220-1102 Software Troubleshooting Study Guide

General Information - When software is deficient, so is the system that uses it, and processes are slowed down, stopped, or threatened. To be skilled in software troubleshooting, you must be knowledgeable in all types of PC and mobile device software issues. These include things like operating system issues, malware use, and security threats. Of the questions on the CompTIA A+ 1102 test, 22% of them concern these types of concepts. Obviously, software troubleshooting requires a lot of thinking on your feet, so *all* the questions about this topic will begin with a scenario.

Windows OS Problems - Many organizations utilize Microsoft Windows as their operating system of choice. This means that, as a tech, you should be able to troubleshoot issues with the Windows OS and quickly identify common problems. Questions in this area will be scenario based.

Common Symptoms - that we see when there is an issue with the Windows OS.

Blue Screen of Death (BSOD) - is a proprietary crash screen on Windows OS. A BSOD that occurs during the initial boot sequence could be caused by bad hardware, drivers, and/or bad applications. Since a BSOD can be caused by many different things, technicians need to research the specific error message provided by the BSOD.

Sluggish Performance - or slow performance is one of the most commonly reported problems with the Windows OS and may be caused by a wide variety of issues. Troubleshooting should start by narrowing down the component that is most affected by the slowdown, such as the CPU, RAM, hard drive, network, or graphics. You should begin by launching the **Task Manager**, which will provide insight into the performance of the various components.

Boot Problems - The boot-up process of a computer occurs when the hardware transfers control of the computer to the OS. A failure to boot occurs when the computer is unable to load the operating system. Troubleshooting begins by collecting as much information as possible. The **Windows Recovery Environment** provides this information as well as options to allow Windows to repair itself via the Startup Repair option.

Frequent Shutdowns - are most often caused by faulty hardware or faulty drivers, but they may also be caused by power settings. To begin troubleshooting, check the **Event Viewer** first to view the Kernel-Boot or Kernel-General logs. These logs will let you know if the OS is shutting down properly or due to a lack of power. If you suspect a hardware problem, the first step is to reinstall the drivers before swapping for known working components.

Services Not Starting - Services are the backbones of our computers. Sometimes, necessary services do not start when the computer loads. Services can be stopped, started, and restarted in the **Services menu** and can also be viewed from **Task Manager**. When a service associated with a specific application won't start, it might be time to consider **reinstalling** it.

Applications Crashing - It is not uncommon for applications to crash on a computer, and there are many different causes for these crashes. When an application crashes, the user may see the application close unexpectedly or simply **freeze**. If the application freezes rather than closes when it crashes, it may be necessary to **end the task** in Task Manager.

Low Memory Warnings - RAM is where the OS stores the data it is currently using. If the RAM on a computer fills up, it will move some of the working data into the page or paging file. A low memory warning occurs when there is not enough room in the page file for RAM to move data to it. The available space in the page file can be configured to auto-allocate space by the Windows OS via the **Control Panel**.

USB Controller Resource Warnings - provides power and a data path to connected devices. Most 2.0 ports can accommodate five concurrent loads of 100 mA, while 3.0 ports can accommodate six concurrent loads of 150 mA. If the connected device draws more power than the USB controller can handle, the USB controller resource warning will appear. The simplest way to address this problem is to **relocate some USB-connected devices** to other USB ports.

System Instability - can cause application crashes. The first step to take is to look for **uninstalled updates** or **patches** for the application or the OS. The **Reliability Monitor** is also a helpful tool that provides information on application crashes as well as the dates when updates and patches were installed. The **Events Viewer** in the Reliability Monitor provides information and insight into Microsoft-based applications.

No OS Found - is a specific type of failure to boot. *No OS found* occurs when the computer is unable to locate OS files. This can be either because the storage devices do not contain any OS files, or the **boot configuration loader** is pointing to the wrong partition.

Slow Profile Load - A profile that takes a long time to load can be a result of having too many applications load at startup. It could also be a result of insufficient hard drive space or memory.

Time Drift - occurs when the **real-time clock (RTC)** on the motherboard begins to shift, causing the computer to run either faster or slower. Time drift on an OS running on hypervisor experiences this issue more drastically due to the fact that the hypervisor has to emulate the RTC rather than be in direct communication with the motherboard. Time drift can cause authentication problems as well as invalidated certificates.

