Free Questions for 220-1102 by braindumpscollection

Shared by Bartlett on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A technician requires graphical remote access to various Windows, Linux, and macOS desktops on the company LAN. The security administrator asks the technician to utilize a single software solution that does not require an external internet connection. Which of the following remote access tools is the technician most likely to install?

Options:

A- VNC

B- RMM

C- RDP

D- SSH

Answer:

A

Explanation:

VNC (Virtual Network Computing) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a graphical user interface. VNC does not require an external internet connection, as it works over a local network or a VPN. VNC uses a client-server model, where the server runs on the remote desktop and the client connects to it from another device.VNC can transmit the keyboard and mouse events from the client to the server, and the screen updates from the server to the client, enabling the technician to interact with the remote desktop as if it were local12.

VNC is a better option than the other choices because:

RMM (Remote Monitoring and Management) (B) is not a single software solution, but a category of software solutions that enable IT professionals to remotely monitor, manage, and troubleshoot multiple devices and networks. RMM software may include remote access tools, but also other features such as patch management, backup and recovery, security, reporting, and automation.RMM software may require an external internet connection, as it often relies on cloud-based services or web-based consoles34.

RDP (Remote Desktop Protocol) is a remote access tool that allows the technician to access and control Windows desktops on the company LAN using a graphical user interface. However, RDP is not compatible with Linux or macOS desktops, unless they have third-party software installed that can emulate or translate the RDP protocol.RDP also has some security and performance issues, such as encryption vulnerabilities, bandwidth consumption, and latency problems56.

SSH (Secure Shell) (D) is a remote access tool that allows the technician to access and control various Windows, Linux, and macOS desktops on the company LAN using a command-line interface. SSH does not require an external internet connection, as it works over a local network or a VPN. SSH uses encryption and authentication to secure the communication between the client and the server.However, SSH does not provide a graphical user interface, which may limit the functionality and usability of the remote desktop7.

1: What is VNC?- Definition from Techopedia12: How VNC Works - RealVNC23: What is Remote Monitoring and Management (RMM)?- Definition from Techopedia34: What is RMM Software?- NinjaRMM45: What is Remote Desktop Protocol (RDP)?- Definition from Techopedia56: Remote Desktop Protocol: What it is and how to secure it - CSO Online67: What is Secure Shell (SSH)?- Definition from

Question 2

Question Type: MultipleChoice

A user is unable to access a remote server from a corporate desktop computer using the appropriate terminal emulation program. The user contacts the help desk to report the issue. Which of the following clarifying questions would be most effective for the help desk technician to ask the user in

Options:

A- order to understand the issue?

B- What is the error message?

C- Does the program work on another computer?

D- Did the program ever work?

E- Is anyone else having this issue?

Answer:

A

Explanation:

The most effective clarifying question for the help desk technician to ask the user in order to understand the issue is

A) What is the error message? This question will help the technician to identify the possible cause and solution of the problem, as the error message will provide specific information about the nature and location of the error, such as the server name, the port number, the protocol, the authentication method, or the network status. The error message will also help the technician to troubleshoot the issue by following the suggested steps or searching for the error code online .

This question is more effective than the other choices because:

B) Does the program work on another computer? is not a very helpful question, as it will not reveal the source of the error or how to fix it. The program may work on another computer for various reasons, such as different network settings, firewall rules, permissions, or software versions. However, this question will not tell the technician what is wrong with the user's computer or the remote server, or what needs to be changed or updated to make the program work.

C) Did the program ever work? is not a very relevant question, as it will not address the current issue or how to resolve it. The program may have worked in the past, but it may have stopped working due to changes in the network configuration, the server status, the software updates, or the user credentials. However, this question will not tell the technician what has changed or how to restore the program functionality.

D) Is anyone else having this issue? is not a very useful question, as it will not explain the reason or the solution for the error. The issue may affect only the user, or multiple users, depending on the scope and the impact of the error. However, this question will not tell the technician what is causing the error or how to fix it for the user or the others.

: How to Troubleshoot Terminal Emulation Problems - Techwalla : How to Read and Understand Windows Error Messages - Lifewire : How to Troubleshoot Network Connectivity Problems - How-To Geek : How to Troubleshoot Software Problems - dummies : How to Troubleshoot Common PC Issues For Users - MakeUseOf

Question 3

Question Type: MultipleChoice

A large organization is researching proprietary software with vendor support for a multiuser environment. Which of the following EULA types should be selected?

Options:

A- Corporate

B- Perpetual

C- Open-source

D- Personal

Answer:

A

Explanation:

A corporate EULA is a type of end-user license agreement that is designed for a large organization that needs to use proprietary software with vendor support for a multiuser environment. A corporate EULA typically grants the organization a volume license that allows it to install and use the software on multiple devices or servers, and to distribute the software to its employees or affiliates. A corporate EULA also usually provides the organization with technical support, maintenance, updates, and warranty from the software vendor, as well as some customization options and discounts.A corporate EULA may also include terms and conditions that specify the rights and obligations of both parties, such as confidentiality, liability, indemnification, termination, and dispute resolution12.

