CompTIA.220-1202.v2026-11-11.q209

Exam Code:	220-1202
Exam Name:	CompTIA A+ Certification Exam: Core 2
Certification Provider:	CompTIA
Free Question Number:	209
Version:	v2026-11-11
# of views:	125
# of Questions views:	2606
https://www.freecram.net/torrent/CompTIA.220-1202.v2026-11-11.q209.html	

NEW QUESTION: 1
Which of the following is the quickest way to move from Windows 10 to Windows 11 without losing data?
A. Using gpupdate
B. Image deployment
C. Clean install
D. In-place upgrade
Answer: (SHOW ANSWER)
An in-place upgrade directly installs Windows 11 over the existing Windows 10 installation, preserving user files, applications, and settings. It's much faster than capturing and redeploying an image, and it avoids the data loss risk of a clean install.

NEW QUESTION: 2
Which of the following filesystems supports read and write operations for Windows, macOS, and Linux?
A. exFAT
B. ReFS
C. NTFS
D. APFS
E. ext4
Answer: (SHOW ANSWER)
exFAT is supported by Windows, macOS, and Linux for both read and write operations, making it the most compatible file system among the options listed.

NEW QUESTION: 3

A technician completes all steps to remove malware from a computer. All scans show the infection has been removed, but the device still does not function properly. Which of the following should the technician do next?

A. Update the antivirus software.

B. Quarantine the system.

C. Enable System Restore.

D. Reimage the device.

Answer: (SHOW ANSWER)

After malware removal is complete and scans confirm the infection is gone, a system that still does not function properly may have damaged operating system files or persistent configuration issues. Reimaging restores the device to a known-good state.

NEW QUESTION: 4

A user encounters an issue where documents used by multiple team members are out of sync. Which of the following will best allow all users to make changes simultaneously?

A. Restricting permissions to the document's folder

B. Expanding the cloud file storage size limit

C. Working from a browser-based productivity suite

D. Increasing the frequency of file synchronization

Answer: (SHOW ANSWER)

The correct answer is C. Working from a browser-based productivity suite. The issue is not simply storage capacity or sync frequency; the users need simultaneous document collaboration. Browser-based suites such as Microsoft 365 or Google Workspace allow multiple users to work on the same shared document in real time, reducing version conflicts and out-of-sync copies. The All-in-One Exam Guide explains that cloud file synchronization is often bundled with productivity suites such as Microsoft 365 and Google Workspace, and that this helps users collaborate or work on the same files from multiple devices without manually moving files around. The Mike Meyers/Mark Soper material also notes that mobile versions of major productivity applications such as Microsoft 365, Google Workspace, and Apple's iCloud-based apps can synchronize data across devices. Restricting permissions may prevent editing. Expanding storage does not solve simultaneous editing. Increasing sync frequency still risks conflicts between separate local copies.

NEW QUESTION: 5

Which of the following is used to store passwords in macOS?

A. FileVault

B. Keychain

C. Accessibility

D. Mission Control

Answer: B (LEAVE A REPLY)

Keychain is the built-in macOS utility that manages and stores credentials, including passwords and certificates.

NEW QUESTION: 6
Which of the following devices can provide combined data and power to hardwired VoIP phones in a small office?
A. Router
B. Injector
C. Optical network terminal
D. PoE switch
Answer: (SHOW ANSWER)

NEW QUESTION: 7
Which of the following types of malware would most likely be detected when observing unusually high CPU usage?
A. Keylogger
B. Trojan
C. Cryptominer
D. Rootkit
Answer: (SHOW ANSWER)
Cryptominer malware uses the computer's processing power to mine cryptocurrency, which commonly causes unusually high CPU usage, slow performance, overheating, and increased fan activity.

NEW QUESTION: 8
Which of the following commands lists running processes in Linux?
A. apt-get
B. top
C. cat
D. ls
Answer: (SHOW ANSWER)

NEW QUESTION: 9
An end user is unable to print to a network printer but can access everything else on the network. Other users in the organization have no issues printing. A technician opens the print queue on the user's computer and sees the job has failed. Which of the following is the next step to troubleshoot the issue?
A. Printing a test document from another computer on the network
B. Restarting the print spooler from services
C. Removing the printer from the computer and reinstalling it
D. Starting the computer again and attempting to print again
Answer: (SHOW ANSWER)

Since other users can print and the job has failed in the local print queue, the issue is likely related to the print spooler service on the user's machine. Restarting the print spooler clears stalled jobs and resets the printing service, allowing new print jobs to process correctly.

NEW QUESTION: 10

A user called the help desk to report an issue with the internet connection speed on a laptop. The technician thinks that background services may be using extra bandwidth. Which of the following tools should the technician use to investigate connections on the laptop?

Freecram.net

A. nslookup
B. net use
C. netstat
D. net user
Answer: (SHOW ANSWER)
The netstat tool displays active network connections and listening ports, allowing the technician to identify background services and processes that may be using extra bandwidth on the laptop.

NEW QUESTION: 11
A technician needs to map a shared drive from a command-line interface. Which of the following commands should the technician use?
A. pathping
B. nslookup
C. net use
D. tracert
Answer: C (LEAVE A REPLY)
The Windows net use command is used to connect, remove, and configure connections to shared network resources. To map a shared drive from the CLI, you'd run a command like:
net use Z: \\ServerName\ShareName
This assigns the shared folder to drive letter Z:.

NEW QUESTION: 12
Which of the following commands is used to validate the IP settings of a Windows OS?
A. ipconfig
B. net use
C. route print
D. ping
Answer: (SHOW ANSWER)
The ipconfig command displays the current TCP/IP configuration of a Windows system, including IP address, subnet mask, default gateway, and DNS information. This allows a technician to validate and troubleshoot the system's IP settings directly from the command line.

NEW QUESTION: 13

A user is trying to install a preferred word processor on their work laptop, but the installation fails each time. Which of the following is most likely the cause of this failure?

A. Full browser cache

B. Slow internet speeds

C. Incorrectly configured ACL

D. Unformatted hard drive

Answer: (SHOW ANSWER)

An incorrectly configured access control list can prevent the user from having the necessary permissions to install software. If the user lacks write or execute permissions on required directories or system areas, the installation process will fail.

NEW QUESTION: 14

Which of the following methods would make data unrecoverable but allow the drive to be repurposed?

A. Deleting the partitions

B. Implementing EFS

C. Performing a low-level format

D. Degaussing the device

Answer: C (LEAVE A REPLY)

A low-level format (more accurately, a secure erase that overwrites all sectors with zeroes or random data) effectively wipes all data on the drive, making previous content unrecoverable while leaving the drive's structure intact for reuse. Unlike degaussing - which destroys the drive's magnetic media and renders it unusable - overwriting allows the drive to be repurposed safely.

NEW QUESTION: 15

A technician verifies that a malware incident occurred on some computers in a small office. Which of the following should the technician do next?

A. Quarantine the infected systems.

B. Educate the end users.

C. Disable System Restore.

D. Update the anti-malware and scan the computers.

Answer: (SHOW ANSWER)

Once an incident is confirmed, the immediate priority is containment. Isolating (quarantining) the infected machines prevents the malware from spreading to other systems or exfiltrating data, enabling safe analysis and remediation.

NEW QUESTION: 16

A company wants to use a single operating system for its workstation 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: (SHOW ANSWER)
Linux distributions are open-source and generally free of licensing fees, making them suitable for both desktop workstations and servers. Organizations can use the same Linux OS across all their systems without incurring per-seat or per-server costs, unlike proprietary systems such as Windows or macOS.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 17
After completing malware removal steps, what is the next step the technician should take?
A. Perform a secondary antivirus scan
B. Educate the end user
C. Reimage the computer
D. Review system logs
Answer: (SHOW ANSWER)
End-user education is crucial after malware removal to prevent recurrence. Teaching safe browsing habits and security awareness completes the remediation cycle.

NEW QUESTION: 18
Which of the following authentication methods is token-based?
A. Kerberos
B. TACACS+
C. Passwords
D. TKIP
Answer: (SHOW ANSWER)
TACACS+ (Terminal Access Controller Access-Control System Plus) is a token-based authentication protocol that can use tokens (such as one-time passwords or security tokens) for authenticating users.

NEW QUESTION: 19

An administrator is investigating a zero-day vulnerability on a core system. If the vulnerability is not patched, the negative impact to business could be significant. The vendor has released a patch, but it requires downtime to deploy. Which of the following actions should the administrator take?

A. Create a standard change request.

B. Implement an emergency change.

C. Immediately freeze all changes.

D. Continue operations until the next change interval.

Answer: B (LEAVE A REPLY)

An emergency change is appropriate when a critical vulnerability poses significant business risk and must be addressed immediately, even if downtime is required.

NEW QUESTION: 20

An international traveler is concerned about others accessing the contents of their smartphone if it is lost or stolen. The traveler has enabled biometrics. Which of the following additional security measures further reduces the risk of unauthorized data access?

Freecram.net

A. Remote backups

B. Location tracking

C. PIN code screen lock

D. Device encryption

Answer: (SHOW ANSWER)

Device encryption further reduces the risk of unauthorized data access by ensuring the contents of the smartphone cannot be read without proper authentication, even if the device is lost or stolen.

NEW QUESTION: 21

A systems administrator logs in to a developer's machine to update the system and notices a performance issue. To troubleshoot the issue, the administrator attempts to open Task Manager multiple times, but it does not open. Which of the following is most likely the cause of this issue?

A. A software development application is running

B. Windows Update Service is set to manual

C. The operating system has a malware infection

D. A page file was moved to D:\ drive

Answer: (SHOW ANSWER)

Malware commonly disables system utilities such as Task Manager to prevent detection and termination of malicious processes, which explains why Task Manager fails to open despite multiple attempts.

NEW QUESTION: 22

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

A. Restricted log-in times

B. Secure master password

C. TPM module
D. Windows lock screen
Answer: (SHOW ANSWER)
A credential manager encrypts and stores multiple credentials behind a single master password. Ensuring that this master password is strong and kept secure is critical; if it's compromised, all stored credentials become vulnerable.

NEW QUESTION: 23
Multiple users clicked a phishing link from a compromised email account. The security team isolates and removes the threat. Then, the management team provides security awareness training to the company. What step is this?
A. Provide user education.
B. Compile lessons learned.
C. Update the antivirus software.
D. Perform additional scans.
Answer: A (LEAVE A REPLY)
This is part of the user education step after a security incident to prevent future occurrences.

NEW QUESTION: 24
Which of the following is used to identify potential issues with a proposed change prior to implementation?
A. Request form
B. Rollback plan
C. End-user acceptance
D. Sandbox testing
Answer: (SHOW ANSWER)
Sandbox testing allows proposed changes to be evaluated in an isolated environment to identify potential issues before implementation.

NEW QUESTION: 25
A junior technician is working on a customer request. The junior technician cannot complete the work and escalates the issue to a senior technician. The senior technician completes the work, but the outcome does not match the customer's request. Which of the following communication techniques should the junior technician have followed?
A. Ask open-ended questions to verify understanding.
B. Maintain a positive attitude and project confidence.
C. Avoid dismissing the customer's issues.
D. Use proper language and avoid jargon.
Answer: (SHOW ANSWER)
Asking open-ended questions helps clarify the customer's actual needs and verify understanding before escalating, reducing the chance of miscommunication and incorrect outcomes.

NEW QUESTION: 26
A user is unable to log in to the network. The network uses 802.1X with EAP-TLS to authenticate on the wired network. The user has been on an extended leave and has not logged in to the computer in several months. Which of the following is causing the login issue?
A. Expired certificate
B. OS update failure
C. Service not started
D. Application crash
E. Profile rebuild needed
Answer: (SHOW ANSWER)
EAP-TLS authentication relies on digital certificates. If the user has not logged in for several months, their authentication certificate may have expired, preventing successful network login.

NEW QUESTION: 27
A user's workstation was infected with a newly discovered virus that the AV system detected. After a full virus scan and a workstation reboot, the virus is still present in the OS. Which of the following actions should the user take to remove the virus?
A. Run the operating system update process.
B. Use bootable antivirus media to scan the system.
C. Enable the system firewall.
D. Download software designed to specifically target the virus.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
An IT technician is attempting to install a video-rendering application for a client when the installation program halts. The technician sees an error message about the system not meeting the VRAM requirement. The system has a popular, integrated video solution and twice the required DRAM. Which of the following should the technician access to meet the VRAM requirement?
A. Device Manager
B. Virtual RAM
C. BIOS options
D. System Configuration
Answer: (SHOW ANSWER)
Integrated video solutions use system memory as shared video memory, and the amount allocated to VRAM is configured in the BIOS. Adjusting BIOS options allows the technician to increase the VRAM allocation to meet the application's requirements.

NEW QUESTION: 29
Which of the following are system folders on macOS? (Choose two)
A. Applications

B. Spotlight
C. Time Machine
D. Library
E. FileVault
F. iCloud
Answer: (SHOW ANSWER)
Applications and Library are core system directories in macOS. The Applications folder contains installed applications. The Library folder contains support files, preferences, and other system-related files.

NEW QUESTION: 30
A Chief Executive Officer wants to meet with remote employees in a way that will allow for collaboration and training. Which of the following software technologies is the best for this situation?
Freecram.net
A. Videoconferencing
B. Screen sharing
C. Remote Desktop Protocol
D. Virtual desktop infrastructure
Answer: (SHOW ANSWER)
Videoconferencing software enables collaboration and training with remote employees, allowing for real-time meetings and interaction.

NEW QUESTION: 31
An employee is using a photo editing program. Certain features are disabled and require a log-in, which the employee does not have. Which of the following is a way to resolve this issue?
A. License assignment
B. VPN connection
C. Application repair
D. Program reinstallation
Answer: (SHOW ANSWER)
When features in an application are disabled pending a login, it typically indicates those capabilities are controlled by the software's licensing system. Assigning (or activating) the proper license entitles the user to those premium features, restoring full functionality without unnecessary repair or reinstall steps.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here:

https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 32
A user reports that the time on their computer does not match the time on their VoIP phone. What should a technician do?
A. Confirm the user is logging in to the domain.
B. Manually set the time on the phone to match the computer.
C. Download and install the latest BIOS update.
D. Configure access to an available NTP server.
Answer: (SHOW ANSWER)
This scenario involves a mismatch in device time settings, which can affect synchronization and authentication across the network. Using a Network Time Protocol (NTP) server ensures all networked devices maintain accurate and synchronized clocks.

