220-1102Q&As

CompTIA A+ Certification Exam: Core 2

Pass CompTIA 220-1102 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/220-1102.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA Official Exam Center

QUESTION 1

A Windows administrator is creating user profiles that will include home directories and network printers for several new users. Which of the following is the MOST efficient way for the technician to complete this task?

A. Access control

B. Authentication application

C. Group Policy

D. Folder redirection

Correct Answer: C

This falls under the category of Group Policy, which is related to Access Control. in gpedit, you can find settings for networks and printers under Computer Configurations >Administrative Templates.

QUESTION 2

A technician is troubleshooting application crashes on a Windows workstation. Each time the workstation user tries to open a website in a browser, the following message is displayed:

crypt32.d11 is missing not found

Which of the following should the technician attempt FIRST?

A. Rebuild Windows profiles.

B. Reimage the workstation

C. Roll back updates

D. Perform a system file check

Correct Answer: D

If this file is missing or corrupted, it can cause application crashes or errors when trying to open websites in a browser. To fix this, the technician can perform a system file check, which is a utility that scans and repairs corrupted or missing system files. To perform a system file check, the technician can follow these steps: Open the Command Prompt as an administrator. To do this, type cmd in the search box on the taskbar, right-click on Command Prompt, and select Run as administrator. In the Command Prompt window, type sfc /scannow and hit Enter. This will start the scanning and repairing process, which may take some time. Wait for the process to complete. If any problems are found and fixed, you will see a message saying Windows Resource Protection found corrupt files and successfully repaired them. If no problems are found, you will see a message saying Windows Resource Protection did not find any integrity violations. Restart your computer and check if the issue is resolved.

QUESTION 3

A small library has an integrated switch and router that is not wireless. All of the public PCs in the library are connected to the device. Which of the following is the FIRST thing the library should do to deter curious patrons from interfering with the device?

A. Configure DNS to resolve externally rather than internally

B. Enable MAC filtering to permit public PCs

C. Change the default user name and password

D. Set up the DHCP server to use a different gateway option

Correct Answer: C

QUESTION 4

Each time a user tries to go to the selected web search provider, a different website opens. Which of the following should the technician check FIRST?

A. System time

B. IP address

C. DNS servers

D. Windows updates

Correct Answer: C

When a user experiences unexpected or erratic behavior while browsing the internet, it could be caused by the DNS servers. DNS translates human-readable domain names (like google.com) into IP addresses, which computers can use to communicate with web servers. If the DNS servers are not functioning correctly or have been compromised, it can result in the browser being redirected to unintended websites.

QUESTION 5

A user is unable to log in to the domain with a desktop PC, but a laptop PC is working properly on the same network. A technician logs in lo the desktop PC with a local account but is unable to browse to the secure intranet site to get troubleshooting tools. Which of the following is the MOST likely cause of the issue?

A. Time drift

B. Dual in-line memory module failure

C. Application crash

D. Filesystem errors

Correct Answer: A

The most likely cause of the issue is a "time drift". Time drift occurs when the clock on a computer is not synchronized with the clock on the domain controller. This can cause authentication problems when a user tries to log in to the domain. The fact that the technician is unable to browse to the secure intranet site to get troubleshooting tools suggests that there may be a problem with the network connection or the firewall settings on the desktop PC

QUESTION 6

A user updates a mobile device\\'s OS. A frequently used application becomes consistently unresponsive immediately after the device is launched. Which of the following troubleshooting steps should the user perform FIRST?

A. Delete the application\\'s cache.

B. Check for application updates.

C. Roll back the OS update.

D. Uninstall and reinstall the application.

Correct Answer: B

Checking for application updates is the first troubleshooting step that the user should perform, because the application may not be compatible with the new OS version and may need an update to fix the issue. Deleting the application\\'s cache,

rolling back the OS update, or uninstalling and reinstalling the application are possible solutions, but they are more time-consuming and disruptive than checking for updates.

References:

https://www.comptia.org/training/resources/exam-objectives/comptia-a-core-2-exam-objectives

https://www.lifewire.com/how-to-update-apps-on-android-4173855

QUESTION 7

A user corrects a laptop that is running Windows 10 to a docking station with external monitors when working at a desk. The user would like to close the laptop when it is docked, but the user reports it goes to sleep when it is closed. Which of the following is the BEST solution to prevent the laptop from going to sleep when it is closed and on the docking station?

A. Within the Power Options of the Control Panel utility click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the Plugged In category to Never

B. Within the Power Options of the Control Panel utility, click the Change Plan Settings button for the enabled power plan and select Put the Computer to Sleep under the On Battery category to Never

C. Within the Power Options of the Control Panel utility select the option Choose When to Turn Off the Display and select Turn Off the Display under the Plugged In category to Never

D. Within the Power Options of the Control Panel utility, select the option Choose What Closing the Lid Does and select When I Close the Lid under the Plugged in category to Do Nothing

Correct Answer: D

The laptop has an additional option under power and sleep settings that desktops do not have. Switching to do nothing prevents the screen from turning off when closed.

QUESTION 8

A company recently experienced a security incident in which a USB drive containing malicious software was able to covertly install malware on a workstation. Which of the following actions should be taken to prevent this incident from happening again? (Choose two.)

A. Install a host-based IDS.

B. Restrict log-In times.

C. Enable a BIOS password.

D. Update the password complexity.

E. Disable AutoRun.

F. Update the antivirus definitions.

G. Restrict user permissions.

Correct Answer: EG

QUESTION 9

A technician is troubleshooting boot times for a user. The technician attempts to use MSConfig to see which programs are starting with the OS but receives a message that it can no longer be used to view startup items. Which of the following programs can the technician use to view startup items?