A corporate EULA is a better option than the other choices because:

A perpetual EULA (B) is a type of end-user license agreement that grants the user a permanent and irrevocable license to use the software, without any time limit or expiration date. However, a perpetual EULA does not necessarily include vendor support, updates, or warranty, and it may not allow the user to install the software on multiple devices or servers, or to distribute the software to other users.A perpetual EULA may also be more expensive than a corporate EULA, as it requires a one-time payment upfront, rather than a recurring subscription fee34.

An open-source EULA is a type of end-user license agreement that grants the user a license to use, modify, and redistribute the software, which is publicly available and free of charge. However, an open-source EULA does not provide any vendor support, maintenance, updates, or warranty, and it may impose some restrictions or obligations on the user, such as disclosing the source code, attributing the original author, or using a compatible license for derivative works.An open-source EULA may not be suitable for a large organization that needs proprietary software with vendor support for a multiuser environment56.

A personal EULA (D) is a type of end-user license agreement that grants the user a license to use the software for personal, non-commercial purposes only. A personal EULA may limit the number of devices or servers that the user can install the software on, and prohibit the user from distributing, copying, or reselling the software to other users. A personal EULA may also provide limited or no vendor support, maintenance, updates, or warranty, and it may have a fixed or renewable term.A personal EULA may not meet the needs of a large organization that needs proprietary software with vendor support for a multiuser environment7.

1: What is a Corporate License Agreement?- Definition from Techopedia12: Corporate License Agreement - Template - Word & PDF23: What is a Perpetual License?- Definition from Techopedia34: Perpetual vs.Subscription Software Licensing: Which Is Best for You?45: What is an Open Source License?- Definition from Techopedia56: Open Source Licenses: Which One Should You Use?67: What is a Personal License Agreement?- Definition from Techopedia7: Personal License Agreement - Template - Word & PDF

Question 4

Question Type: MultipleChoice

A technician is hardening a company file server and needs to prevent unauthorized LAN devices from accessing stored files. Which of the following should the technician use?

Options:

A- Software firewall

B- Password complexity

C- Antivirus application

D- Anti-malware scans

Answer:

A

Explanation:

A software firewall is a program that monitors and controls the incoming and outgoing network traffic on a computer or a server. A software firewall can help prevent unauthorized LAN devices from accessing stored files on a company file server by applying rules and policies that filter the network packets based on their source, destination, protocol, port, or content.A software firewall can also block or allow specific applications or services from communicating with the network, and alert the administrator of any suspicious or malicious activity12.

A software firewall is a better option than the other choices because:

Password complexity (B) is a good practice to protect the file server from unauthorized access, but it is not sufficient by itself. Password complexity refers to the use of strong passwords that are hard to guess or crack by attackers, and that are changed frequently and securely.Password complexity can prevent brute force attacks or credential theft, but it cannot stop network attacks that exploit vulnerabilities in the file server software or hardware, or that bypass the authentication process34.

Antivirus application and anti-malware scans (D) are important tools to protect the file server from viruses and malware that can infect, damage, or encrypt the stored files. However, they are not effective in preventing unauthorized LAN devices from accessing the files in the first place. Antivirus and anti-malware tools can only detect and remove known threats, and they may not be able to stop zero-day attacks or advanced persistent threats that can evade or disable them.Moreover, antivirus and anti-malware tools cannot control the network traffic or the file server permissions, and they may not be compatible with all file server platforms or configurations56.

1: What is a Firewall and How Does it Work?- Cisco12: How to Harden Your Windows Server - ServerMania23: Password Security: Complexity vs.Length - Norton74: Password Hardening: 5 Ways to Protect Your Passwords - Infosec5: What is Antivirus Software and How Does it Work?- Kaspersky6: What is Anti-Malware? - Malwarebytes

Question 5

Question Type: MultipleChoice

A branch office suspects a machine contains ransomware. Which of the following mitigation steps should a technician take first?

Options:

A- Disable System Restore.

B- Remediate the system.

C- Educate the system user.

D- Quarantine the system.

Answer:

D

Explanation:

The first mitigation step that a technician should take when a machine is suspected to contain ransomware is to quarantine the system. This means isolating the infected machine from the network and other devices, to prevent the ransomware from spreading and encrypting more dat

a.The technician can quarantine the system by disconnecting the network cable, turning off the wireless adapter, or using firewall rules to block the traffic from and to the machine12.