NEW QUESTION: 33
A technician recently installed a program that uses several anti-piracy technologies. When the program is launched, it briefly opens and then closes. Which of the following is most likely the reason?
A. 32-bit program on a 64-bit computer
B. CPU incompatibility
C. Outdated video card drivers
D. USB key not plugged in
Answer: (SHOW ANSWER)
Many anti-piracy technologies require a USB key (dongle) to be plugged in for the program to run; if it is missing, the program will open and then immediately close.

NEW QUESTION: 34
An administrator is investigating a zero-day vulnerability. If left unpatched, it could severely impact business. The patch requires downtime. What should the administrator do?
A. Create a standard change request.
B. Implement an emergency change.
C. Immediately freeze all changes.
D. Continue operations until the next change interval.
Answer: (SHOW ANSWER)
A zero-day vulnerability demands an emergency change to quickly secure the system, even if downtime is needed.

NEW QUESTION: 35
A user's computer is connected with LAN IP address 10.203.10.12 and a gateway set to

10.203.10.1. The computer is not able to connect to any resources. Which of the following should the technician use to check communication?

A. ipconfig 10.203.10.12

B. nslookup 10.203.10.1

C. ping 10.203.10.1

D. net use

Answer: C (LEAVE A REPLY)

The correct answer is C. ping 10.203.10.1. The technician should test whether the computer can communicate with its default gateway. Quentin Docter's Complete Study Guide explains that the ping command verifies network connectivity using ICMP packets and that a common troubleshooting step is to ping the default gateway. If the gateway responds, the system has basic connectivity to that device. The All-in-One Exam Guide also states that ping is a great way to determine whether a computer can talk to another system by sending packets to an IP address or DNS name. ipconfig is used to view TCP/IP configuration, not to ping an address in that syntax. nslookup checks DNS resolution, which is not the first test for reaching the gateway. net use maps or manages network resources, but it does not directly test gateway communication.

NEW QUESTION: 36

A location is experiencing under-voltage events during peak periods. Which of the following should be deployed at this location?

A. Proper ventilation

B. Surge protector

C. PDU

D. UPS

Answer: (SHOW ANSWER)

NEW QUESTION: 37

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: (SHOW ANSWER)

A rogue access point mimics the legitimate SSID, allowing clients to connect (often with internet access via its own uplink) but isolating them from internal resources like file shares. This behavior matches the symptoms - users join what appears to be the corporate WLAN but can't reach internal servers.

NEW QUESTION: 38

Which of the following should an organization use when it wants to enable SSO for a third-party application by utilizing its existing identity service?

A. OTP

B. ACL

C. SAML

D. UAC

Answer: (SHOW ANSWER)

The correct answer is C. SAML. Security Assertion Markup Language is commonly used for single sign-on between an identity provider and a service provider, especially when an organization wants a third-party application to trust its existing identity service. The CompTIA A+ objectives include SSO, meaning single sign-on, and the objectives' acronym list identifies SSO as a relevant exam term. In this scenario, the organization wants users to authenticate through its existing identity system rather than maintaining separate credentials for the third-party application. SAML is the best match because it passes authentication assertions between trusted parties. OTP means one-time password and is an authentication factor, not an SSO federation standard. ACL means access control list and controls permissions to resources. UAC is Windows User Account Control, which prompts for administrative approval on a local system. Therefore, SAML is the correct technology for third-party SSO integration.

NEW QUESTION: 39

Whenever a user clicks on a .jpg, Notepad opens and displays illegible characters. Otherwise, the workstation functions normally. Which of the following is the most likely cause of this issue?

A. The workstation has been infected with malware.

B. The default application for image files is misconfigured.

C. The operating system needs the most current update.

D. A new image editor needs to be installed on the user's computer.

Answer: (SHOW ANSWER)

The behavior indicates that Windows is opening .jpg files with the wrong default application. Correcting the file association resolves the issue.

NEW QUESTION: 40

A busy network printer is producing faded printouts after a technician performed maintenance on the printer several months ago. The technician now replaces the toner cartridge, but the issue persists. Which of the following should the technician check next?

Freecram.net

A. The firmware version

B. The paper type

C. The drum unit for wear

D. The print resolution settings

Answer: C (LEAVE A REPLY)

If replacing the toner does not resolve faded prints, the next likely cause is a worn drum unit, which is responsible for transferring toner to paper and degrades over time, leading to poor print quality.

NEW QUESTION: 41

SIMULATION 5

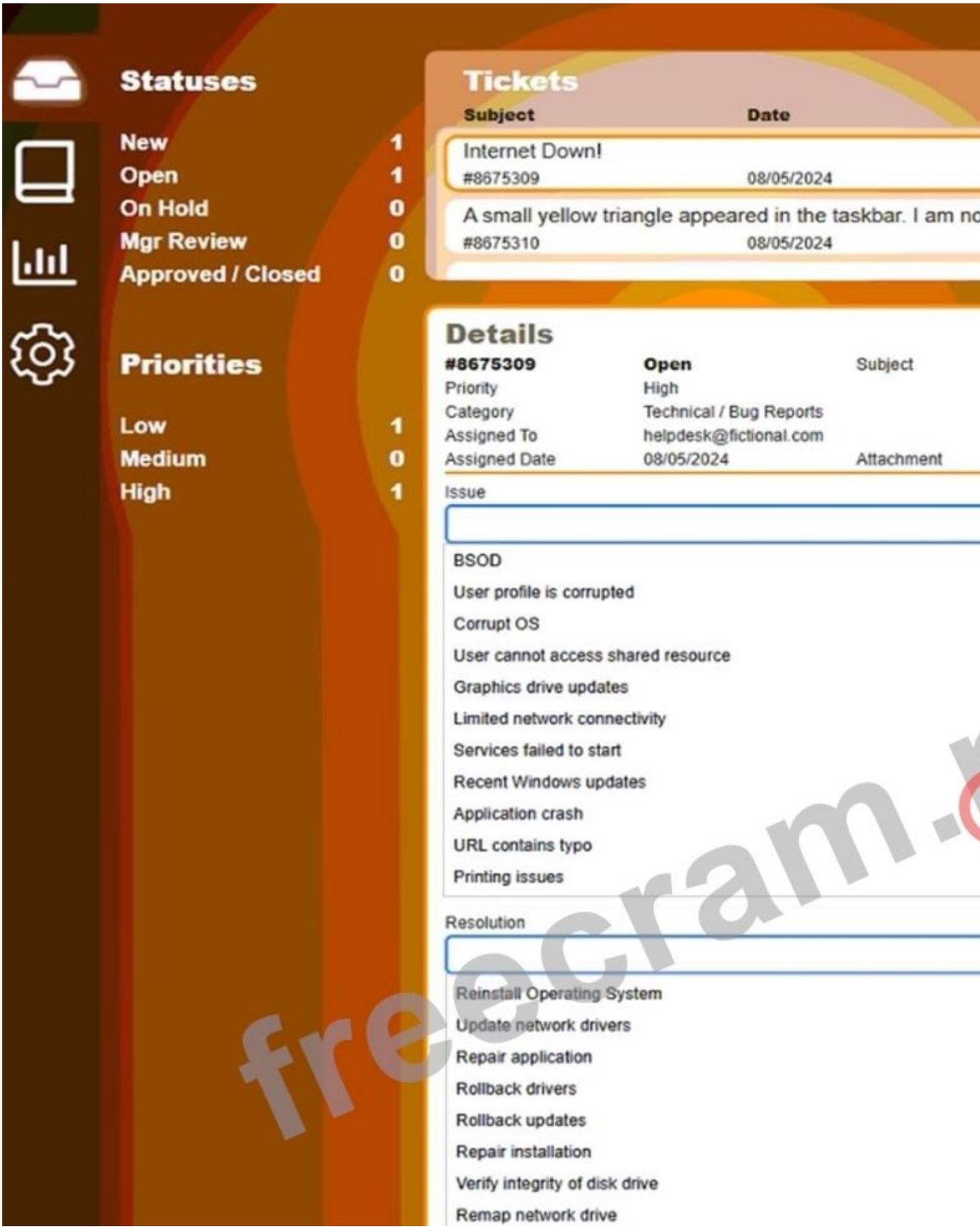
Welcome to your first day as a Fictional Company, LLC helpdesk employee. Please work the tickets in your helpdesk ticket queue.