Common Troubleshooting Steps - In the above section, we discussed some of the common symptoms of computer issues. Below, let's look at some common solutions to these problems.
Reboot - many issues really can be solved with a simple reboot. Before diving into any more complicated troubleshooting, a reboot should **always be one of the first steps** in troubleshooting.
Restart Services - Services are related to both system functions and specific applications. If an application or program isn't running as it should, the service should be restarted to see if that helps. Services can be restarted in the **Computer Management MMC** by selecting Services.
Uninstall/Reinstall/Update Applications - Crashing applications may occur when critical files of the application are overwritten or corrupted. The application can be accessed via the **Start Menu** by selecting Settings, then Apps, and then Apps and Features. Once the application is located, you can choose to **repair** or **update** the application and see if the problem is resolved. If the problem persists, the next step is to **uninstall and reinstall** a clean installation of the application.
Add Resources - Computers are built with a finite amount of resources. Adding additional resources, such as RAM, CPUs, GPUs, or SSDs, is **scaling up hardware** and may be required for efficient performance.
Verify Requirements - Applications and software specify minimum requirements for installation. While this is valuable information, always keep in mind that the resources needed to run the application are being used by more than one program.
System File Checker - tool is used to scan files for integrity and replace critical files when an OS stops functioning properly. The System File Checker can be accessed through **Command Prompt** using **sfc.exe** and can be tasked to evaluate all files or a specific file.
Repair Windows - While the System File Checker only replaces files if they fail an integrity check, Repair Windows reinstalls all files from the source media regardless of integrity while maintaining applications and user files. A clean copy of Windows is needed for this process, typically contained on a flash drive or a mounted ISO file.
Restore - System Restore allows for the creation of a restore point. The restore point is a copy of the OS configuration at a specific point in time. Using a restore point allows the user to return the OS to a known working point in time. Windows 10 and 11 have the automatic system restore function disabled by default, so it must be turned on to use.
Reimage - In some extreme cases, it may be easier to simply uninstall and reload the operating system. Windows has options so that files can be saved even when a refresh of the OS is needed.
Roll Back Updates - Although updates are meant to improve computers, sometimes they can corrupt files and cause issues. In these cases, it's necessary to roll back the updates and take your computer to a previous state before the updates were installed.
Rebuild Windows Profiles - If there is only an issue with a specific Windows profile, it may not be necessary to rebuild the entire computer operating system; instead, rebuilding that user's profile could do the trick. This is because profiles can become corrupted.
Personal Computer (PC) Security Issues - Some computer issues have to do with security. To address them, you should be able to spot the signs of particular problems and know the tools available to render a solution. Questions in this area will be scenario based.
Common Symptoms - While symptoms of PC security issues can be highly intricate and complicated, you will need to be familiar with some of the more common symptoms that may indicate a security-related problem.
Unable to Access the Network - The inability to access the network can be caused by various conditions, both security-related and not, such as a **faulty NIC** or improperly installed network software. Security-related inability to access the network can be caused by malware, which can redirect network settings or force the connection to go through a proxy that may attempt to steal data.
Desktop Alerts - An OS infected with **malware** may produce a desktop alert that is designed to look like a legitimate OS alert. These alerts are typically designed to **scare the user** into taking action, such as calling a specified number. When the number is dialed, the threat actor may attempt to sell a product or garner information from the user.
False Antivirus Protection Alerts - One of the most common false alerts is designed to imitate antivirus protection. These alerts tell the end user that their system is at risk and immediate action should be taken. The main goal of such alerts is to **sell a product or collect information** from the user.
Altered System or Personal Files - Indicators of a security issue can also be evident in the files stored on the computer. Malware may rename or delete files as well as alter the permissions on a file, locking the user out. Common malware that can affect files includes the **rootkit**, which gains embedded privileged access to the OS, and ransomware, which holds files or the entire system hostage until a set amount is paid.

