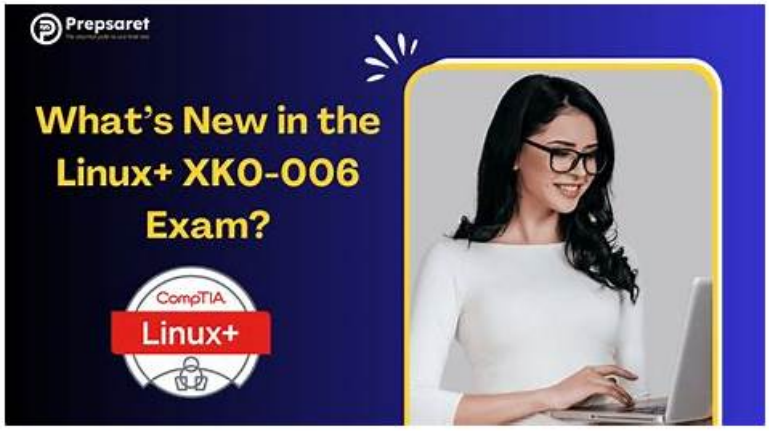
New CompTIA XK0-006 Dumps - Get Ready With XK0-006 Exam Questions



DOWNLOAD the newest RealValidExam XK0-006 PDF dumps from Cloud Storage for free: https://drive.google.com/open?id=13KpZYpj4ZskTKfuQp3JTZG453Mw8UWOO

Our CompTIA Linux+ Certification Exam test torrent was designed by a lot of experts in different area. You will never worry about the quality and pass rate of our study materials, it has been helped thousands of candidates pass their exam successful and helped them find a good job. If you choose our XK0-006 study torrent, we can promise that you will not miss any focus about your exam. There are three different versions to meet customers' needs you can choose the version that is suitable for you to study. If you buy our CompTIA Linux+ Certification Exam test torrent, you will have the opportunity to make good use of your scattered time to learn whether you are at home, in the company, at school, or at a metro station.

Based on high-quality products, our XK0-006 guide torrent has high quality to guarantee your test pass rate, which can achieve 98% to 100%. XK0-006 study tool is updated online by our experienced experts, and then sent to the user. So you don't need to pay extra attention on the updating of study materials. The data of our XK0-006 Exam Torrent is forward-looking and can grasp hot topics to help users master the latest knowledge. If you are not reconciled and want to re-challenge yourself again, we will give you certain discount.

>> Free XK0-006 Study Material <<

2026 High Hit-Rate Free XK0-006 Study Material | XK0-006 100% Free Reliable Study Materials

As is known to us, the XK0-006 certification has been increasingly important for a lot of modern people in the rapid development world. Why is the XK0-006 certification so significant for many people? Because having the certification can help people make their dreams come true, including have a better job, gain more wealth, have a higher social position and so on. Many people are difficult in getting the XK0-006 Certification successfully. If you also have trouble in passing your exam and getting your certification, we think it is time for you to use our XK0-006 quiz prep.

CompTIA XK0-006 Exam Syllabus Topics:

Topic	Details
Topic 1	• Services and User Management: Covers day-to-day Linux administration including file management, user accounts, processes, software, services, and container operations.
Topic 2	• Security: Focuses on securing Linux systems through authentication, firewalls, OS hardening, account policies, cryptography, and compliance checks.
Topic 3	• Automation, Orchestration, and Scripting: Covers task automation with tools like Ansible, shell and Python scripting, Git version control, and responsible AI-assisted development.

Topic 4	• Troubleshooting: Addresses diagnosing and resolving issues across system health, hardware, storage, networking, security configurations, and performance optimization.

CompTIA Linux+ Certification Exam Sample Questions (Q140-Q145):

NEW QUESTION # 140
A Linux administrator just finished setting up passwordless SSH authentication between two nodes. However, upon test validation, the remote host prompts for a password. Given the following logs:
Which of the following is the most likely cause of the issue?

- A. The SELinux policy is incorrectly targeting the unconf ined_u context.
- B. The administrator forgot to restart the SSHD after creating the authorizedjceys file.
- C. The authorized_keys file has the incorrect root permissions assigned.
- D. The authorized_keys file does not have the correct security context to match SELinux policy.

Answer: D

Explanation:
This issue is directly related to SELinux enforcement, which is a key topic in the Security domain of CompTIA Linux+ V8. The logs clearly indicate that SSH key-based authentication is failing due to an SELinux access control violation rather than a traditional file permission or SSH configuration problem.
The most important clue is the AVC denial message, which shows that the sshd process is being denied read access to the authorized_keys file. The security context of the file is listed as unconfined_u:object_r:
home_root_t:s0. Under a targeted SELinux policy, SSH is only permitted to read authorized_keys files that are labeled with the correct SELinux type, typically ssh_home_t.
Because SELinux is running in enforcing mode, it actively blocks access that violates policy rules, even if standard UNIX permissions are correct. Although the file permissions (600) are acceptable for an authorized_keys file, SELinux does not rely solely on traditional permissions. The mismatch between the expected SELinux context and the actual context prevents sshd from accessing the file, causing SSH to fall back to password authentication.
Option D correctly identifies the root cause: the authorized_keys file does not have the correct SELinux security context. This is a well-documented Linux+ V8 troubleshooting scenario, commonly resolved by restoring the correct context using commands such as restorecon or by ensuring the file resides in a properly labeled home directory.
The other options are incorrect. Restarting sshd does not fix SELinux labeling issues. The policy itself is functioning as intended, and file ownership alone does not override SELinux access controls.
Linux+ V8 documentation emphasizes that SELinux denials must be addressed by correcting file contexts rather than weakening security controls. Therefore, the correct answer is D.