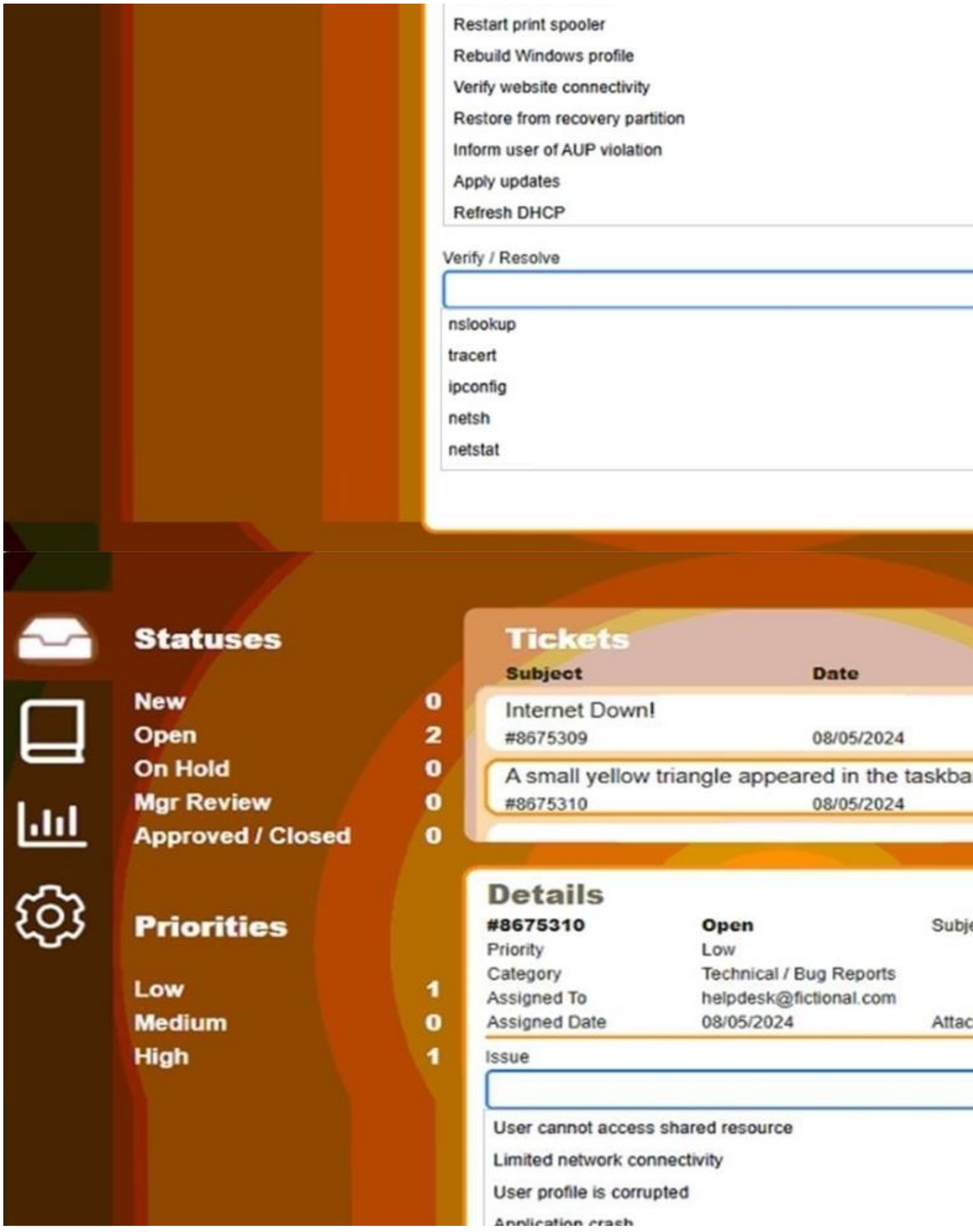
INSTRUCTIONS

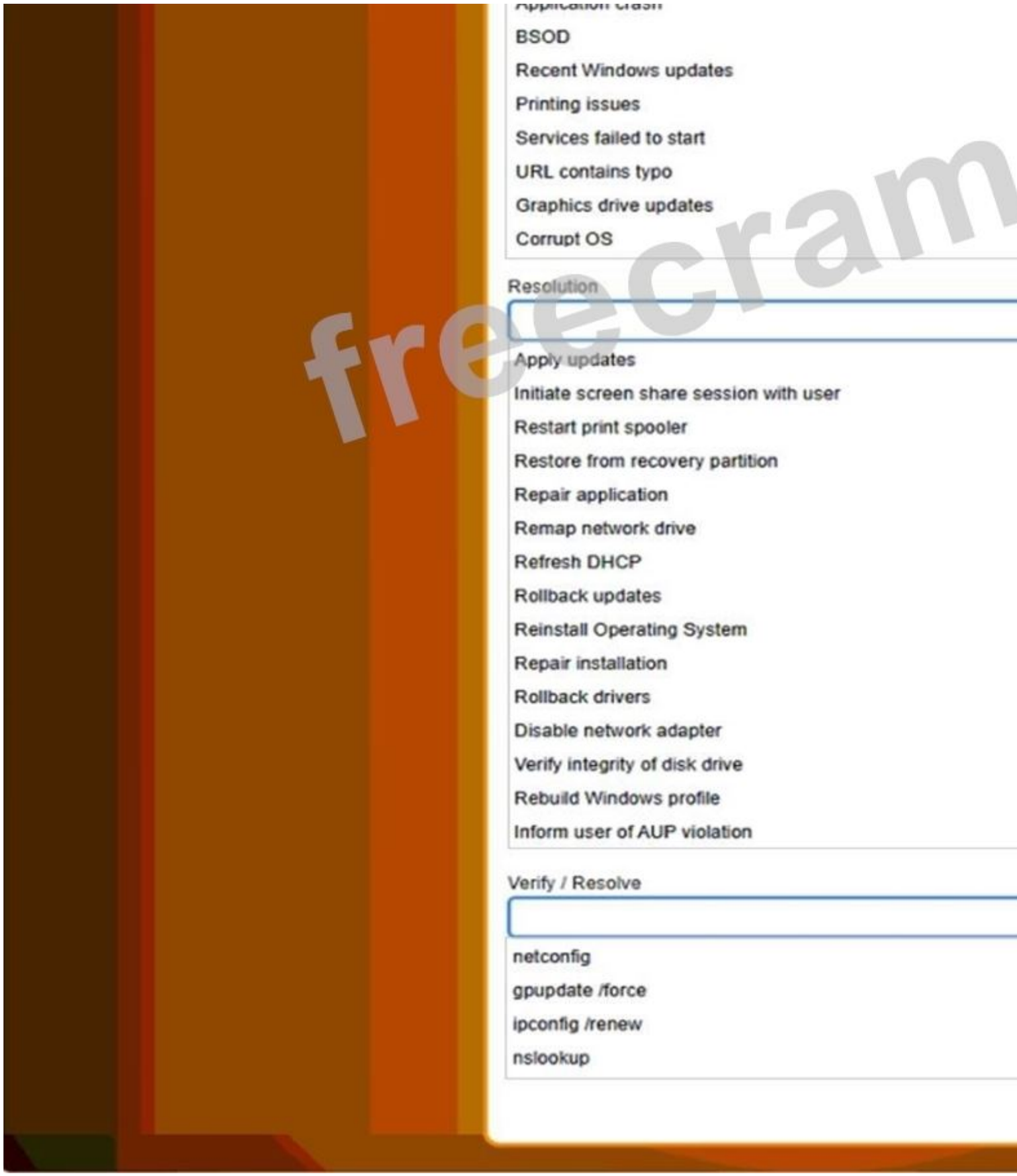
Click on individual tickets to see the ticket details, and view applicable attachments to determine the problem.

Select the appropriate issue from the 'Issue' drop-down menu. Then, select the most efficient resolution from the 'Resolution' drop-down menu. Finally, select the proper command or verification to remediate or confirm your fix of the issue from the 'Verify/Resolve' drop-down menu.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.


Statuses
New 1
Open 1
On Hold 0
Mgr Review 0
Approved / Closed 0
Priorities
Low 1
Medium 0
High 1
Tickets
Subject
Date
Internet Down!
#8675309
08/05/2024
A small yellow triangle appeared in the taskbar. I am no
#8675310
08/05/2024
Details
#8675309
Open
Subject
Priority
High
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
08/05/2024
Attachment
Issue
BSOD
User profile is corrupted
Corrupt OS
User cannot access shared resource
Graphics drive updates
Limited network connectivity
Services failed to start
Recent Windows updates
Application crash
URL contains typo
Printing issues
Resolution
Reinstall Operating System
Update network drivers
Repair application
Rollback drivers
Rollback updates
Repair installation
Verify integrity of disk drive
Remap network drive
freecram.


Restart print spooler
Rebuild Windows profile
Verify website connectivity
Restore from recovery partition
Inform user of AUP violation
Apply updates
Refresh DHCP
Verify / Resolve
nslookup
tracert
ipconfig
netsh
netstat
Statuses
New 0
Open 2
On Hold 0
Mgr Review 0
Approved / Closed 0
Priorities
Low 1
Medium 0
High 1
Tickets
Subject
Date
Internet Down!
#8675309
08/05/2024
A small yellow triangle appeared in the taskba
#8675310
08/05/2024
Details
#8675310
Open
Priority
Low
Category
Technical / Bug Reports
Assigned To
helpdesk@fictional.com
Assigned Date
08/05/2024
Issue
User cannot access shared resource
Limited network connectivity
User profile is corrupted



Answer:

Ticket #8675309

Limited network connectivity

Update network drivers
ipconfig
The ticket indicates "Internet Down," which aligns with limited network connectivity. Updating the network drivers is the most efficient fix when connectivity is lost due to adapter or driver issues. Using ipconfig verifies proper IP configuration after the driver update to confirm restored connectivity.
Ticket #8675310
Limited network connectivity
Refresh DHCP
ipconfig /renew
A small yellow triangle in the taskbar indicates limited connectivity, commonly caused by an invalid or missing IP address from DHCP. Refreshing DHCP forces the system to request a new IP configuration. Using ipconfig /renew verifies that the client successfully obtains a valid IP address and restores network access.

NEW QUESTION: 42
An administrator must write a script that will output the host name to a file. Which of the following commands is the best way to accomplish this task?
A. hostname
B. netstat
C. whoami
D. winver
Answer: (SHOW ANSWER)
The correct answer is A. hostname. I corrected the wording from "OS name" to "host name" because, based on the answer choices, this question is testing the command that displays the computer's host name. Quentin Docter's Complete Study Guide explains that the hostname command returns the name of the host computer on which it is executed. This makes it appropriate for scripting because its output can be redirected to a file, such as hostname > computername.txt. The CompTIA A+ Core 2 objectives also list hostname, netstat, whoami, and winver as Windows command-line tools candidates should recognize. netstat displays active TCP/IP connections and network statistics, not the computer name. whoami displays the currently logged-in user account. winver displays Windows version information, but it opens a graphical dialog and is not the best option for writing simple script output to a file.

NEW QUESTION: 43
Which of the following are system folders on the macOS? (Choose two.)
A. Applications
B. Spotlight
C. Time Machine
D. Library
E. FileVault

F. iCloud

Answer: (SHOW ANSWER)

Applications is a core macOS system folder that stores installed apps.
Library is a system folder that contains system and user resources required by macOS and applications.

NEW QUESTION: 44

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: (SHOW ANSWER)

Windows includes .NET Framework 3.5 as an optional feature. Enabling it via Control Panel Programs and Features Turn Windows features on or off ensures the OS installs the correct version directly from Microsoft without relying on untrusted sources or skipping needed dependencies.

NEW QUESTION: 45

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: (SHOW ANSWER)

Since the fix did not persist and the issue recurred, it indicates there may be an underlying configuration or policy problem that requires deeper troubleshooting than a frontline technician can provide. Escalating to the next support tier ensures that the root cause is identified and a more permanent solution is implemented, rather than repeatedly applying a temporary workaround.

NEW QUESTION: 46

A user's new laptop, which was advertised as gaming ready, is performing slowly when the user is playing a modern game. However, when the user is playing a less resource-demanding game, the user does not see any lag. Which of the following should a technician do to resolve the issue?

A. Overclock the RAM.

B. Enable NIC teaming.

C. Select dedicated graphics.

D. Activate CPU hyperthreading.

Answer: (SHOW ANSWER)

Modern games require significant graphical processing power, and systems with both integrated and dedicated graphics may default to the integrated option to save power. Selecting the dedicated graphics processor ensures the game uses the more powerful GPU, resolving performance issues during demanding gameplay.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 47

A user wants to use a USB to move a 4.57GB .pst file from one Windows computer to another. Which of the following filesystems should the USB be formatted with?

A. ext4

B. NTFS

C. FAT32

D. APFS

Answer: (SHOW ANSWER)

FAT32 cannot support files larger than 4GB. NTFS supports large file sizes and is compatible across Windows systems, making it the correct choice for transferring a 4.57GB file.

NEW QUESTION: 48

A secretary receives an email from the company's chief executive officer with a request to pay a vendor immediately. After the payment is made, the chief executive officer tells the secretary that they never sent that email. Which of the following social engineering tactics best describes this type of attack?

A. Evil twin

B. Impersonation

C. Whaling

D. Spear phishing

Answer: (SHOW ANSWER)

This is a classic Business Email Compromise (BEC) scam - the attacker pretended to be (impersonated) the CEO in order to trick the secretary into making an urgent payment. The key detail is that the attacker assumed someone else's identity (the CEO) to exploit the trust and authority associated with that role.

NEW QUESTION: 49
A user needs to install and uninstall software on their Windows laptop but does not need to manage user accounts. The company follows least-privilege principles. Which of the following account types meets these requirements?
A. Guest
B. Power user
C. Service
D. Administrator
Answer: (SHOW ANSWER)
A Power User account allows installing and uninstalling software but does not grant full administrative control, aligning with the principle of least privilege.

NEW QUESTION: 50
Which of the following is occurring when a vulnerability is placed inside of a software package without the vendor's knowledge and it is deployed to customers?
Freecram.net
A. Zero-day attack
B. Brute-force attack
C. Dictionary attack
D. Supply chain attack
Answer: D (LEAVE A REPLY)
A supply chain attack occurs when malicious code or vulnerabilities are introduced into software during development or distribution without the vendor's knowledge, and then delivered to customers through trusted channels.

NEW QUESTION: 51
A technician installs a Bluetooth headset for a user. During testing, the sound is still coming from the speaker on the computer. The technician verifies the headset shows up in Device Manager.
Which of the following would the technician most likely do to fix this issue?
A. Update the drivers for the wireless headset
B. Replace the battery on the headset and try again later
C. Verify that the sound is not muted in the control panel
D. Change the headset as the default device in sound settings
Answer: (SHOW ANSWER)
The technician should change the headset to the default device in the sound settings to ensure audio is routed to the Bluetooth headset instead of the computer's speakers.
NEW QUESTION: 52
Which of the following is the most secure method of preventing someone from accessing a cell phone?
A. PIN
B. Swipe
C. Passphrase

D. Pattern

Answer: (SHOW ANSWER)

A passphrase is typically longer and more complex than a PIN, swipe, or pattern, making it the most secure method for preventing unauthorized access to a cell phone.

NEW QUESTION: 53

A utility failure causes a workstation to immediately shut down. Which of the following would help prevent this from reoccurring?

A. Surge suppressor

B. Uninterruptible power supply

C. Line voltage regulator

D. Redundant PSU

Answer: (SHOW ANSWER)

This device provides temporary battery power during a utility power loss, allowing the workstation to continue running or shut down gracefully instead of immediately powering off.

NEW QUESTION: 54

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: (SHOW ANSWER)

In Internet Options (under the Browsing History Settings), you can configure how often the browser checks for newer versions of stored pages and content. Adjusting the "Check for newer versions of stored pages" setting forces the browser to retrieve up-to-date images rather than using cached copies.

NEW QUESTION: 55

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

A. Bollards

B. Video surveillance

C. Badge readers

D. Fence

Answer: (SHOW ANSWER)

Badge readers authenticate and log each entry attempt - recording who accessed (or tried to access) a secured area and when. This audit trail is essential for monitoring and reviewing access to restricted zones.

NEW QUESTION: 56

Which of the following is provided to a user during MFA?

A. TOTP

B. DLP

C. FRT

D. MDM

Answer: (SHOW ANSWER)

Time-based One-Time Passwords are provided to users during multifactor authentication as a temporary, dynamically generated code. This code serves as an additional authentication factor beyond a username and password, enhancing security by requiring something the user has in addition to something they know.

NEW QUESTION: 57

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: (SHOW ANSWER)

Event Viewer logs system, application, and service events, including errors and warnings when a service stops unexpectedly. Reviewing these logs provides detailed error codes and messages that help identify the root cause of the service interruptions.

NEW QUESTION: 58

A technician receives a ticket from a user that reads, "My computer is having issues." Which of the following should the technician do next?

A. Review the user's system resources.

B. Ask the user to resubmit a ticket with more information.

C. Upgrade the user's computer.

D. Ask the user follow-up questions.

Answer: (SHOW ANSWER)

Asking follow-up questions allows the technician to gather the details needed to diagnose the vague issue described in the ticket.

NEW QUESTION: 59

A technician needs to prevent accidental access to Wi-Fi networks available in a shared office space. The BYOD and company-owned devices already have Wi-Fi settings configured via MDM solutions. Which of the following settings should the technician change?

A. IP filtering configuration

B. SSID configuration

C. Content filtering configuration

D. Port forwarding/mapping

Answer: (SHOW ANSWER)

The correct answer is B. SSID configuration, because controlling SSID visibility and behavior directly affects which wireless networks devices can see and attempt to join. In shared office environments, multiple Wi-Fi networks may be present, increasing the risk of users accidentally connecting to the wrong network.

NEW QUESTION: 60

When logging in to a workstation, a technician notices that the roaming profile takes a long time to fully load. Which of the following should the technician check first to troubleshoot this issue?

Freecram.net

A. The home folder for large files

B. The hard drive storage usage

C. The PSU's power output

D. Task Manager for unresponsive applications

Answer: (SHOW ANSWER)

Large files stored in the home folder increase the size of the roaming profile, causing slow login times as the profile is copied across the network. Checking for large files is the first and most direct step.

NEW QUESTION: 61

A user reports getting a BSOD 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: (SHOW ANSWER)

Event Viewer logs system errors, including the critical events that lead up to and include Blue Screen of Death (BSOD) incidents. By reviewing the "System" and "Application" logs, especially the error entries and any bugcheck codes, you can identify the faulting driver, service, or hardware component responsible for the crashes.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 62

An administrator is investigating a technical outage. The management team wants information that includes the summary of the outage and actions taken. Which of the following documentation should

the administrator provide to the management team?

A. Knowledge base article

B. Non-disclosure agreement

C. Incident report

D. Standard operating procedure

Answer: (SHOW ANSWER)

An incident report documents key details such as the cause of the outage, steps taken to resolve it, and measures to prevent recurrence. It is a post-mortem analysis often shared with stakeholders to improve future response.

NEW QUESTION: 63

Which of the following data destruction methods is most appropriate to ensure that classified information on hard drives cannot be recovered?