Missing/Renamed Files - If an OS is infected with malware, the threat actor may move or rename files or replace the files with malicious files. Also, renaming a file or moving a file changes the **path** of the file. If the file is needed in the running of an application or program, changing the path of the file can render the program useless.
Unwanted OS Notifications - may also be a sign of malware infection. These OS notifications may attempt to coax the user into installing additional malicious programs, possibly in the form of a **Trojan horse** or a program hidden behind a legitimate program.
OS Update Failures - this could be a symptom of a **virus**. Malware can interfere with normal operating system updates.
Browser-Related Symptoms - Security issues can also be evident in a web browser. Since they are so frequently used, the web browser is the easiest avenue for a threat actor to infect a system.
Random/Frequent Pop-Ups - While pop-ups occur for a variety of reasons, including some legitimate reasons, if you click on the wrong pop-up, it may expose you to malware. Pop-ups that occur randomly should be addressed with a **malware cleaner**.
Certificate Warnings - If you are browsing the internet and receive a security alert that a site has an invalid certificate, that could indicate the site is malicious and should be avoided. However, it may simply be that the site has an incorrect PC clock setting, causing its site certificate date to differ from your PC's date. If you do receive a certificate warning, it is best to take caution unless you know for certain the site is safe.
Redirection - If you find your browser has been changed or the results of a search come from a third-party site, it is likely that your browser has been redirected by **malware**. An anti-malware cleaner may or may not address the issue. You may want to restore your system from a known good backup.
Malware Removal - Malware can spread rapidly and cause severe damage to a PC. Discovering malware is just the first step. It's vital that you can remove the malware quickly without causing further damage. Be sure to follow these steps *in order*. Questions in this area will be scenario based.
1. Investigate and Verify Malware Symptoms - Malware is not often as obvious as strange error messages and odd security warnings. It may be as subtle as a slight slowdown of the system or unexplained files appearing. If malware is suspected, the first step is to **identify the type of malware** being used. Antivirus and anti-malware software can be used to identify known threats. Also, various online resources are dedicated to identifying malware and its signatures.
2. Quarantine Infected Systems - Any system suspected of being infected by malware should immediately be quarantined. This is so that the malware doesn't spread across the network to other devices. The easiest way to quarantine a device is to simply pull out the network cord or disconnect it from Wi-Fi. **Maintain all the files** on the machine, and **don't attempt to move them** to another system.
3. Disable System Restore in Windows - The next step after quarantine is disabling System Restore in Windows. You do not want the virus to infect your restore points.
4. Remediate Infected Systems - When you have identified the type of malware and ensured that it can't spread to other devices, remediation can begin.
a. Update Anti-Malware Software - The first step is to ensure you have an updated antivirus/anti-malware application with a new engine and signature files.
b. Scanning and Removal Techniques - Once the anti-malware software is updated, restart the system in Safe Mode, the pre-installation environment, and run a **virus scan**. While some viruses are more complicated and may require further remediation techniques, this will be able to remove most basic malware infections.
5. Schedule Scans and Run Updates - When a virus is removed, set the antivirus software to automatically update the signature files and schedule scans to prevent future infections.
6. Enable System Restore and Create a Restore Point in Windows - The next step is to re-enable System Restore and create Windows restore points.
7. Educate the End User - Users are the **last line of defense** when it comes to computer security. There is no antivirus or spam filter program that is 100% accurate, so even with these items in place, the user should be educated on proper email and internet usage to avoid getting a malware infection on their device.
Mobile OS and Application Issues - Portable devices are common in the workplace, so you will need to become familiar with the following items related to the support of these devices. Questions in this area will be scenario based.
Common Symptoms - Like operating systems, mobile operating systems and applications may suffer from common symptoms. These are some of the issues you may encounter on the CompTIA A+ exam.
Application Fails to Launch - it may be because the application was not shut down completely and is still running in the background. Another potential cause of a failure to load is a **corrupted application cache**. When troubleshooting

application failures to launch, first try to force quit the application, then clear the application cache if allowed, and, finally, delete and reinstall the application if the first two options do not remedy the issue.
Application Fails to Close/Crashes - attempt to **recreate the scenario** that caused the issue, which may help narrow down what is causing the failure. Remediation is the same as for a failure to launch. Force quit the application, clear the cache if possible, then uninstall and reinstall the application.
Application Fails to Update - Most application updates are controlled by the Google Play Store or the Apple App Store, which automatically update applications. If an application fails to update, the first step is to try to manually update the application. Make sure that the phone is compatible with the current version of the application as well. If this does not work, force quit the application and reboot the device. You may also need to temporarily disable antivirus or anti-malware on the device. Finally, uninstall and reinstall the application.
Slow to Respond - Slow performance or response time is typically related to **RAM**. RAM usage on a mobile device works like it does on a standard computer. If the device is slow, free up RAM space by closing applications and currently running processes.
OS Fails to Update - on a mobile device, it may be caused by multiple conditions that require similar troubleshooting steps as a desktop OS. First, reboot the system to clear up RAM space, then check the specifications for the updated OS to ensure device compatibility, check storage space, and check network connectivity.
Battery Life Issues - A mobile device battery, like all batteries, has a life span. To increase the life of the battery or to reduce how quickly the battery drains, make sure applications are closed when not in use, limit background applications, allow the device to dim automatically, turn off location services, and disconnect peripherals and Wi-Fi when not in use.
Random Reboots - of a mobile device may be indicative of a hardware problem within the device that may be difficult to diagnose. To troubleshoot, check the most common culprits, including battery health, storage capacity, needed updates, overload of running applications, or auto-restart options.
Connectivity Issues - for mobile devices may include local connectivity issues or broader provider connectivity issues. If, after rebooting the device, the connectivity issue is determined to be a provider issue, contact the provider for support. However, local connectivity issues may be troubleshot.
***Bluetooth* -** To troubleshoot Bluetooth connectivity issues, first check to make sure Bluetooth is enabled and the device is not set to airplane mode. If Bluetooth is enabled, check to ensure the desired device is paired. If not currently paired, pair the device by allowing the mobile device to scan for peripherals within range.
***Wi-Fi* -** connectivity issues can be troubleshot the same way as Bluetooth issues. Make sure Wi-Fi is enabled, make sure the device is not in airplane mode, check to see if a **wireless access point (WAP)** is within range, and connect to it.
***Near-Field Communication (NFC)* -** most commonly used for hands-free/tap payment, may be caused by the distance from the reader, having airplane mode enabled, a phone case, or a faulty reader. You can also try to log out of the payment system and log back in, which will verify the device's credentials.
***AirDrop* -** allows for the transfer of data, such as files and pictures, to other Apple users within a certain proximity of the sender. AirDrop uses both Bluetooth and Wi-Fi to transfer data between devices. Make sure the devices are not in airplane mode and have Bluetooth and Wi-Fi enabled and working properly. Also, check the AirDrop settings on the device to ensure it allows for discoverability as well as transfer.
Screen Does Not Auto-Rotate - is the process of switching automatically between landscape and portrait mode on a screen. If the screen does not auto-rotate, the auto-rotate function is most likely disabled. If auto-rotate is enabled, but the screen still does not rotate, the application may be frozen. Force quit the application or reboot the device. If none of these work, it may be a hardware sensor issue.
Mobile OS and Application Security Issues - Questions in this area will be scenario based.
Security Concerns - there are some security issues that are unique to mobile devices.
Android Package (APK) Source - Unlike an Apple device, Android devices are not proprietary and are **open-source**. Most applications that a user may download are obtained through the **Google Play Store**, which verifies and monitors the APK of the application for malicious or inappropriate content. However, if an application is installed via an untrusted source, it poses the risk of being malicious.
Developer Mode - is a function that allows a user to connect to a device via USB. Developer mode allows increased access to the functionality of the device. The Android OS still offers developer mode, while the latest Apple iOS offers the **Xcode** application, which limits the range of access for a developer while still allowing for the development of iOS applications.
Root Access/Jailbreak - Root access on an Android device allows the user to function as a superuser on the device, with access to the entire OS and device. With root access, the user can **flash** the device and install different OSs. Once a