This step is more important than the other options because:

Disabling System Restore (A) is not a priority, as it will not stop the ransomware from running or spreading. System Restore is a feature that allows users to restore their system to a previous state, but it may not work if the ransomware has encrypted or deleted the restore points.Moreover, disabling System Restore may prevent the user from recovering some data or settings in the future13.

Remediating the system (B) is the ultimate goal, but it cannot be done before quarantining the system. Remediating the system means removing the ransomware, restoring the data, and fixing the vulnerabilities that allowed the attack. However, this process requires careful analysis, planning, and execution, and it may not be possible if the ransomware is still active and communicating with the

attackers.Therefore, the technician should first isolate the system and then proceed with the remediation steps12.

Educating the system user is a preventive measure, but it is not a mitigation step. Educating the system user means raising awareness and providing training on how to avoid ransomware attacks, such as by recognizing phishing emails, avoiding suspicious links or attachments, and updating and patching the system regularly. However, this step will not help if the system is already infected, and it may not be effective if the user is not willing or able to follow the best practices.Therefore, the technician should focus on resolving the current incident and then educate the user as part of the recovery plan14.

1: How to Mitigate Ransomware Attacks in 10 Steps - Heimdal Security12: 3 steps to prevent and recover from ransomware | Microsoft Security Blog33: How to use System Restore on Windows 10 | Windows Central54: Ransomware Mitigation | Prevention and Mitigation Strategies - Delinea4

Question 6

Question Type: MultipleChoice

A user reports seeing random, seemingly non-malicious advertisement notifications in the Windows 10 Action Center. The notifications indicate the advertisements are coming from a web browser. Which of the following is the best solution for a technician to implement?

Options:

A- Disable the browser from sending notifications to the Action Center.

B- Run a full antivirus scan on the computer.

C- Disable all Action Center notifications.

D- Move specific site notifications from Allowed to Block.

Answer:

A

Explanation:

The best solution for a technician to implement is to disable the browser from sending notifications to the Action Center. This will prevent the random advertisement notifications from appearing in the Windows 10 Action Center, which can be annoying and distracting for the user.The technician can follow these steps to disable the browser notifications1:

Open the browser that is sending the notifications, such as Microsoft Edge, Google Chrome, or Mozilla Firefox.

Go to the browser settings or options menu, and look for the privacy and security section.

Find the option to manage site permissions or notifications, and click on it.

You will see a list of sites that are allowed or blocked from sending notifications to the browser and the Action Center. You can either block all sites from sending notifications, or select specific sites that you want to block or allow.

Save the changes and close the browser settings.

This solution is better than the other options because:

Running a full antivirus scan on the computer (B) is not necessary, as the advertisement notifications are not malicious or harmful, and they are not caused by a virus or malware infection. Running a scan will not stop the notifications from appearing, and it will consume system resources and time.

Disabling all Action Center notifications is not advisable, as the Action Center is a useful feature that shows notifications and alerts from various apps and system events, such as email, calendar, security, updates, etc. Disabling all notifications will make the user miss important information and reminders, and reduce the functionality of the Action Center.

Moving specific site notifications from Allowed to Block (D) is not the best solution, as it will only stop the notifications from some sites, but not from others. The user may still receive advertisement notifications from other sites that are not blocked, or from new sites that are added to the Allowed list. This solution will also require the user to manually manage the list of sites, which can be tedious and time-consuming.

1: How to Disable Annoying Browser Notifications - PCMag

Question 7

Question Type: **MultipleChoice**

A user's Windows computer seems to work well at the beginning of the day. However, its performance degrades throughout the day, and the system freezes when several applications are open. Which of the following should a technician do to resolve the issue? (Select two).

Options:

A- Install the latest GPU drivers.

B- Reinstall the OS.

C- Increase the RAM.

D- Increase the hard drive space.

E- Uninstall unnecessary software.

F- Disable scheduled tasks.

Answer:

C, E

Explanation:

The most likely causes of the user's Windows computer performance degradation and freezing are insufficient RAM and excessive software running in the background. Therefore, the technician should do the following to resolve the issue:

Increase the RAM. RAM is the memory that the computer uses to store and run applications and processes. If the RAM is not enough to handle the workload, the computer will use the hard drive as a virtual memory, which is much slower and can cause performance issues. Increasing the RAM will allow the computer to run more applications and processes smoothly and avoid freezing. The technician should check the system requirements of the applications that the user needs to run, and install additional RAM modules that are compatible

with the motherboard and the existing RAM.The technician should also make sure that the system is managing the page file size automatically, or adjust it manually to optimize the virtual memory usage12.

Uninstall unnecessary software. Software that the user does not need or use can take up valuable disk space and system resources, and can interfere with the performance of other applications. Some software may also run in the background or start automatically when the computer boots up, which can slow down the system and cause freezing. The technician should help the user to identify and uninstall unnecessary software from the control panel or the settings app, and disable unnecessary startup programs from the task manager or the system configuration tool.The technician should also check for and remove viruses and malware that may affect the system performance134.