NEW QUESTION # 141
A systems administrator is configuring new Linux systems and needs to enable passwordless authentication between two of the servers. Which of the following commands should the administrator use?

- A. ssh-agent -i rsa && ssh-copy-id ~/.ssh/key john@server2
- B. ssh-keyscan -t rsa && ssh-copy-id john@server2 -i ~/.ssh/key
- C. ssh-add -t rsa && scp -rp ~/.ssh john@server2
- D. ssh-keygen -t rsa && ssh-copy-id -i ~/.ssh/id_rsa.pub john@server2

Answer: D

Explanation:
Comprehensive and Detailed 250 to 350 words of Explanation From Linux+ V8 documents:
Passwordless authentication using SSH key pairs is a foundational security practice covered in the Security domain of CompTIA Linux+ V8. It allows administrators to securely authenticate between systems without transmitting passwords over the network, significantly reducing the risk of credential compromise.
The correct approach involves two essential steps: generating an SSH key pair and installing the public key on the remote system. Option A correctly performs both steps using best-practice commands.
The command ssh-keygen -t rsa generates an RSA public/private key pair in the user's ~/.ssh/ directory. The private key (id_rsa) remains securely on the local system, while the public key (id_rsa.pub) is intended to be shared. The second part of the command, ssh-copy-id -i ~/.ssh/id_rsa.pub john@server2, securely copies the public key to the remote server's ~/.ssh/authorized_keys file.

This enables key-based authentication for the specified user.
The other options are incorrect or incomplete. Option B uses ssh-keyscan, which is intended for collecting host keys to populate known_hosts, not for user authentication. Option C misuses ssh-agent, which manages keys already generated and does not create or install them. Option D is insecure and incorrect because copying the entire .ssh directory risks exposing private keys and violates security best practices.
Linux+ V8 documentation emphasizes the use of ssh-keygen and ssh-copy-id as the standard, secure method for configuring passwordless SSH access. This approach ensures proper permissions, correct key placement, and minimal risk.

NEW QUESTION # 142
A systems administrator is decommissioning a service. Which of the following commands should the administrator use to make sure users cannot start the service again?

- A. systemctl disable service
- B. systemctl kill service
- C. systemctl isolate service
- D. systemctl mask service

Answer: D

Explanation:
This command prevents the service from being started manually or automatically by linking it to a null target, ensuring it cannot be restarted even if another service or user attempts to start it.

NEW QUESTION # 143
An administrator has generated an RSA SSH key pair to log in to a remote server. After copying the public key and attempting to log in, the administrator sees the following message:
admin@192.168.10.50: Permission denied (publickey,password)
After seeing the message, the administrator attempts to connect using ssh -v admin@192.168.10.50 and notices the following debug output:
debug1: send_pubkey_test: no mutual signature algorithm
Which of the following actions should the administrator take first to remediate this issue?

- A. Update permissions on the /home/admin/.ssh directory to 700 on the remote server.
- B. Issue systemctl restart sshd on the local server.
- C. Create a new key pair by running ssh-keygen -t ecdsa.
- D. Set PermitRootLogin yes in the /etc/ssh/sshd_config file.

Answer: C

Explanation:
The "no mutual signature algorithm" error means the RSA/SHA-1 key type (ssh-rsa) isn't supported by both client and server. Generating a new key with a modern algorithm (e.g., ssh- keygen -t ecdsa) ensures a mutually supported signature method.

NEW QUESTION # 144
A systems administrator receives reports from users who are having issues while trying to modify newly created files in a shared directory. The administrator sees the following outputs:
Which of the following provides the best resolution to this issue?

- A. Adding a setgidbit to the group in the shared folder
- B. Adding a setuidbit to the user in the shared folder
- C. Manually changing the group of the newly created files
- D. Changing all directory contents to be writable and readable for everyone

Answer: A

Explanation:
Setting the setgid bit on the shared directory ensures that all newly created files and subdirectories inherit the directory's group ownership, allowing all group members to modify files consistently without manual intervention.

NEW QUESTION # 145

......

Passing the XK0-006 exam certification will be easy and fast, if you have the right resources at your fingertips. As the advanced and reliable website, RealValidExam will offer you the best study material and help you 100% pass. XK0-006 online test engine can simulate the actual test, which will help you familiar with the environment of the XK0-006 real test. The XK0-006 self-assessment features can bring you some convenience. The 24/7 customer service will be waiting for you, if you have any questions.