A. Overwriting with a software-based secure erase program

B. Degaussing followed by physical shredding

C. Formatting with a low-level format tool

D. Encrypting the drives and storing them securely

Answer: (SHOW ANSWER)

Degaussing removes all magnetic data on the drive, and physical shredding ensures the remaining media cannot be reconstructed, making this combination the most secure method for destroying classified information.

NEW QUESTION: 64

An employee's corporate phone is experiencing connectivity issues. The user is unable to access the internet, send emails, or use business applications outside the office. The device is not in airplane mode, and Wi-Fi is turned off. Which of the following is the most likely cause of the issue?

A. The SIM is malfunctioning and needs to be replaced.

B. The user has exceeded the phone's mobile data plan.

C. The SSID settings are misconfigured.

D. The phone is missing security updates.

Answer: (SHOW ANSWER)

If Wi-Fi is turned off and the user cannot access internet services outside the office, the device relies on cellular data. Exceeding the mobile data plan can result in restricted or blocked data access, preventing internet connectivity, email, and application usage.

NEW QUESTION: 65

An administrator must configure computers for remote users. The computers will be shipped directly to users from the manufacturer. Which of the following solutions should the administrator use?

A. Clean install

B. Zero-touch deployment

C. Remote Desktop Protocol

D. Private cloud

Answer: (SHOW ANSWER)

Zero-touch deployment allows devices to be preconfigured and automatically provisioned when first powered on by the end user. This enables remote users to receive systems directly from the manufacturer and have them automatically configured with corporate settings without manual IT intervention.

NEW QUESTION: 66

A technician sees a certificate warning on a new website stating that the certificate source cannot be verified. The technician bypasses the warning. Which of the following must be done to prevent this warning from appearing for other users?

A. A trusted certificate authority must generate the certificate.

B. The certificate must be signed by the administrator.

C. A new certificate must be created from a local computer.

D. The certificate must be added to the personal root.

Answer: (SHOW ANSWER)

When a certificate is generated and signed by a trusted certificate authority, browsers can validate the certificate chain automatically, preventing trust warnings for all users accessing the website.

NEW QUESTION: 67

A systems administrator plans to upgrade a server to the latest operating system. Which of the following should the administrator do before placing a change request?

A. Roll back any previous changes

B. Establish a scope

C. Create a test environment

D. Get change board approval

Answer: (SHOW ANSWER)

NEW QUESTION: 68

Which of the following tools would most likely be used to identify a cable's location in the network closet?

A. Loopback plug

B. Crimper

C. Toner probe

D. Network tap

Answer: (SHOW ANSWER)

A toner probe is used to trace and identify cables by sending a signal through the wire and detecting it at the other end, allowing technicians to locate specific cables in a network closet.

NEW QUESTION: 69

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: (SHOW ANSWER)

When uninstalling and reinstalling network-based software like a VPN client, orphaned or "ghost" adapters can linger in the system, especially if they're no longer visible in Device Manager. Removing these hidden adapters clears the path for the updated client software to recreate its virtual network interface without conflict.

NEW QUESTION: 70

Which of the following applications allows a user to create backups in macOS?

A. Time Machine

B. FileVault

C. Keychain

D. Mission Control

Answer: (SHOW ANSWER)

Time Machine (Option A) is macOS's built-in backup application. It allows users to automatically back up their entire system, including apps, music, photos, emails, and system files. Time Machine provides an easy way to restore files from a previous state or recover from a system failure.

NEW QUESTION: 71

A technician is setting up a new work phone for a user. The company requires that all phones be compliant with business standards and be up to date on all OS patches. Which of the following should the technician use to meet the requirements?

A. MDM

B. Antivirus software

C. BYOD

D. Content filtering

Answer: (SHOW ANSWER)

An MDM (Mobile Device Management) solution enforces compliance requirements such as OS patch levels, security policies, and configuration standards on all company phones.

NEW QUESTION: 72

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: (SHOW ANSWER)

Multi-factor authentication (MFA) combines at least two of the following factors: something you know (password), something you have (a phone-generated or SMS-delivered one-time code), and something you are (biometric). Sending a code to the user's phone provides a "something you have" factor in addition to the password.

NEW QUESTION: 73

An organization notices that its employees often leave their desks without logging off their workstations, leading to unauthorized access by other staff members. Which of the following should the IT department do to address this issue?

A. Implement full disk encryption.

B. Disable remote desktop access.

C. Configure inactivity timeout settings.

D. Set up multifactor authentication.

Answer: (SHOW ANSWER)

Configuring inactivity timeout settings automatically locks a workstation after a defined period of inactivity. This prevents unauthorized users from accessing a session when an employee leaves their desk without logging off, directly addressing the issue of unattended workstations.

NEW QUESTION: 74

A desktop technician is mapping a remote windows share \\WinNAS\sharedas a local disk z:.
Which of the following commands should the technician run?

A. nslookup -opt Z: \\WinNAS\shared

B. net use Z: \\WinNAS\shared

C. chkdsk /R Z: \\WinNAS\shared

D. sfc /offwindir Z: \\WinNAS\shared

Answer: B (LEAVE A REPLY)

The correct command to map a network share as a local drive letter is net use Z: \\WinNAS\shared.

NEW QUESTION: 75

Some users report that they cannot use the VPN to connect to the office via their browsers. A technician finds that the users are all receiving the error message, "Your connection is not secure." Which of the following is most likely causing this issue?

A. The users are not using the VPN client.

B. The operating systems need to be updated.

C. The users' credentials are incorrect.

D. The firewall certificate has expired.

Answer: (SHOW ANSWER)

The correct answer is D. The firewall certificate has expired. The phrase "Your connection is not

secure" is a strong browser certificate warning, not a normal VPN credential or client error. Quentin Docter's Complete Study Guide explains that HTTPS/SSL/TLS communications rely on certificates and that each certificate has an expiration date. When certificates expire, are replaced, or are revoked, browsers may no longer trust the connection. The All-in-One Exam Guide also explains that secure web connections use digital certificates issued by trusted certificate authorities to prove the site or device identity and support encrypted communication. If the organization's firewall, VPN portal, or SSL inspection device presents an expired certificate, browsers will warn users that the connection is not secure. Incorrect credentials would cause an authentication failure, and not using the VPN client would usually prevent connection rather than create a certificate trust warning.

NEW QUESTION: 76
A customer must access the contents of the AppData folder, which is in the local user profile. Which of the following should a technician configure so the customer can easily navigate to this location?
A. Indexing
B. File Explorer Options
C. Privacy
D. Ease of Access
Answer: B (LEAVE A REPLY)
The AppData folder is hidden by default. The technician should configure File Explorer Options to show hidden files so the customer can easily access the folder.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 77
A user's computer is running slowly. Web pages take several seconds to open, and applications are slow to respond. A technician opens the Windows Task Manager and sees the following:
Disk: 2%
Network: 12%
GPU: 15%
CPU: 70%
Memory: 97%
Which of the following would a technician most likely do to resolve the issue?

A. Clear browser cached data
B. Upgrade the network connection
C. Close unnecessary programs
D. Delete temporary files
Answer: (SHOW ANSWER)
High memory usage (97%) suggests the system is overloaded with active processes. The technician should close unneeded applications to free up RAM and improve performance.

NEW QUESTION: 78
Which of the following contains details about its manufacturer and is hardcoded?
A. DSL
B. MAC
C. APIPA
D. IP
Answer: (SHOW ANSWER)
A MAC address is a hardware identifier assigned to a network interface and includes an Organizationally Unique Identifier that identifies the manufacturer, making it hardcoded and unique.

NEW QUESTION: 79
Which of the following Linux commands is used to read another command's documentation?
A. chmod
B. cat
C. man
D. sudo
Answer: (SHOW ANSWER)
The man command displays the manual pages for other Linux commands. It provides detailed documentation, including usage, options, and descriptions, allowing users to read a command's official reference directly from the terminal.
NEW QUESTION: 80
Which of the following controls access to certain services to ensure that administrators are not automatically given elevated permissions?
Freecram.net
A. PAM
B. MFA
C. DLP
D. SSO
Answer: (SHOW ANSWER)
PAM (Privileged Access Management) controls access to certain services so that administrators are not automatically granted elevated permissions.

NEW QUESTION: 81
A company's directory services server is located on premises. Which of the following best describes

the directory services infrastructure?

A. Hybrid cloud

B. Private cloud

C. Public cloud

D. Community cloud

Answer: (SHOW ANSWER)

An on-premises directory services server is hosted and managed within the organization's own infrastructure, which aligns with a private cloud model where resources are dedicated and not shared with external organizations.

NEW QUESTION: 82

Which of the following is an example of malware that runs on the device and uses built-in sensors to monitor targets without their consent?

A. Spyware

B. Rootkit

C. Trojan

D. Stalkerware

Answer: (SHOW ANSWER)

Stalkerware is designed to secretly monitor a user's activity by leveraging device features such as GPS, microphone, camera, and other sensors without the user's consent.

NEW QUESTION: 83

A technician needs to apply a settings file to all user workstations. Which of the following tools should the technician use to import the file?

A. lusrmgr.msc

B. devmgmt.msc

C. regedit.exe

D. msconfig.exe

Answer: (SHOW ANSWER)

regedit.exe allows importing a settings file (such as a .reg file) into the Windows Registry so the configuration applies to all user workstations.

NEW QUESTION: 84

Which of the following technologies uses smartphones to allow contactless entry to secure areas?

A. NFC

B. IR

C. RFID

D. Bluetooth

Answer: (SHOW ANSWER)

Near Field Communication allows smartphones to perform contactless authentication by communicating with access control readers at very short range, enabling secure entry without

physical cards.

NEW QUESTION: 85
A company's IT department discovers that unauthorized software has been installed on several workstations. The IT manager requests a review and an update of the workstation security posture, focusing on preventing future unauthorized software installations. Which of the following should the company do?
A. Remove account administrative rights.
B. Turn on the workstation firewall.
C. Enable Windows Defender SmartScreen.
D. Install EDR on all devices.
Answer: (SHOW ANSWER)
Removing administrative rights from standard user accounts prevents users from installing unauthorized software. Limiting elevated privileges enforces the principle of least privilege and directly reduces the ability to install unapproved applications on workstations.

NEW QUESTION: 86
A technician thinks that an application a user downloaded from the internet may not be the legitimate one, even though the name is the same. The technician needs to confirm whether the application is legitimate. Which of the following should the technician do?
A. Compare the hash value from the vendor.
B. Run Task Manager and compare the process ID.
C. Run the application in safe mode.
D. Verify the file name is correct.
Answer: (SHOW ANSWER)
By computing the downloaded application's checksum (e.g., SHA-256 or MD5) and comparing it against the official hash published by the software vendor, the technician can verify the file's integrity and authenticity. A matching hash confirms the application is genuine and unaltered, whereas any discrepancy indicates a potentially illegitimate or tampered file.

NEW QUESTION: 87
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: (SHOW ANSWER)
While strong passwords and encryption are important, multifactor authentication (MFA) provides the most effective defense against external threat actors targeting cloud-based services. By requiring a second verification step, such as a push notification, one-time code, or hardware token, MFA

ensures that even if credentials are compromised, attackers cannot gain access without the additional factor. This significantly reduces the risk of unauthorized account takeovers in cloud environments.

NEW QUESTION: 88
A user receives an unexpected text message containing a link to reset an expired password. Which of the following social engineering attacks is taking place?
A. Vishing
B. Spear phishing
C. Whaling
D. Smishing
Answer: (SHOW ANSWER)
Smishing is a social engineering attack conducted via SMS or text messages, where attackers send fraudulent links or messages to trick users into revealing credentials or sensitive information.

NEW QUESTION: 89
A user keeps seeing malicious ads in the bottom right corner of their screen. When the ads appear, the icon for the internet browser process is visible in Task Manager. A technician runs an anti-malware scan that shows no results. Which of the following is the cause of this issue?
A. Browser notifications
B. Remote access Trojan
C. Browser cache
D. Browser hijacker
Answer: (SHOW ANSWER)
Browser notifications can display pop-up ads from websites even when no malware is detected. Since the browser process is associated with the ads, the issue is most likely caused by notification permissions granted to a malicious or unwanted website.

NEW QUESTION: 90
A support technician must install software that allows a user to deliver a project status presentation to external stakeholders. Which of the following software types should the technician install?
Freecram.net
A. WinRM
B. RMM
C. Videoconferencing
D. Secure file transfer
Answer: C (LEAVE A REPLY)
Videoconferencing software enables real-time audio and video communication and screen sharing, which is required for delivering a project status presentation to external stakeholders.

NEW QUESTION: 91
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: (SHOW ANSWER)

When a subnet does not offer DHCP, workstations cannot automatically obtain IP configuration. Supplying help desk technicians with the correct static IP address, subnet mask, gateway, and DNS ensures the newly deployed machines can communicate on the secure network segment without relying on DHCP.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 92

Which of the following is an example of an application publisher including undisclosed additional software in an installation package?

A. Virus

B. Ransomware

C. Potentially unwanted program

D. Trojan

Answer: (SHOW ANSWER)

A potentially unwanted program (PUP) refers to software bundled with an installer that the user did not explicitly request and that's often advertised or installed without clear disclosure. While not always malicious, PUPs can degrade performance or introduce unwanted behavior, matching the description of undisclosed additional software in a package.

NEW QUESTION: 93

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: (SHOW ANSWER)

netstat reveals active network connections and listening ports on the local machine. By using it, you can confirm that the application has successfully opened (or attempted) a connection to the database server's port, verify the remote server's address and port, and detect any failed or hanging TCP sessions that would prevent data retrieval.

NEW QUESTION: 94
A malicious actor uses multiple endpoints to target a single endpoint. Which of the following describes this threat?
A. On-path attack
B. Structured Query Language injection
C. Brute-force attack
D. Distributed Denial of Service
Answer: (SHOW ANSWER)
A Distributed Denial of Service attack uses multiple endpoints simultaneously to overwhelm a single target system, exhausting its resources and making it unavailable to legitimate users.