1: Tips to improve PC performance in Windows - Microsoft Support12: How to Upgrade or Install RAM on Your Windows PC - Lifewire53: How to Uninstall Programs on Windows 10 - PCMag64: How to Fix a Windows Computer that Hangs or Freezes - wikiHow

Question 8

Question Type: **MultipleChoice**

Which of the following is the best reason for sandbox testing in change management?

Options:

A- To evaluate the change before deployment

B- To obtain end-user acceptance

C- To determine the affected systems

D- To select a change owner

Answer:

A

Explanation:

Sandbox testing is a method of testing changes in a simulated environment that mimics the real one, without affecting the actual production system. Sandbox testing is useful for change management because it allows the testers to evaluate the change before deployment, and ensure that it works as intended, does not cause any errors or conflicts, and meets the requirements and expectations of the stakeholders. Sandbox testing also helps to protect the investment in the existing system, as it reduces the risk of introducing bugs or breaking functionality that could harm the customer experience or the business operations. Sandbox testing also gives the testers more control over the customer experience, as they can experiment with different scenarios and configurations, and optimize the change for the best possible outcome.

1: Change Management and Sandbox - Quickbase1 2: Embracing change: Build, test, and adapt in a sandbox environment - Zendesk3

Question 9

Question Type: MultipleChoice

A Linux technician needs a filesystem type that meets the following requirements:

. All changes are tracked.

. The possibility of file corruption is reduced.

* Data recovery is easy.

Which of the following filesystem types best meets these requirements?

Options:

A- ext3

B- FAT32

C- exFAT

D- NTFS

Answer:

A

Explanation:

The ext3 file system is a Linux native file system that meets the requirements of the question. It has the following features:

All changes are tracked. The ext3 file system uses a journaling mechanism that records all changes to the file system metadata in a special log called the journal before applying them to the actual file system.This ensures that the file system can be restored to a consistent state in case of a power failure or system crash12.

The possibility of file corruption is reduced. The journaling feature of ext3 also reduces the possibility of file corruption, as it avoids the need for a full file system check after an unclean shutdown.The file system can be quickly replayed from the journal and any inconsistencies can be fixed12.

Data recovery is easy.The ext3 file system supports undeletion of files using tools such as ext3grep or extundelete, which can scan the file system for deleted inodes and attempt to recover the data blocks associated with them34.

1: Introduction to Linux File System [Structure and Types] - MiniTool12: 7 Ways to Determine the File System Type in Linux (Ext2, Ext3 or Ext4) - Tecmint33: How to Recover Deleted Files in Linux with ext3grep4: How to Recover Deleted Files from ext3 Partitions

Question 10

Question Type: MultipleChoice

A user recently purchased a second monitor and wants to extend the Windows desktop to the new screen. Which of the following Control Panel options should a technician adjust to help the user?

Options:

A- Color Management

B- System

C- Troubleshooting

D- Device Manager

E- Administrative Tools

Answer:

D

Question 11

Question Type: **MultipleChoice**

A technician is troubleshooting a Windows 10 PC that is unable to start the GUI. A new SSD and a new copy of Windows were recently installed on the PC. Which of the following is the most appropriate command to use to fix the issue?

Options:

A- msconfig

B- chkdsk

C- sfc

D- diskpart

E- mstsc

Answer:

C

Explanation:

The sfc command is a tool for scanning and repairing system files that are corrupted or missing on Windows operating systems12. System files are essential files that are required for the proper functioning of the operating system, such as the GUI, drivers, services, and applications. If system files are damaged or deleted, the operating system may fail to start or run properly, causing errors, crashes, or blue screens.

The sfc command can be used to fix the issue of the PC that is unable to start the GUI, assuming that the problem is caused by corrupted or missing system files.The sfc command can be run from the command prompt, which can be accessed by booting the PC from the installation media, choosing the repair option, and selecting the command prompt option3.The sfc command can be used with

different switches, such as /scannow, /verifyonly, /scanfile, or /offbootdir, depending on the situation and the desired action4.The most common switch is /scannow, which scans all the system files and repairs any problems that are found5. The syntax of the sfc command with the /scannow switch is:

sfc /scannow

The sfc command will then scan and repair the system files, and display the results on the screen. If the sfc command is able to fix the system files, the PC should be able to start the GUI normally after rebooting. If the sfc command is unable to fix the system files, the PC may need further troubleshooting or a clean installation of Windows.

Reference: 1: CompTIA A+ Certification Exam Core 2 Objectives, page 102: CompTIA A+ Core 2 (220-1102) Complete Video Course, Lesson 26 Documentation3:How to use SFC Scannow to repair Windows system files4:SFC Command (System File Checker)5:How to Repair Windows 10 using Command Prompt