KaozhengPro

IT認證考試題庫

專業平臺

考證寶提供最新考古題與模擬試題
協助您高效通過認證考試

www.kaozhengpro.com

Exam : **220-1202**

Title : CompTIA A+ Certification Exam: Core 2

Version : DEMO

1.A technician needs to provide remote support for a legacy Linux-based operating system from their Windows laptop. The solution needs to allow the technician to see what the user is doing and provide the ability to interact with the user's session.
Which of the following remote access technologies would support the use case?
A. VPN
B. VNC
C. SSH
D. RDP
Answer: B
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The correct answer is VNC (Virtual Network Computing). VNC is a graphical desktop-sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It is platform-independent and widely supported on Linux, which makes it ideal for providing interactive remote support for a Linux-based operating system. It allows the technician not only to view the remote desktop session but also to control it, fulfilling the need to see and interact with the user’s session.
A. VPN (Virtual Private Network) creates a secure tunnel to a network but does not provide desktop sharing or session control by itself.
C. SSH (Secure Shell) provides secure command-line access to Unix/Linux systems but does not offer graphical desktop interaction, which is a requirement in this case.
D. RDP (Remote Desktop Protocol) is primarily a Microsoft protocol, and although it can be made to work on Linux, it is not natively supported on legacy Linux systems, and thus less suitable than VNC in this scenario.
CompTIA A+ 220-1102 Core 2 Objective
Reference: Objective 1.8 – Given a scenario, use features and tools of the operating system.
Under this objective, candidates are expected to be familiar with remote access technologies, including RDP, SSH, and VNC, and understand their appropriate uses and limitations on different platforms such as Windows and Linux.

2.A technician is attempting to join a workstation to a domain but is receiving an error message stating the domain cannot be found. However, the technician is able to ping the server and access the internet.
Given the following information:
IP Address – 192.168.1.210
Subnet Mask – 255.255.255.0
Gateway – 192.168.1.1
DNS1 – 8.8.8.8
DNS2 – 1.1.1.1
Server – 192.168.1.10
Which of the following should the technician do to fix the issue?
A. Change the DNS settings.
B. Assign a static IP address.
C. Configure a subnet mask.
D. Update the default gateway.
Answer: A

Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The issue described—“domain cannot be found” despite the ability to ping the server and access the internet—indicates a DNS resolution problem, not a network connectivity issue. The workstation is currently using public DNS servers (8.8.8.8 and 1.1.1.1) which cannot resolve internal domain names, such as the ones used in Active Directory environments. To resolve this, the technician needs to change the DNS settings to point to the internal DNS server, which in most domain setups is the domain controller itself (likely 192.168.1.10 in this case).
Here’s the breakdown of the incorrect options:
B. Assign a static IP address: The IP is already assigned and functioning; the device can ping and reach the network and internet.
C. Configure a subnet mask: The subnet mask is appropriate for the network range (Class C /24).
D. Update the default gateway: The gateway is valid and allows internet access; this is not the issue.
CompTIA A+ 220-1102 Core 2 Objective
Reference: Objective 1.8 – Given a scenario, use features and tools of the operating system.
Under this objective, candidates must know how to troubleshoot OS-based network configurations, including proper DNS settings in domain environments.

3.A network technician notices that most of the company's network switches are now end-of-life and need to be upgraded.
Which of the following should the technician do first?
A. Implement the change
B. Approve the change
C. Propose the change
D. Schedule the change
Answer: C
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
The first step in the IT change management process is to identify and propose the change. In this case, the technician notices a need (end-of-life network switches), so the appropriate action is to formally propose a change. This proposal would be documented and submitted for approval before any planning or implementation occurs.
According to the CompTIA A+ 220-1102 objectives under Operational Procedures (Domain 4.0), the change management process follows these typical steps:
Submit a change request (Propose the change)
Review and approval (Approve the change)
Planning and scheduling (Schedule the change)
Implementation
Documentation and review
Therefore, proposing the change is the correct first step in accordance with standard ITIL-based change management practices.
Reference: CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information management.
Study Guide Section: Change Management Process

4.MFA for a custom web application on a user's smartphone is no longer working. The last time the user remembered it working was before taking a vacation to another country.
Which of the following should the technician do first?
A. Verify the date and time settings
B. Apply mobile OS patches
C. Uninstall and reinstall the application
D. Escalate to the website developer
Answer: A
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
Multi-Factor Authentication (MFA) apps, especially time-based one-time password (TOTP) apps (e.g., Google Authenticator, Authy), rely on accurate time synchronization between the device and the authentication server. If the user recently traveled internationally, the device may have incorrect date/time settings due to time zone changes or failed synchronization, leading to MFA failure.
The most logical and non-intrusive first step is to verify and correct the date and time settings. This aligns with basic troubleshooting principles—start with the simplest and most likely cause before taking more drastic action.
Reference: CompTIA A+ 220-1102 Objective 2.6: Given a scenario, apply cybersecurity best practices to secure a workstation.
Study Guide Section: Authentication technologies and MFA troubleshooting

5.Which of the following is found in an MSDS sheet for a battery backup?
A. Installation instructions
B. Emergency procedures
C. Configuration steps
D. Voltage specifications
Answer: B
Explanation:
Comprehensive and Detailed Explanation From Exact Extract:
An MSDS (Material Safety Data Sheet), now commonly referred to as SDS (Safety Data Sheet), is a document that provides detailed information on the properties of a particular substance. It includes safety guidelines and emergency procedures related to handling, exposure, fire hazards, and first aid—not installation or configuration instructions.
For a battery backup (UPS device), the MSDS would include emergency procedures such as what to do in case of a chemical spill, exposure to battery acid, or fire hazard due to overheating or chemical leakage. This ensures the safety of personnel and complies with hazardous materials handling regulations.
Reference: CompTIA A+ 220-1102 Objective 4.1: Given a scenario, implement best practices associated with documentation and support systems information management.
Study Guide Section: MSDS/SDS usage and safety documentation