NEW QUESTION: 95
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: (SHOW ANSWER)
When users have local administrative rights, they can install unauthorized applications - leading to licensing prompts, unsupported software, and potential security risks. By removing users from the local Administrators group, installations require elevated credentials, ensuring that only approved software is installed and reducing these recurring issues.

NEW QUESTION: 96
A small company is experiencing unauthorized access attempts to its Windows workstations. The company suspects that some default security settings may be too permissive. Which of the following actions should an IT technician take?
A. Implement an appropriate group policy.
B. Configure automatic updates for Windows.
C. Reset account passwords.
D. Enable account lockout policies.
Answer: (SHOW ANSWER)
Group Policy allows centralized enforcement of security settings across Windows workstations,

making it the appropriate method for tightening default permissions and reducing unauthorized access attempts.

NEW QUESTION: 97
Which of the following is typically associated with a Linux filesystem?
A. FAT32
B. XFS
C. NTFS
D. APFS
Answer: (SHOW ANSWER)
XFS is a high-performance filesystem commonly used in Linux environments.

NEW QUESTION: 98
A company is implementing the 3-2-1 backup rule. Which of the following should the company do?
A. Perform both full and differential backups.
B. Test the backup integrity every three weeks.
C. Keep all backup media on site for fast recovery.
D. Use at least two different types of media.
Answer: (SHOW ANSWER)
The 3-2-1 backup rule recommends keeping at least two different types of media to ensure data redundancy and protection.

NEW QUESTION: 99
A support specialist must apply a new application update to an entire organization. Which of the following is the first step in this process?
A. Backup plan
B. Request forms
C. Sandbox testing
D. Peer review
Answer: (SHOW ANSWER)
Sandbox testing is performed first to validate the application update in a controlled environment, ensuring it functions correctly and does not introduce issues before deployment across the organization.

NEW QUESTION: 100
Which of the following prevents forced entry into a building?
A. PIV card
B. Motion-activated lighting
C. Video surveillance
D. Bollard
Answer: (SHOW ANSWER)

Bollards are sturdy, fixed posts installed around buildings or sensitive areas to physically block vehicles and prevent ramming attacks or forced vehicular entry. Unlike surveillance or lighting, bollards provide a direct physical barrier.

NEW QUESTION: 101
A developer who is using a personal laptop that is running Windows wants to leverage virtual technologies. The developer does not see an option to enable the Hyper-V feature. Which of the following is the most likely reason?
A. The system is not fully patched.
B. The OS edition is Home.
C. The motherboard does not have a TPM.
D. The user has not joined a domain.
Answer: (SHOW ANSWER)
Hyper-V cannot be enabled on Windows Home editions; it requires Windows Pro, Enterprise, or Education.

NEW QUESTION: 102
Which of the following types of social engineering attacks sends an unsolicited text message to a user's mobile device?
A. Impersonation
B. Vishing
C. Spear phishing
D. Smishing
Answer: (SHOW ANSWER)
Smishing is the act of sending fraudulent messages via SMS or other texting platforms to trick users into revealing sensitive information or clicking malicious links. This distinguishes it from phishing over email (spear phishing), voice calls (vishing), or in-person deception (impersonation).

NEW QUESTION: 103
A customer is unable to open some files on their system. Each time the customer attempts to open a file, the customer receives a message that the file is encrypted. Which of the following best describes this issue?
A. Keylogger
B. Ransomware
C. Phishing
D. Cryptominer
Answer: (SHOW ANSWER)
Ransomware is malware that encrypts a user's files and then demands payment (a ransom) in exchange for the decryption key. The user's inability to open the files and the message indicating they're encrypted are classic signs of a ransomware attack.

NEW QUESTION: 104
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: (SHOW ANSWER)
Facial recognition leverages biometric characteristics unique to each user, offering stronger security than shared passcodes or easily observed pattern locks. It ensures that only the enrolled individual can unlock the device, reducing the risk of unauthorized access from shared codes.

NEW QUESTION: 105
A customer is upgrading their workstation from Windows 10 to Windows 11. They perform a clean installation from a USB drive. After the system restarts, the installer loads again. Which of the following should the user do to complete the installation?
A. Run chkdskfrom the USB.
B. Turn off TPM.
C. Change MBR to UEFI.
D. Remove the USB drive.
Answer: (SHOW ANSWER)
Removing the USB drive allows the system to boot from the newly installed Windows 11 operating system, rather than restarting the installation process.

NEW QUESTION: 106
The Chief Information Officer (CIO) is overseeing a project to integrate existing business processes to an enterprise resource planning system. The CIO identifies the scope of the change and provides it to the IT department. Which of the following is the first change management procedure to perform before measuring the impact to the systems?
A. Backup plan
B. Risk analysis
C. Document findings
D. Sandbox testing
Answer: (SHOW ANSWER)
Risk analysis is the first step in the change management process before measuring system impact. It identifies potential threats, vulnerabilities, and the likelihood of adverse effects resulting from the change. Performing risk analysis ensures informed decision-making prior to further evaluation, testing, or implementation.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 107

A technician is setting up a Windows server to allow remote desktop connections for multiple users. Which of the following should the technician configure on the workstation?

A. Firewall

B. Computer Management

C. User Accounts

D. Ease of Access

Answer: (SHOW ANSWER)

To allow Remote Desktop connections, the Windows Firewall on the server (or workstation acting as the host) must have the Remote Desktop (TCP port 3389) rule enabled. This opens the necessary port so multiple users can establish RDP sessions. The other settings (User Accounts, Computer Management, Ease of Access) don't directly control network access for RDP.

NEW QUESTION: 108

A user calls the help desk to report potential malware on a computer. The anomalous activity began after the user clicked a link to a free gift card in a recent email. The technician asks the user to describe any unusual activity, such as slow performance, excessive pop-ups, and browser redirections.

Which of the following should the technician do next?

A. Advise the user to run a complete system scan using the OS anti-malware application.

B. Guide the user to reboot the machine into safe mode and verify whether the anomalous activities are still present.

C. Have the user check for recently installed applications and outline those installed since the link in the email was clicked.

D. Instruct the user to disconnect the Ethernet connection to the corporate network.

Answer: (SHOW ANSWER)

Disconnecting from the corporate network helps prevent the potential spread of malware and protects other systems while the issue is investigated.

NEW QUESTION: 109

A new software installation requires administrative privileges for deployment. Which of the following is the best way to provide the necessary permissions to install the software?

A. Granting just-in-time access

B. Assigning the power user role

C. Performing the installation manually

D. Adding the user to the local administrator group

Answer: (SHOW ANSWER)

Granting just-in-time access provides temporary administrative privileges only for the duration required to perform the installation. This approach follows the principle of least privilege by minimizing the time elevated permissions are active, reducing security risk while still allowing the software to be deployed.

NEW QUESTION: 110

A software developer has tested an enhancement that would improve performance of the company's critical, cloud-deployed applications. The developer has shared the results with peers and received positive feedback. Which of the following change management procedures should the developer perform next?

Freecram.net

A. Seek end-user acceptance.

B. Submit relevant requests for approval.

C. Determine organizational impact.

D. Document the scope of the change.

Answer: B (LEAVE A REPLY)

After peer review, the next step in change management is to formally submit the change request for approval so it can be evaluated, scheduled, and implemented through the proper governance process.

NEW QUESTION: 111

A user reports that double-clicking on an application's shortcut fails to launch a program. A technician thinks that the application process is running in the background in an unresponsive state. Which of the following tools should the technician use to resolve the issue?

A. Resource Monitor

B. Task Manager

C. Event Viewer

D. Registry Editor

Answer: B (LEAVE A REPLY)

Task Manager allows the technician to view running processes and terminate an unresponsive application process, enabling the program to be launched again properly.

NEW QUESTION: 112

Which of the following is most important for protecting intellectual property from being shared on social media platforms?

A. SLA

B. AUP

C. ACL

D. NDA

Answer: D (LEAVE A REPLY)

A nondisclosure agreement legally binds individuals to protect confidential and proprietary

information, making it the most important control for preventing intellectual property from being shared on social media platforms.

NEW QUESTION: 113
A company network is spread across multiple office branches that are located within the same postal code and connected using leased lines. Which of the following best describes this network type?
A. Campus area network
B. Metropolitan area network
C. Local area network
D. Wide area network
Answer: (SHOW ANSWER)
A campus area network connects multiple buildings or office locations within a limited geographic area, such as the same postal code, using high-speed links like leased lines, providing centralized network management and connectivity.

NEW QUESTION: 114
Which of the following describes an attack in which an attacker sets up a rogue AP that tricks users into connecting to the rogue AP instead of the legitimate network?
A. Stalkerware
B. Evil twin
C. Tailgating
D. Shoulder surfing
Answer: (SHOW ANSWER)
An evil twin attack involves an adversary configuring a rogue wireless access point with the same SSID and similar settings as a legitimate network. Unsuspecting users connect to this rogue AP, allowing the attacker to intercept traffic, capture credentials, and launch further attacks.

NEW QUESTION: 115
A user's PC is performing slowly after the user clicked on a suspicious email attachment. The technician notices that a single process is taking 100% of RAM, CPU, and network resources. Which of the following should the technician do first?
A. Disconnect the computer from the network
B. Run an antivirus scan
C. Reboot the computer
D. Educate the user about cybersecurity best practices
Answer: (SHOW ANSWER)
The technician should disconnect the computer from the network (Option A) first to prevent any further spread of the infection or data loss. Once the machine is isolated from the network, the technician can safely investigate the malware without risking infection to other systems.

NEW QUESTION: 116
An administrator must rename the administrator account on a Windows desktop. Which of the following tools is best for this task?
A. lusrmgr.msc
B. devmgmt.msc
C. gpedit.msc
D. eventvwr.msc
Answer: (SHOW ANSWER)
The Local Users and Groups Manager (lusrmgr.msc) is the utility for managing user accounts, including renaming the default Administrator.

NEW QUESTION: 117
A user logs in to a computer each morning and tries to print a daily report, but it will not print. The user calls the help desk, they change a setting, and the user is able to print that day but the same issue happens again the next day. Because the issue occurs every day, the issue gets escalated. Which of the following does the technician need to do so the user does not have to report the issue every day? (Choose two.)
A. Set the print spooler to have no dependencies
B. Set the print spooler recovery to take no action
C. Start the printer extensions and notifications service
D. Start the print spooler service
E. Set the print spooler to Automatic
F. Set the print spooler log-on to the user's account
Answer: (SHOW ANSWER)
Starting the print spooler service ensures printing functionality is restored immediately.
Setting the print spooler to Automatic ensures the service starts each time the computer boots, preventing the issue from recurring daily.

NEW QUESTION: 118
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: (SHOW ANSWER)
Large gatherings like music festivals often overwhelm local cellular towers due to the sheer number of devices competing for bandwidth and signal. This congestion can cause mobile applications, such

as email clients, to stall or fail when attempting to download messages.

NEW QUESTION: 119

A new employee at a 3D-printing company is in training. The employee's first training task is to learn about health hazards at the company. Which of the following documents should the new employee read?

A. NDA

B. SDS

C. EULA

D. AUP

Answer: (SHOW ANSWER)

A Safety Data Sheet provides information about chemical hazards, handling, storage, and safety precautions, which is essential for understanding workplace health risks.

NEW QUESTION: 120

A technician completes the installation of an OS that appears to be successful. However, when the technician removes the USB drive that was used for the installation and restarts the system, the following error appears:

No OS found.

Which of the following should the technician do next to resolve the issue?

Freecram.net

A. Reinstall the OS from a new ISO

B. Enable UEFI devices in the BIOS

C. Restart in recovery mode and troubleshoot

D. Install storage drivers for the motherboard

E. Reseat the SATA cable

Answer: (SHOW ANSWER)

Enabling UEFI devices in the BIOS ensures that the system can detect and boot from the OS installed on a UEFI-configured drive, resolving the "No OS found" error after installation.

NEW QUESTION: 121

Which of the following should a technician consider when adding ten new high-end graphic design and animation desktops at a client site?

A. The local area's temperature

B. The proper ventilation for hazardous fumes

C. The interior office space's humidity levels

D. The electrical circuit's power consumption

Answer: (SHOW ANSWER)

High-end graphic design desktops draw significant power, so the technician must ensure the electrical circuit can support the increased power consumption to prevent overloads and outages.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 122
A developer asks a public chatbot to generate a function to convert a .pdf file into a Word document. The chatbot responds that the function exists in the pdf2word library. However, the developer cannot find any evidence that this library exists. Which of the following describes what most likely happened with the chatbot?
A. Plagiarized public repository content
B. Leaked proprietary information
C. Misunderstood the developer's request
D. Hallucinated the solution
Answer: (SHOW ANSWER)
A hallucination occurs when a chatbot generates information that sounds plausible but is not factually supported. In this case, the chatbot invented or incorrectly referenced a library that the developer could not verify.

NEW QUESTION: 123
A SOHO customer purchases a Windows 11 computer. When the technician attempts to join the computer to the domain, the option is grayed out. Which of the following explains the reason the option is unavailable?
A. The computer OS needs to be updated to the latest version.
B. Network settings need to be changed on the Pro edition of Windows.
C. The computer needs to be restarted to apply new group policies.
D. The computer operating system is Home edition.
Answer: (SHOW ANSWER)
Windows Home edition does not support joining an Active Directory domain. Only Professional, Enterprise, and Education editions include domain join capabilities, which is why the option is unavailable.

NEW QUESTION: 124
A user reports some single sign-on errors to a help desk technician. Currently, the user is able to sign in to the company's application portal but cannot access a specific SaaS-based tool. Which of the following would the technician most likely suggest as a next step?
A. Reenroll the user's mobile device to be used as an MFA token.
B. Use a private browsing window to avoid local session conflicts.
C. Bypass single sign-on by directly authenticating to the application.
D. Reset the device being used to factory defaults.

Answer: (SHOW ANSWER)

Single sign-on issues that affect only a specific application often stem from stale or conflicting session data in the user's browser. Launching a private (incognito) window ensures a fresh session without cached cookies or tokens, which can resolve access to the SaaS tool without affecting other configurations.

