated images while browsing websites. Which of the following settings should a technician use to correct this issue?

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

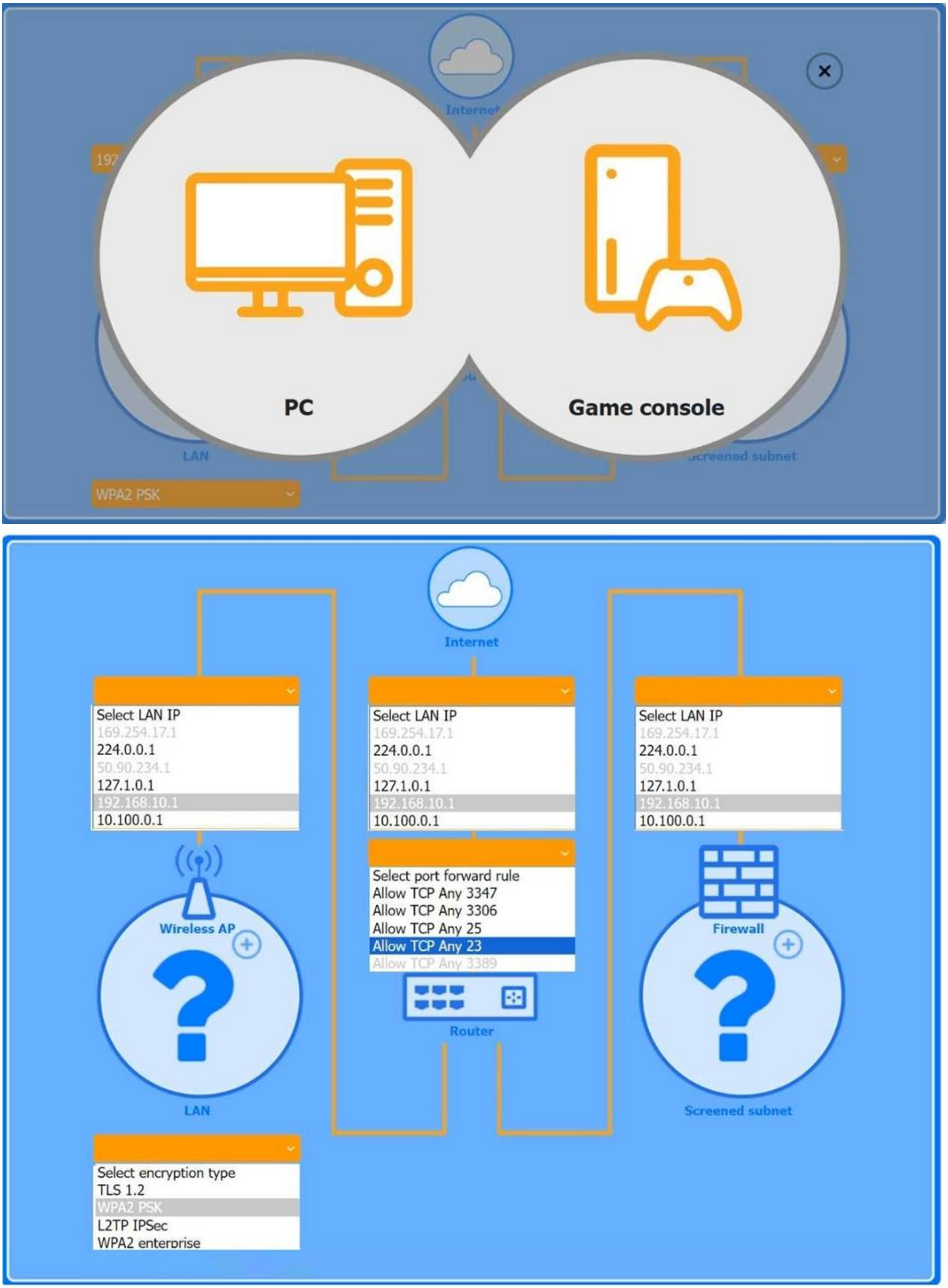
Answer: C

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 9
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 10
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 10
A technician notices that the weekly backup is taking too long to complete. The daily backups are incremental. Which of the following would most likely resolve the issue?

A. Changing the backup window
B. Performing incremental weekly backups
C. Increasing the backup storage
D. Running synthetic full weekly backups

Answer: D

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
A synthetic full backup combines the last full backup with subsequent incremental backups to create a new full backup without re-reading data from the source system. This method significantly reduces the backup window and network impact. It is especially useful when traditional full backups are too time-consuming.
* A. Changing the backup window only shifts timing, not duration.
* B. Incremental weekly backups would lack a proper full recovery point and aren't ideal alone.
* C. Storage space isn't the bottleneck in backup speed—it??s read/write operations and network load.
Reference:
CompTIA A+ 220-1102 Objective 4.2: Summarize backup and recovery concepts.
Study Guide Section: Backup types — full, incremental, differential, and synthetic backups
==========

NEW QUESTION 11
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 13
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 17
A technician is assigned to offboard a user. Which of the following are common tasks on an offboarding checklist? (Choose two.)

A. Quarantine the hard drive in the user's laptop.
B. Deactivate the user's key fobs for door access.
C. Purge all PII associated with the user.
D. Suspend the user's email account.
E. Turn off the network ports underneath the user's desk.
F. Add the MAC address of the user's computer to a blocklist.

Answer: BD

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
User offboarding involves disabling the departing user's access to company systems and
facilities. Two key tasks typically include:
? Deactivating physical access credentials (e.g., key fobs or badges) to prevent unauthorized entry (B).
? Suspending or disabling the user??s email account to prevent future use and to retain business communications (D).
* A. Quarantining a hard drive is not standard unless malware or legal issues are involved.
* C. Purging PII must follow legal retention policies; it's not typically an immediate offboarding task.
* E. Disabling network ports may be relevant in some cases but is not a standard offboarding step.
* F. Blocking MAC addresses is not typical unless the device is considered a security threat. Reference:
CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement proper documentation and offboarding procedures.
Study Guide Section: User lifecycle management — onboarding and offboarding tasks
==========

NEW QUESTION 18
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 21
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 24
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 29
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 31
A customer wants to be able to work from home but does not want to be responsible for bringingcompany 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 36
A user reports getting a BSOD (Blue Screen of Death) error on their computer at least twice a day. Which of the following should the technician use to determine the cause?

A. Event Viewer
B. Performance Monitor
C. System Information
D. Device Manager

Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Event Viewer is the primary tool used to investigate system-level errors and logs, including BSODs. When a BSOD occurs, Windows logs the error codes and associated system behavior under ??System?? logs in Event Viewer. This allows the technician to review crash events, identify error codes (e.g., STOP codes), and pinpoint hardware or driver issues.
* B. Performance Monitor is used for real-time performance tracking and trend analysis, not crash logs.
* C. System Information displays system specs but not crash logs or events.
* D. Device Manager shows device status and driver issues but doesn??t retain error logs related to BSODs.
Reference:
CompTIA A+ 220-1102 Objective 3.1: Given a scenario, troubleshoot common Windows OS problems.
Study Guide Section: Troubleshooting BSODs using Event Viewer and system logs
==========

NEW QUESTION 40
A user reports some single sign-on errors to a help desk technician. Currently, the user is able tosign 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 41
.....

Relate Links

100% Pass Your 220-1202 Exam with Exambible Prep Materials

https://www.exambible.com/220-1202-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/