A. msinfo32

B. perfmon

C. regedit

D. taskmgr

Correct Answer: D

When troubleshooting boot times for a user, a technician may want to check which programs are starting with the operating system to identify any that may be slowing down the boot process. MSConfig is a tool that can be used to view

startup items on a Windows system, but it may not always be available or functional. In this scenario, the technician receives a message that MSConfig cannot be used to view startup items. As an alternative, the technician can use Task

Manager (taskmgr), which can also display the programs that run at startup. To access the list of startup items in Task Manager, the technician can follow these steps:

Open Task Manager by pressing Ctrl+Shift+Esc.

Click the "Startup" tab.

The list of programs that run at startup will be displayed.

QUESTION 10

A user reports that antivirus software indicates a computer is infected with viruses. The user thinks this happened white browsing the internet. The technician does not recognize the interface with which the antivirus message is presented. Which of the following is the NEXT step the technician should take?

A. Shut down the infected computer and swap it with another computer

B. Investigate what the interface is and what triggered it to pop up

C. Proceed with initiating a full scan and removal of the viruses using the presented interface

D. Call the phone number displayed in the interface of the antivirus removal tool

Correct Answer: B

The technician should not proceed with initiating a full scan and removal of the viruses using the presented interface or call the phone number displayed in the interface of the antivirus removal tool12 Shutting down the infected computer and swapping it with another computer is not necessary at this point12

The technician should not immediately assume that the message is legitimate or perform any actions without knowing what the interface is and what triggered it to pop up. It is important to investigate the issue further, including checking the legitimacy of the antivirus program and the message it is displaying.

QUESTION 11

Which of the following command-line tools will delete a directory?

A. md

B. del

C. dir

D. rd

E. cd

Correct Answer: D

To delete an empty directory, enter rd Directory or rmdir Directory . If the directory is not empty, you can remove files and subdirectories from it using the /s switch. You can also use the /q switch to suppress confirmation messages (quiet mode).

QUESTION 12

Which of the following wireless security features can be enabled lo allow a user to use login credentials to attach lo available corporate SSIDs?

A. TACACS+

B. Kerberos

C. Preshared key

D. WPA2/AES

Correct Answer: D

WPA2/AES (Wi-Fi Protected Access 2/Advanced Encryption Standard) is a wireless security standard that supports enterprise mode, which allows a user to use login credentials (username and password) to authenticate to available corporate SSIDs (service set identifiers). TACACS+ (Terminal Access Controller Access-Control System Plus) and Kerberos are network authentication protocols, but they are not wireless security features. Preshared key is another wireless security feature, but it does not use login credentials. References: https://www.comptia.org/blog/wireless-security-standards https://www.comptia.org/certifications/a

---

QUESTION 13

A company needs employees who work remotely to have secure access to the corporate intranet. Which of the following should the company implement?

A. Password-protected Wi-Fi

B. Port forwarding

C. Virtual private network

D. Perimeter network

Correct Answer: C

A virtual private network (VPN) is a technology that creates a secure and encrypted connection over a public network, such as the internet. A VPN allows remote employees to access the corporate intranet as if they were physically connected to the local network. Password-protected Wi-Fi is a security measure for wireless networks that does not provide access to the corporate intranet. Port forwarding is a technique that allows external devices to access services on a private network through a router, but does not provide access to the corporate intranet. A perimeter network is a network segment that lies between an internal network and an external network, such as the internet, and provides an additional layer of security, but does not provide access to the corporate intranet.

QUESTION 14

A Windows user recently replaced a computer The user can access the public internet on the computer; however, an internal site at https7/companyintranet.com:8888 is no longer loading. Which of the following should a technician adjust to resolve the issue?

A. Default gateway settings

B. DHCP settings

C. IP address settings

D. Firewall settings

E. Antivirus settings

Correct Answer: D

The technician should adjust the firewall settings to resolve the issue of not being able to access an internal site at https://companyintranet.com:8888. The firewall settings control how the firewall filters and allows network traffic based on rules and policies. The firewall settings may be blocking or preventing the access to the internal site by mistake or by default, especially if the site uses a non-standard port number such as 8888. The technician should check and modify the firewall settings to allow the access to the internal site or its port number. Default gateway settings determine how a computer connects to other networks or the internet. Default gateway settings are not likely to cause the issue of not being able to access an internal site if the user can access the public internet. DHCP settings determine how a computer obtains its IP address and other network configuration parameters automatically from a DHCP server. DHCP settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. IP address settings determine how a computer identifies itself and communicates with other devices on a network. IP address settings are not likely to cause the issue of not being able to access an internal site if the user can access other network resources. Antivirus settings control how the antivirus software scans and protects the computer from malware and threats. Antivirus settings are less likely to cause the issue of not being able to access an internal site than firewall settings, unless the antivirus software has its own firewall feature that may interfere with the network traffic. References: CompTIA A+ Core 2 (220-1002) Certification Exam Objectives Version 4.0, Domain 1.6

QUESTION 15

A user in a corporate office reports the inability to connect to any network drives. No other users have reported this issue. Which of the following is the MOST likely reason the user is having this issue?

A. The user is not connected to the VPN.

B. The file server is offline.

C. A low battery is preventing the connection.

D. The log-in script failed.

Correct Answer: A