NEW QUESTION: 125

A technician is selecting a remote access method so users can securely access Linux and Windows servers when working from home. Which of the following should the technician choose to best meet this requirement?

A. File Transfer Protocol

B. Virtual private network

C. Remote Desktop Protocol

D. Remote monitoring and management

Answer: (SHOW ANSWER)

A virtual private network provides secure, encrypted remote access to internal resources across both Linux and Windows systems, making it the best choice for remote users connecting from home.

NEW QUESTION: 126

A user wants to use a popular search engine. When the user enters the URL in the address bar. the web page displays the following message instead of the expected search engine:

The antivirus has expired.

Which of the following would most likely cause this issue?

A. Random pop-ups

B. Browser redirection

C. Certificate warnings

D. Internet failure

Answer: (SHOW ANSWER)

Browser redirection occurs when malware or unwanted software forces the browser to load an unexpected page instead of the intended site, such as showing an "antivirus expired" page instead of a search engine.

NEW QUESTION: 127

A developer needs to isolate a testing VM in a Type 1 hypervisor from the other guests. Which of the following does the administrator need to use to accomplish this task?

A. VDI

B. Container

C. Private cloud

D. Sandbox

Answer: (SHOW ANSWER)

A sandbox provides an isolated environment within the hypervisor where a virtual machine can run

independently without affecting other guests, ensuring safe testing and containment.

NEW QUESTION: 128
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 (LEAVE A REPLY)
Batch files (.bat) are classic Windows script files that execute a series of command-line instructions. They can be linked to user logon events via Group Policy or the Startup folder to automate tasks (like mapping drives or launching applications) when a user signs in.

NEW QUESTION: 129
A help desk technician needs to remove RAM from retired workstations and upgrade other workstations that have applications that use more memory with this RAM. Which of the following actions would the technician most likely take?
A. Demagnetize memory for security.
B. Use antistatic bags for storage and transport.
C. Plug in the power supply to ground each workstation.
D. Install memory in identical pairs.
Answer: (SHOW ANSWER)
When handling and moving RAM modules, it's vital to protect them from electrostatic discharge (ESD). Storing the removed RAM in antistatic bags prevents damage during transport or while they're in storage before being installed in other workstations.

NEW QUESTION: 130
A user submits a support ticket after receiving the following error:



The technician confirms that the website loads properly on a test workstation. Which of the following is a possible cause for this error?
A. Misconfigured security settings

B. Unencrypted network
C. Missing SSL certificate
D. Incorrect NTP settings
Answer: (SHOW ANSWER)
The error NET::ERR_CERT_DATE_INVALID commonly occurs when the client device's date or time is incorrect. Incorrect NTP settings cause the browser to see the certificate as expired or not yet valid, even though the site works normally on other systems.

NEW QUESTION: 131
Performance on a user's smartphone is degrading. Applications take a long time to start, and switching between windows also takes a long time. Which of the following diagnostic steps should a mobile technician take first?
A. Restore the phone to factory settings
B. Restart the phone
C. Check the phone's battery state
D. Uninstall unneeded applications
Answer: (SHOW ANSWER)
Restarting the phone is a simple first diagnostic step that can resolve performance issues by clearing temporary memory and processes.
NEW QUESTION: 132
A technician is designing a solution to automatically save users' local documents, pictures, and files to the network. The network is in an Active Directory environment. Which of the following will the technician most likely do?
A. Enable System Restore.
B. Create recovery points.
C. Configure folder redirection.
D. Manage Windows server backups.
Answer: (SHOW ANSWER)
Configuring folder redirection in an Active Directory environment allows user folders such as Documents, Pictures, and Desktop to be automatically redirected and stored on a network server. This ensures files are centrally saved, backed up, and accessible regardless of which domain-joined computer the user logs into.

NEW QUESTION: 133
The screen of a previously working computer repeatedly displays an OS Not Founderror 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: (SHOW ANSWER)
An "OS Not Found" error most commonly indicates the system isn't booting from the correct device. Verifying and correcting the boot order (ensuring the internal hard drive is prioritized over USB or other entries) is the quickest first step before making any changes to the disk or firmware settings.

NEW QUESTION: 134
A technician needs to delete an application's local data from a specific user account, but when the technician navigates to the C:\Users\EmployeeA directory, the AppData folder is not present.
Which of the following should the technician do to see the appropriate folder?
A. Grant full control permissions on the folder to everyone
B. Adjust the display options to show all file details
C. Change the settings to view hidden items
D. Log in to the workstation as a domain administrator
Answer: (SHOW ANSWER)
The AppData folder is hidden by default in Windows, so changing the settings to view hidden items allows the technician to see and access the folder to delete the application's local data.

NEW QUESTION: 135
When a corporate laptop is connected to the company network, the laptop is able to reach external websites. However, when the laptop tries to reach any internal websites the following error message appears:
Hmm... Cannot reach this page.
Which of the following should a technician configure?
A. Subnet mask
B. DNS settings
C. Default gateway
D. DHCP
Answer: (SHOW ANSWER)
Incorrect DNS settings prevent the laptop from resolving internal hostnames. External sites work because they use public DNS, but internal addresses fail without the correct internal DNS server. Configuring the proper DNS settings resolves the issue.

NEW QUESTION: 136
A technician is preparing to replace the batteries in rack-mounted UPS system. After ensuring the power is turned off and the batteries are fully discharged, the technician needs to remove the battery modules from the bottom of the rack. Which of the following steps should the technician take?
A. Ensure the fire suppression system is ready to be activated.
B. Use appropriate lifting techniques and guidelines.
C. Place the removed batteries in an antistatic bag.
D. Wear a face mask to filter out any harmful fumes.
Answer: (SHOW ANSWER)

UPS battery modules are heavy and awkward; employing proper lifting techniques (e.g., lifting with the legs, keeping the back straight, and using team lifts or mechanical aids as necessary) prevents musculoskeletal injuries and ensures safe removal.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 137
A user reports a critical application issue. The user tells the technician that a former IT employee previously resolved this same issue. Which of the following steps should the technician take first?
A. Consult the technician who previously solved the issue.
B. Escalate the issue to the software manufacturer to develop a patch.
C. Review the ticketing system for details related to the prior occurrence.
D. Open a case to document the issue and progress until the issue is resolved.
Answer: (SHOW ANSWER)
Reviewing the ticketing system for details related to the prior occurrence is the first step because it allows the technician to gather relevant historical information and previously documented resolutions. This supports efficient troubleshooting by leveraging existing knowledge before taking further action.

NEW QUESTION: 138
Which of the following is a key AI characteristic that is applied in operational procedures?
A. AI systems can support any kind of operations relying on historical data.
B. AI leverages preset rules and algorithms to imitate human decision-making.
C. AI eliminates the need for human oversight in all operational processes.
D. AI is primarily used to upgrade software components in IT systems.
Answer: (SHOW ANSWER)
AI applies preset rules and algorithms to analyze data and mimic human decision-making, which is a key characteristic used in operational procedures.

NEW QUESTION: 139
Which of the following depends on system time accuracy to function properly?
A. Terminal Access Controller Access-control System
B. Kerberos token
C. Remote Authentication Dial-in User Service

D. Wi-Fi Protected Access

Answer: (SHOW ANSWER)

Kerberos relies on accurate system time to validate authentication tickets, as it uses time- stamped tokens with strict expiration windows to prevent replay attacks. If system clocks are not synchronized, authentication fails.

NEW QUESTION: 140

Which of the following threats is shoulder surfing an example of?

A. Zero-day

B. Evil twin

C. Social engineering

D. Brute-force

Answer: (SHOW ANSWER)

Shoulder surfing is a social engineering threat because the attacker captures sensitive information by observing the user's actions, relying on human behavior rather than exploiting a technical vulnerability.

NEW QUESTION: 141

An employee's personal smartphone was stolen. The employee's corporate email account is set up on the smartphone. Which of the following is the first action to take to prevent unauthorized users from accessing this email account?

A. Enforcing existing BYOD policies

B. Changing the password on the email account

C. Remotely wiping any non-personal data

D. Enabling GPS and geofencing

Answer: (SHOW ANSWER)

Changing the email account password immediately invalidates the existing authentication token on the stolen device and prevents unauthorized access to the corporate email account. This is the fastest and most direct action to secure the account while additional steps, such as remote wipe, can be performed afterward.

NEW QUESTION: 142

A user installed a free application from an unofficial application store. Now, their smartphone displays random pop-ups and shows increased data usage. Additionally, the user cannot perform certain actions such as opening banking applications or updating their OS. Which of the following should the user do first to address the security issues on their smartphone?

A. Perform a factory reset.

B. Clear the device cache.

C. Contact the manufacturer's support line.

D. Change all passwords on the device.

Answer: (SHOW ANSWER)

A factory reset is the first step because the device is showing clear signs of malware infection from an unverified app. Resetting the smartphone removes malicious software and restores the device to a secure, clean state.

NEW QUESTION: 143
After installing a new video card in their workstation, a user reports that the workstation randomly crashes. The user updates the drivers according to the manufacturer's recommendation, but the issue persists. Which of the following steps should a technician take next to troubleshoot the issue?
A. Add additional fans for cooling.
B. Check the anti-malware software for recent activity.
C. Install third-party graphics drivers for better stability.
D. Review system logs for error messages.
Answer: D (LEAVE A REPLY)
When a system begins randomly crashing after a hardware change (installing a GPU) and the correct vendor driver update does not resolve it, the best next troubleshooting step is to collect evidence about what is failing. Windows records crash details, driver faults, and unexpected shutdowns in Event Viewer (System/Application logs) and related reliability tools. Quentin Docter specifically states that Event Viewer should be the first place you look when the solution is not evident because applications and the OS often create log entries that help verify operation and diagnose problems. These logs can reveal whether the crash is tied to a display driver fault, power/kernel events, or another subsystem. Docter also notes you can often find more information about application crashes by reviewing the Application log, and for instability/shutdown patterns you "start combing through the logs" in Event Viewer to determine whether the system lost power or crashed. Mike Meyers adds that Event Viewer is the tool used to read and understand Windows logs (Application/System/Setup/Security) for diagnosing what's happening on a system.

NEW QUESTION: 144
A company computer is being repurposed within an organization. The existing configuration has a static IP address, but it is no longer required. Which of the following should a technician do to satisfy the network requirements?
A. Make a DHCP reservation for the computer
B. Create an exclusion in the existing IP scheme
C. Switch the NIC settings from manual to automatic
D. Change the currently assigned static IP
Answer: C (LEAVE A REPLY)
Switching the NIC settings from manual to automatic allows the computer to obtain its IP configuration dynamically from DHCP, which is appropriate when a static IP address is no longer required.

NEW QUESTION: 145
The battery on a user's smartphone discharges quickly when the user travels. The smartphone was

replaced two weeks ago. Which of the following should a technician do first?

A. Replace the battery with a higher capacity option

B. Provide an external battery to extend the usage time

C. Ensure that the charging port is working as expected

D. Look for applications that are reporting the highest utilization

Answer: (SHOW ANSWER)

The technician should first look for applications reporting the highest utilization, as some apps or services may be consuming excessive battery, especially when the user is traveling.

NEW QUESTION: 146

A project team needs special access on a shared repository to add new content, edit existing content, and prevent content deletion. Which of the following should an administrator do to configure this setup with the least amount of effort?

A. Map the network folder on each user's workstation for controlled access.

B. Create and assign a security group with adequate permissions

C. Grant administrative permissions to the team.

D. Apply the required permissions to each individual user.

Answer: (SHOW ANSWER)

Creating and assigning a security group allows the administrator to manage permissions centrally, granting the required access to all team members efficiently with minimal effort.

NEW QUESTION: 147

Which of the following tasks would most likely be automated by utilizing a script?

A. Overclocking processors

B. Troubleshooting BSODs

C. Creating user accounts

D. Monitoring room humidity

Answer: (SHOW ANSWER)

Creating user accounts is a repetitive administrative task that can be efficiently automated with scripts to streamline provisioning and reduce manual effort.

NEW QUESTION: 148

An administrator applies security controls to a workstation that will provide protection from a brute-force attack against the user account. Which of the following actions should the administrator take?

A. Restrict login times to the users' working hours.

B. Force login when waking up the workstation.

C. Lock the account after three failed attempts.

D. Implement least privilege principles on the computer.

Answer: (SHOW ANSWER)

The correct answer is C. Lock the account after three failed attempts. A brute-force attack attempts many password guesses. Account lockout directly slows or stops this by preventing unlimited login

attempts. Quentin Docter's Complete Study Guide explains that administrators should configure user account settings to limit the number of failed login attempts before the account is locked for a period of time. It specifically notes that setting a failed login attempt counter and lockout duration slows the progress of password attacks. The same material notes that three failed attempts provides better security, although it may create more help desk calls.
Restricting login times may reduce the attack window but does not stop repeated guessing during allowed hours. Requiring login after wake protects unattended sessions. Least privilege limits damage after compromise, but account lockout best mitigates brute-force password attempts.

NEW QUESTION: 149
A help desk technician is setting up speech recognition on a Windows system. Which of the following settings should the technician use?
A. Time and Language
B. Personalization
C. System
D. Ease of Access
Answer: (SHOW ANSWER)
Windows places speech recognition and other accessibility features under the Ease of Access settings. From there, you can configure Speech options - including enabling Windows Speech Recognition and adjusting its settings - so that users relying on voice input can operate the system effectively.

NEW QUESTION: 150
Which of the following concepts should a technician consider when discussing confidential work projects with individuals outside the company?
Freecram.net
A. EULA
B. EOL
C. SLA
D. NDA
Answer: D (LEAVE A REPLY)
An NDA (Non-Disclosure Agreement) is the concept a technician should consider to ensure that confidential work project details are not shared with unauthorized individuals outside the company.