device is flashed, it will no longer be connected to the manufacturer, meaning it will no longer auto-update or patch the device and OS. **Jailbreaking** is most commonly associated with Apple devices and is similar to rooting an Android device, allowing access to the device's OS.

Bootleg/Malicious Application - typically in the form of an APK, is a premium application that has had the digital rights management removed. Bootleg applications often contain malicious software. Only download applications from a trusted source and check the permissions that the application has on the device.

***Application Spoofing* -** is a security concern for both Apple and Android devices and occurs when an application imitates a legitimate application. Application spoofing acts similarly to a Trojan horse, where malicious software is installed when the user intends to install a legitimate application.

Common Symptoms - that the security-related issue may cause, including high resource utilization, connectivity issues, pop-ups or ads, and missing or altered files or data.

High Network Traffic - can indicate that data is being removed from the device or being sent through the device. To troubleshoot high network traffic, begin opening and closing applications one at a time and look for a usage spike beyond the norm for the application.

Sluggish Response Time - may be indicative of a security problem. First, check to ensure the slow performance is not due to too many applications running at once, and then check individual applications for excessive CPU and RAM usage, which may indicate the application is infected with malware.

Data-Usage Limit Notification - occurs when a device has reached its data limit for a set period. When a data-usage limit notification is sent, the first step is to view typical **usage patterns** for the device to see if usage is out of the ordinary. If the data usage is atypical, malicious software may be exfiltrating data from the device or using the device as a bot to send information through.

Limited Internet Connectivity - is not necessarily a sign of a security issue, as it can be caused by proximity to WAPs or problems with the transceivers or firmware. However, if these potential causes have been ruled out, the limited connectivity may be caused by malicious software using the majority of the bandwidth on the connection.

No Internet Connectivity - like limited internet connectivity, is not necessarily a security-related problem. However, if all other likely scenarios have been exhausted, there are some malicious programs that will stop connectivity completely. To prevent connectivity issues, it is best to use a firewall or anti-malware software.

High Number of Ads - a mobile device can become infected with **adware**, which spams the device with unwanted or unsolicited ads. Adware is typically installed when it is attached to an application. One way to isolate the malicious application is to uninstall and reinstall suspected applications until the ads stop. If this does not work, you may have to perform a factory reset on the device.

Fake Security Warnings - on a mobile device are another symptom of malware infection. If this occurs, factory reset the device and install anti-malware before reinstalling applications.

Unexpected Application Behavior - is not always a sign of malware. Sometimes applications just glitch. However, if a freshly installed application behaves in an unexpected manner, this is a likely sign of a security breach. Run a malware scan on the device and factory reset the device if an application is flagged.

Leaked Personal Files/Data - If a device is infected with malware, there is the potential for leaked files and data. To prevent and limit the impact of a data breach, layer security techniques. Install antivirus or anti-malware software, use a mobile firewall, and employ MFA, data encryption, and remote wipe.