NEW QUESTION: 151
A customer wants to format an external hard drive to work on both Windows and macOS. Which of the following filesystems is the best to use?
A. NTFS
B. exFAT
C. APFS
D. XFS
Answer: (SHOW ANSWER)

exFAT is natively supported for both read and write access on Windows and macOS. It is specifically designed for removable storage and supports large files and large volumes, making it the best choice for cross-platform compatibility.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 152
A customer laptop has been shutting down unexpectedly. The customer explains that a blue screen appears just before the laptop turns off. but the screen disappears too quickly to see anything. Which of the following tools should a technician use to find details about the error?
A. Performance Monitor
B. Device Manager
C. Event Viewer
D. System Information
Answer: C (LEAVE A REPLY)
Event Viewer logs system events, including critical errors like blue screen crashes, allowing the technician to review details about the failure after the system restarts.

NEW QUESTION: 153
A technician installed, configured, and hardened a SOHO firewall to meet a customer's needs. The customer asks the technician what can be done to keep the firewall secure in the future. Which of the following should the technician recommend?
A. Changing all of the default passwords
B. Scheduling regular firmware updates
C. Verifying all unneeded ports are disabled
D. Keeping the firewall in a secure location
Answer: (SHOW ANSWER)
Regular firmware updates ensure the firewall receives security patches, vulnerability fixes, and performance improvements, helping maintain protection against newly discovered threats over time.

NEW QUESTION: 154
A company wants to perform an in-place upgrade of operating systems on all workstations. All types of removable storage are disabled for security reasons. Which of the following is the best way to upgrade while keeping security settings in place?

A. Using an external hard drive to upgrade the OS
B. Copying the ISO file to each workstation and executing
C. Setting up image deployment for PXE
D. Using a hardware token to access upgrade files
Answer: (SHOW ANSWER)
PXE image deployment allows operating system upgrades to be performed over the network without enabling removable storage, maintaining the company's security restrictions while upgrading all workstations efficiently.

NEW QUESTION: 155
A technician is troubleshooting a print spooler that fails to start on a Windows 11 desktop computer. The technician determines the root cause is that required dependencies are failing to run. Which of the following tools is the technician using?
A. Process
B. Services
C. Startup
D. Performance
Answer: (SHOW ANSWER)
The Services tool in Windows allows a technician to view service dependencies and status. If the print spooler can't start due to a dependency, Services is the correct tool to inspect and manage them.

NEW QUESTION: 156
A technician is performing an in-place upgrade on a user's laptop. Which of the following is the most effective method of upgrading the workstation to the latest OS?
A. Utilize the latest version of the .iso file.
B. Back up data and perform a fresh installation.
C. Enter the BIOS and enable USB access.
D. Use the System Update utility.
Answer: (SHOW ANSWER)
The System Update utility is designed for in-place upgrades, allowing the technician to upgrade the OS while preserving user data and applications.

NEW QUESTION: 157
A user is working from home and is unable to access work files on a company laptop. Which of the following should a technician configure to fix the network access issue?
A. Wide-area network
B. Wireless network
C. Proxy network settings
D. Virtual private network
Answer: (SHOW ANSWER)

A VPN creates a secure tunnel from the user's home network into the corporate network, providing the necessary routing and access controls for the laptop to reach internal file servers.
Without a VPN, the device remains outside the corporate LAN and cannot directly reach protected resources.

NEW QUESTION: 158
A technician needs to increase the security levels on a laptop that will be used during a conference that is out of the country. Which of the following should the technician configure?
A. Content filtering
B. A screen lock
C. Restricted login times
D. Disk encryption
Answer: D (LEAVE A REPLY)
Disk encryption protects the laptop's stored data if the device is lost, stolen, or accessed without authorization while traveling. It ensures the data remains unreadable without the proper authentication key.
NEW QUESTION: 159
An end user is unable to access the intranet. A technician needs to confirm whether the Windows web server is online and functioning. Which of the following default remote access technologies would the technician most likely use to remotely connect to the server?
A. SPICE
B. VNC
C. RDP
D. SSH
Answer: (SHOW ANSWER)
Remote Desktop Protocol is the default remote access technology for Windows servers. It allows a technician to remotely log in to the Windows web server, verify its status, and confirm that the web service is running properly.

NEW QUESTION: 160
Which of the following must be followed during incident response to ensure the collected evidence is properly handled and accounted for?
Freecram.net
A. Order of volatility for data
B. Law enforcement notification procedures
C. Data integrity best practices
D. Chain of custody process
Answer: D (LEAVE A REPLY)
The chain of custody process ensures that evidence is properly documented, handled, and tracked throughout the incident response lifecycle, preserving its integrity and admissibility.

NEW QUESTION: 161

A computer frequently crashes after an OS patch. Which of the following actions should a technician take to prevent further crashes and look into the issue?

A. Perform a System Restore.

B. Roll back the updates.

C. Apply the optional patches.

D. Change the startup sequence.

Answer: (SHOW ANSWER)

Rolling back the updates will revert the system to its previous stable state, preventing further crashes and allowing investigation into the issue caused by the recent OS patch.

NEW QUESTION: 162

A customer is explaining issues with a workstation to a technician. While the customer is listing the issues, the technician is browsing social media on a smartphone. Which of the following professionalism and communication techniques should the technician be using in this situation? (Choose two.)

A. Follow up with the customer.

B. Avoid personal interruptions.

C. Provide proper documentation.

D. Clarify customer statements.

E. Actively listen and take notes.

F. Maintain professional attire.

Answer: (SHOW ANSWER)

Avoiding personal interruptions ensures the technician gives full attention to the customer. Actively listening and taking notes demonstrates respect and helps accurately address the customer's issues.

NEW QUESTION: 163

Which of the following authentication methods is the best way to prevent users from frequently entering their credentials?

A. Access control list

B. Single sign-on

C. Multifactor authentication

D. One-time password

Answer: (SHOW ANSWER)

Single sign-on (SSO)allows users to authenticate once and gain access to multiple systems without re- entering credentials, which significantly enhances user convenience while maintaining security.

NEW QUESTION: 164

A technician is replacing a rack-mounted UPS. Which of the following should the technician consider?

A. Determining the availability of compressed air

B. Getting assistance to lift the hardware
C. Checking local low-voltage regulations
D. Testing the fire suppression system
Answer: B (LEAVE A REPLY)
The correct answer is B. Getting assistance to lift the hardware. A rack-mounted UPS can be very heavy because it contains one or more internal batteries. When replacing or installing heavy rack-mounted equipment, the technician must consider personal safety and proper lifting techniques before performing the work. The Sybex practice-test explanations state that a UPS, also called a battery backup, can range in size from a small unit to equipment as large as an entire server rack, and it contains batteries and fuses used to provide power protection during power problems. The same source also explains that technicians should bend at the knees, lift with the legs, observe weight limitations, and use a partner lift or cart when needed. Compressed air is related to cleaning, not replacing a UPS. Low-voltage regulations and fire suppression systems may be relevant to facility planning, but the immediate safety concern when replacing rack-mounted hardware is safe lifting and handling.
NEW QUESTION: 165
A user must perform a series of commands each day on a Linux server. The user wants to use a script to automate the process. Which of the following is the most likely file type for the script?
A. .js
B. .vbs
C. .bat
D. .sh
Answer: (SHOW ANSWER)
Linux shell scripts use the .sh extension, making it the appropriate choice for automating commands on a Linux server.

NEW QUESTION: 166
Which of the following is the weakest wireless security protocol?
A. WEP
B. WPA2
C. TKIP
D. AES
Answer: (SHOW ANSWER)
WEP (Wired Equivalent Privacy) is known to be the weakest wireless security protocol due to its vulnerabilities and ease of being compromised.
WEP: The oldest and weakest protocol, susceptible to various attacks and easily cracked.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 167
A user is renaming a .txt file to a .xml file. After renaming the file. Windows Explorer shows the filename as Document.xml. However, the document properties shows the type of file as: Text Document(.txt). Which of the following controls enables the user to correctly change the file type?
A. Indexing options
B. Format command
C. Personalization
D. Hide extensions
Answer: D (LEAVE A REPLY)
The "Hide extensions" control determines whether file extensions are visible in Windows Explorer. Disabling it allows users to change the file extension and, thus, the file type correctly.

NEW QUESTION: 168
An end user reports that their computer will not load Windows. Which of the following should a technician check after inspecting the computer hardware and verifying that it is working properly?
A. Boot order
B. Filesystem
C. Encryption
D. Drivers
Answer: (SHOW ANSWER)
If the hardware is functioning properly but Windows does not load, the technician should verify that the system is configured to boot from the correct drive. An incorrect boot order can prevent the system from locating the installed operating system.

NEW QUESTION: 169
A user frequently misplaces their Windows laptop and is concerned about it being stolen. The user would like additional security controls on their laptop. Which of the following is a built-in technology that a technician can use to enable full drive encryption?
A. Active Directory
B. New Technology File System
C. Encrypting File System
D. BitLocker
Answer: (SHOW ANSWER)
BitLocker is a built-in Windows feature that provides full-volume encryption of the system drive,

protecting all data if the laptop is lost or stolen. It integrates with the TPM (when available) for secure key storage and can be configured via Group Policy or the Control Panel without additional software.

NEW QUESTION: 170

A developer is using an AI tool to generate a complex sorting algorithm for a web application. Which of the following is the best choice to legally generate code in their application?

Freecram.net

A. Use the generated code in their application silently

B. Insert comments in their application for the generated code

C. Credit the author of the generated code in their application

D. Check the sources the AI tool is using for copyrighted content

Answer: (SHOW ANSWER)

To legally use AI-generated code, the developer must ensure that the generated content does not incorporate copyrighted material without permission. Verifying the sources used by the AI tool helps confirm that the code does not violate intellectual property rights and reduces legal risk.

NEW QUESTION: 171

A technician is helping to create a desktop backup policy for the company. The requirements include ensuring that the backups work as intended and recovery is possible. Which of the following routine tasks should the technician include in the policy to meet these requirements?

(Choose two.)

A. Incremental backup

B. Backup reconfiguration

C. Backup testing

D. Differential backup

E. Purging old backups

F. Full backup

Answer: (SHOW ANSWER)

Backup testing verifies that backups are valid and can be successfully restored, ensuring recovery is possible.

Full backup creates a complete copy of all data, providing a reliable baseline needed for successful restoration.

NEW QUESTION: 172

A technician is working on a user's computer. The technician wants to log in to the intranet on the computer without logging the current user out. Which of the following should the technician do?

A. Configure the proxy server.

B. Enable the pop-up blocker on the browser.

C. Use private browsing.

D. Clear the browser cache.

Answer: (SHOW ANSWER)

Private browsing allows the technician to log in to the intranet without affecting the current user's

session, cookies, or logins.

NEW QUESTION: 173
Which of the following filesystem types does the Linux OS use?
A. exFAT
B. APFS
C. ext4
D. NTFS
Answer: (SHOW ANSWER)
ext4 (Fourth Extended Filesystem) is the default filesystem for most Linux distributions. It offers improved performance, reliability, and support for large volumes and files compared to its predecessors (ext2/ext3).

NEW QUESTION: 174
A technician follows the proper procedure for malware removal on an infected computer. However, the technician is unable to remove all the malware and decides to reload the OS. Which of the following should the technician select?
A. Version upgrade
B. System restore
C. OS repair
D. Clean install
Answer: (SHOW ANSWER)
A clean install removes the current OS and all existing data, ensuring all malware is eliminated from the system.

NEW QUESTION: 175
Users access an internal application through a browser website. When a user is browsing the site a message appears that states it is not safe. The message also displays an Advanced Options button to continue or close the site. During security training, all users were told to close any site that displays this message. Which of the following should the technician do to resolve the issue?
A. Add the site to a list of safe senders
B. Install a Secure Sockets Layer certificate for the site
C. Migrate the site to a different server
D. Move the site to a web-hosting company
Answer: (SHOW ANSWER)
Installing a Secure Sockets Layer certificate ensures the website uses trusted HTTPS encryption, eliminating browser security warnings and allowing users to access the internal application safely without bypassing security alerts.

NEW QUESTION: 176
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: (SHOW ANSWER)

Modern authenticator apps (such as Microsoft Authenticator or Google Authenticator with push capability) can send a push notification to the user's registered device. The user approves or denies the login request via the notification, providing a quick and secure second factor for authentication.

NEW QUESTION: 177

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

A. Anti-malware logs

B. Workstation repair options

C. Bandwidth status as reported in the Task Manager

D. File size and related memory utilization

Answer: (SHOW ANSWER)

A very large or complex spreadsheet can consume excessive RAM and CPU cycles, causing the application to hang or become unresponsive. By checking the file's size and monitoring how much memory Excel (or the spreadsheet program) uses when opening it, the technician can confirm whether resource exhaustion is the culprit and take steps - like simplifying the file or adding RAM - to resolve the issue.

NEW QUESTION: 178

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: (SHOW ANSWER)

An Acceptable Use Policy outlines what activities employees are permitted or prohibited from performing when using the organization's IT resources. It provides clear guidance on acceptable behavior, ensuring users understand the rules governing company systems and data.

NEW QUESTION: 179

A technician needs to download and install a new web browser on a desktop computer. Which of the following should the technician use to verify the installer is an authentic version?

A. Date

B. Hash
C. Size
D. Name
Answer: (SHOW ANSWER)
Verifying the hash of the installer ensures that the downloaded file is authentic and has not been tampered with.

NEW QUESTION: 180
A user is unable to use the latest version of an application on a legacy, personal tablet. Which of the following is most likely the reason?
Freecram.net
A. The OS is end-of-life
B. Space is inadequate
C. MDM is blocking updates
D. The tablet is infected with malware
Answer: (SHOW ANSWER)
The OS is end-of-life, which prevents the latest version of the application from being supported or installed on the legacy tablet.

NEW QUESTION: 181
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: (SHOW ANSWER)
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.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF**
Special Discount Code: freecram)

NEW QUESTION: 182
A remote user reports that their screen displays the message, "All of your files have been encrypted.

If you want your files back, you will need to pay us in Bitcoin." Which of the following should a technician do first?

A. Reimage the user's computer.

B. Run updates on the antivirus solution.

C. Scan for malware.

D. Quarantine the infected system.

Answer: (SHOW ANSWER)

The correct answer is D. Quarantine the infected system. The message describes ransomware because the files are encrypted and the attacker is demanding Bitcoin payment. The Mike Meyers/Mark Soper material explains that ransomware encrypts all accessible data and often demands payment in bitcoins for decryption. Quentin Docter's Complete Study Guide explains that ransomware can spread quickly across a network and encrypt files in its path. It also states that after malware is confirmed, the infected system should be quarantined to prevent spread to other systems or network resources. Reimaging and restoring data may be required later, and updating/scanning anti-malware is part of remediation. However, the first action after identifying an active ransomware infection is isolation. Quarantining the system protects shared drives, other endpoints, and network resources from further encryption.

NEW QUESTION: 183

A technician needs to configure settings for password complexity and failed log-in attempts before a user is locked out. These settings cannot be changed by standard users. Which of the following MMC snap-ins should the technician use?

A. taskschd

B. lusrmgr

C. perfmon

D. gpsdit

Answer: (SHOW ANSWER)

The gpedit (Group Policy Editor) MMC snap-in is used to configure password complexity and account lockout policies that standard users cannot change.

NEW QUESTION: 184

Which of the following is used to determine how many active users are currently logged in to the Remote Desktop Services?

A. Local Users and Groups

B. System Information

C. Group Policy Editor

D. Task Manager

Answer: D (LEAVE A REPLY)

Task Manager in Windows allows administrators to view the number of active user sessions connected through Remote Desktop Services under the "Users" tab.

NEW QUESTION: 185
A company wants to use its directory database to authenticate users to its wireless network.
Which of the following should the company use to accomplish this task?
A. MFA
B. WPA3
C. RADIUS
D. LDAP
Answer: (SHOW ANSWER)
RADIUS allows integration with directory databases to authenticate users to the wireless network.

NEW QUESTION: 186
Which of the following types of malware collects and sends data to an unknown third party without the user's consent?
A. Ransomware
B. Virus
C. Trojan
D. Spyware
Answer: (SHOW ANSWER)
Spyware is designed specifically to collect user or system data and transmit it to a third party without the user's knowledge or consent.

NEW QUESTION: 187
Which of the following is found in an SDS for a battery backup?
A. Installation instructions
B. Emergency procedures
C. Configuration steps
D. Voltage specifications
Answer: (SHOW ANSWER)
A Safety Data Sheet contains information about hazards, handling, storage, and emergency procedures related to a product. For a battery backup, it includes guidance on what to do in case of exposure, leaks, spills, or other hazardous situations.

NEW QUESTION: 188
Which of the following security measures addresses the issue of information exfiltration?
A. DLP
B. MDM
C. SAML
D. IAM
Answer: A (LEAVE A REPLY)
Data Loss Prevention is designed to monitor, detect, and prevent unauthorized transmission of sensitive data outside the organization. It directly addresses information exfiltration by controlling

how data is accessed, shared, or transferred.

NEW QUESTION: 189
Which of the following script types requires that the system mode is set to Unrestricted to run unsigned scripts?
A. .js
B. .py
C. .ps1
D. .bat
Answer: (SHOW ANSWER)
PowerShell scripts (.ps1) require the execution policy to be set to Unrestricted (or another permissive level) to run unsigned scripts.

NEW QUESTION: 190
A company wants to reduce the negative ecological impacts of its business and has decided to hire an e-waste company to dispose of equipment. Which of the following should the e-waste company provide the business?
Freecram.net
A. Non-disclosure agreement
B. Certification of destruction
C. Low-level formatting
D. Shredding/drilling
Answer: (SHOW ANSWER)
When disposing of e-waste, it is important to ensure that the data on the equipment is securely destroyed and that the disposal process complies with environmental regulations.
Non-disclosure agreement: Relates to confidentiality, not disposal.
Certification of destruction: The correct document verifying that the equipment has been disposed of in accordance with regulations and standards, ensuring data is irretrievably destroyed.
Low-level formatting: A method to wipe data but does not guarantee compliance with e-waste disposal regulations.
Shredding/drilling: Physical destruction methods that might be used, but certification of destruction is the documentation needed.

NEW QUESTION: 191
After using a third-party disk optimization software package, a technician restarts a laptop and receives the message No operating system found. The technician verifies that the BIOS properly recognizes the SSD. Which of the following should the technician do next?
A. Update BitLocker settings in the BIOS
B. Replace the CMOS battery
C. Boot from installation media and repair the MBR
D. Isolate the system from the corporate network
Answer: (SHOW ANSWER)
Repairing the Master Boot Record (MBR) from installation media is the next step, as the disk

optimization software may have corrupted or removed the boot information, causing the "No operating system found" error.

NEW QUESTION: 192
Which of the following is the best way to distribute custom images to 800 devices that include four device vendor classes with two types of user groups?
A. Use xcopy to clone the hard drives from one to another.
B. Use robocopy to move the files to each device.
C. Use a local image deployment tool for each device.
D. Use a network-based remote installation tool.
Answer: (SHOW ANSWER)
A network-based remote installation tool (such as Windows Deployment Services, MDT, or a similar solution) scales efficiently across hundreds of devices with varying hardware and user configurations. It allows you to segment deployments by vendor classes and user groups, automate imaging processes, and manage version control centrally - far more effectively than one-to-one cloning or file-copy methods.

NEW QUESTION: 193
Which of the following port numbers is used for NetBIOS?
A. 110
B. 137
C. 143
D. 445
Answer: (SHOW ANSWER)
NetBIOS commonly uses port 137 for name services, which is responsible for name registration and resolution on a network.

NEW QUESTION: 194
After new device software for a webcam is installed, a Windows PC is experiencing BSOD. The BSOD occurs during a videoconference call. Which of the following should the technician do next?
A. Update the anti-malware signature and scan the system
B. File a warranty claim with the manufacturer
C. Start in Safe Mode and roll back the device driver
D. Reconnect the webcam to the computer
Answer: (SHOW ANSWER)
Starting in safe mode and rolling back the device driver can resolve BSOD issues caused by newly installed or incompatible webcam drivers.

NEW QUESTION: 195
A user wants to use a USB to move a 4.57GB .pst file from one Windows computer to another. Which of the following filesystems should the USB be formatted with?

A. ext4
B. NTFS
C. FAT32
D. APFS
Answer: B (LEAVE A REPLY)
NTFS supports files larger than 4GB, making it suitable for transferring a 4.57GB .pst file using a USB drive.

NEW QUESTION: 196
Which of the following describes a vulnerability that has been exploited before a patch or remediation is available?
A. Spoofing
B. Brute-force
C. DoS
D. zero-day
Answer: (SHOW ANSWER)
A zero-day vulnerability refers to a security flaw that is actively exploited by attackers before the software vendor has released a patch or remediation - meaning defenders have "zero days" to prepare once the exploit becomes known.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here: https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)

NEW QUESTION: 197
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: (SHOW ANSWER)
As spreadsheets grow in size and complexity, they demand more system memory to load and manipulate data. If the file becomes so large that the available RAM is insufficient, the application may fail to open it. Adding more RAM gives the spreadsheet software the resources it needs to load

and work with the expanded dataset.

NEW QUESTION: 198
A technician is testing a new network monitoring application that enables real-time notifications when remote devices go offline. The remote locations are connected to the corporate offices by a VPN connection over the internet. Which of the following should the technician consider before enabling monitoring in all locations?
A. Operational uptime requirements and maintenance windows
B. Bandwidth consumption at headquarters
C. Impact on the remote devices' baseline performance
D. Business use cases for network monitoring
Answer: (SHOW ANSWER)
Monitoring tools can generate alerts during planned downtime or maintenance, so understanding operational uptime requirements and maintenance windows is essential to avoid false positives and ensure accurate, meaningful alerting across all locations.

NEW QUESTION: 199
Which of the following Microsoft Windows versions would most likely be installed on a server?
A. Windows 10 Enterprise
B. Windows 11 Pro
C. Windows 2022
D. Windows 22H2
Answer: (SHOW ANSWER)
Windows Server 2022 is a server-class operating system designed to provide services such as authentication, file sharing, virtualization, and application hosting for an organization's network.

NEW QUESTION: 200
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?
Freecram.net
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: (SHOW ANSWER)
With technical controls updated, EDR signatures current, and the infected system reimaged, the next step is to address the human factor. Educating the user on how to recognize phishing attempts and follow safe practices helps prevent recurrence and strengthens the organization's overall security posture.

NEW QUESTION: 201
Which of the following file types is best for performing automated tasks on startup on a Windows computer?
A. SH
B. MSI
C. BAT
D. EXE
Answer: (SHOW ANSWER)
A .bat file is a batch script used in Windows to execute a series of commands automatically. It is commonly used for automated tasks at startup by placing the script in the Startup folder or configuring it through Task Scheduler.

NEW QUESTION: 202
A user is trying to install new software. The application downloads successfully, but when the user attempts to install the application, the user receives a prompt for credentials. Which of the following would the technician most likely do to resolve this issue?
A. Restart the user's computer.
B. Use a different web browser to download the application.
C. Change the UAC settings.
D. Contact the software vendor for support.
Answer: (SHOW ANSWER)
The credential prompt during installation is caused by User Account Control requiring administrative privileges to install software. Adjusting UAC settings or providing appropriate administrative approval resolves the issue by allowing the installation to proceed with elevated permissions.

NEW QUESTION: 203
A technician fails to remediate ransomware on a Windows PC. The user is asking for the fastest path for the PC to become operational again. Which of the following actions should the technician take next?
A. Educate the end user on safer browsing techniques.
B. Disable System Restore capability.
C. Reimage the system from a good backup.
D. Run optional Windows updates.
Answer: (SHOW ANSWER)
Reimaging the system from a known-good backup is the fastest and most reliable way to restore full functionality after ransomware when remediation attempts have failed, ensuring all malicious components are completely removed.

NEW QUESTION: 204
An employee accidentally installs software on a company PC. The software sends data to a remote server. Which of the following best describes the software?

A. Trojan
B. Spyware
C. Cryptominer
D. Ransomware
Answer: (SHOW ANSWER)
Spyware secretly collects user or system information and sends it to a remote server, matching the described behavior.

NEW QUESTION: 205
A user's monitor shows strange colored lines and flickers when adjusting the brightness. The user requires the device for daily professional tasks. Which of the following should a technician do to effectively address the screen issue, given cost and urgency considerations?
A. Suggest the user use a secondary monitor for essential tasks.
B. Conduct a factory reset to eliminate software issues
C. Install a screen protector to minimize flickering.
D. Check for loose connections on the display.
Answer: (SHOW ANSWER)
Strange colored lines and flickering when adjusting brightness are commonly caused by a loose or faulty display cable connection. Checking and securing the connection is a quick, low-cost step that can immediately resolve the issue without interrupting the user's work.

NEW QUESTION: 206
A technician is helping a remote user. The technician asks the user to open a specific folder on the root directory of the computer. The user cannot find a folder with that name. The technician explains that a few settings are needed to allow the folder to appear. Which of the following should the user do to be able to see the folder? (Choose two.)
A. Adjust the display properties.
B. Open File Explorer.
C. Open the root drive properties.
D. Configure the system settings.
E. Set the view extensions to "on".
F. Check the box to view hidden files.
Answer: (SHOW ANSWER)
Opening File Explorer is required to access folder view options and navigate to the root directory. Viewing hidden files must be enabled because some system folders are hidden by default and will not appear until this option is checked.

NEW QUESTION: 207
Technicians are failing to document user contact information, device asset tags, and a clear description of each issue in the ticketing system. Which of the following should a help desk management team implement for technicians to use on every call?
A. Service-level agreements

B. Call categories
C. Standard operating procedures
D. Knowledge base articles
Answer: (SHOW ANSWER)
Standard operating procedures (SOPs) define consistent, step-by-step guidelines that technicians must follow - such as capturing user contact details, asset tags, and detailed issue descriptions on every ticket. Implementing SOPs ensures thorough and uniform documentation across all calls.

NEW QUESTION: 208
An IT technician must install a new software application across Linux, macOS, and Windows systems within an organization. The installation files are stored on the intranet. Which of the following approaches should the technician take to ensure proper installation?
A. Create a single batch script to automate the installation on all systems.
B. Use OS-specific package managers and deployment tools for installation.
C. Instruct users to use the manufacturer's website to install the application.
D. Install directly from the installation medium on each machine manually.
Answer: (SHOW ANSWER)
The best answer is B because Linux, macOS, and Windows handle application installation differently, so the technician should use the correct tool or deployment method for each operating system. The A+ Core 2 objectives specifically include diverse OS environments, macOS application installation file types such as .dmg, .pkg, and .app, and Linux tools such as apt-get and yum. The Mike Meyers/Mark Soper material explains that macOS software may be installed from the App Store, a .dmg disk image, or a .pkg installer, while Linux commonly uses package- management tools and distro software stores. The All-in-One Exam Guide also emphasizes that package managers install and update software while handling dependencies, which is especially important in Linux. A single Windows batch script would not properly apply to macOS and Linux.
Sending users to the manufacturer's website bypasses organizational control, and manual installation on every system is inefficient and error-prone.

NEW QUESTION: 209
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 (LEAVE A REPLY)
An MDM (Mobile Device Management) management profile allows administrators to enforce corporate policies on Apple devices, such as restricting app installations, configuring network settings, and applying security restrictions. This profile is installed on the device and centrally managed to ensure compliance.

Valid 220-1202 Dumps shared by ExamDiscuss.com for Helping Passing 220-1202 Exam! ExamDiscuss.com now offer the **newest 220-1202 exam dumps**, the ExamDiscuss.com 220-1202 exam **questions have been updated** and **answers have been corrected** get the **newest** ExamDiscuss.com 220-1202 dumps with Test Engine here:
https://www.examdiscuss.com/CompTIA/exam/220-1202/premium/ (**320** Q&As Dumps, **35%OFF** **Special Discount Code: freecram**)