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 : XK0-006

Title : CompTIA Linux+ Certification Exam

Version : DEMO

1.A systems administrator needs to integrate a new storage array into the company's existing storage pool. The administrator wants to ensure that the server is able to detect the new storage array.
Which of the following commands should the administrator use to ensure that the new storage array is presented to the systems?
A. lsscsi
B. lsusb
C. lsipc
D. lshw
Answer: A
Explanation:
From Exact Extract:
The lsscsi command is used to list information about SCSI devices (including storage arrays) that are attached to the system. This is critical when integrating a new storage array because it allows the administrator to verify that the operating system detects the new device at the SCSI layer, which is the underlying interface for most enterprise storage solutions. lsscsi outputs a list of recognized SCSI devices, their device nodes, and associated information.
Other options:
B. lsusb: Lists USB devices, not storage arrays on SCSI/SATA/SAS.
C. lsipc: Displays information on IPC (inter-process communication) facilities, unrelated to hardware detection.
D. lshw: Lists hardware details and can show storage, but lsscsi is specifically designed for SCSI device detection and is the most direct method for this task.
Reference: CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 7: "Managing Storage", Section:
"Identifying and Accessing Storage Devices"
CompTIA Linux+ XK0-006 Objectives: Domain 4.0 – Storage and Filesystems

2.A Linux systems administrator is running an important maintenance task that consumes a large amount of CPU, causing other applications to slow.
Which of the following actions should the administrator take to help alleviate the issue?
A. Increase the available CPU time with pidstat.
B. Lower the priority of the maintenance task with renice.
C. Run the maintenance task with nohup.
D. Execute the other applications with the bg utility.
Answer: B
Explanation:
Process scheduling and resource management are essential Linux administration skills covered in Linux+ V8.
When a process consumes excessive CPU resources, it can negatively impact overall system performance.
The correct solution is to lower the priority of the CPU-intensive task using the renice command. Niceness values influence how much CPU time a process receives relative to others. Increasing the niceness value reduces the process’s priority, allowing other applications to receive CPU resources more fairly.

Option B directly addresses the issue. The other options do not. pidstat monitors processes but does not modify CPU allocation. nohup allows a process to continue running after logout but does not affect scheduling priority. bg resumes a stopped job in the background but does not reduce CPU usage. Linux+ V8 documentation explicitly references nice and renice for managing CPU contention. Therefore, the correct answer is B.

3.A Linux administrator attempts to log in to a server over SSH as root and receives the following error message: Permission denied, please try again. The administrator is able to log in to the console of the server directly with root and confirms the password is correct.
The administrator reviews the configuration of the SSH service and gets the following output:

```
Port 22
PermitRootLogin prohibit-password
PasswordAuthentication yes
PermitEmptyPassword no
Use PAM no
MaxSessions 1
MaxAuthTries 3
```

Based on the above output, which of the following will most likely allow the administrator to log in over SSH to the server?
A. Log out other user sessions because only one is allowed at a time.
B. Enable PAM and configure the SSH module.
C. Modify the SSH port to use 2222.
D. Use a key to log in as root over SSH.
Answer: D
Explanation:
The SSH configuration option PermitRootLogin prohibit-password prevents the root user from logging in with password authentication. This setting means root cannot use a password to log in via SSH; only key-based authentication is permitted for root. The administrator can still log in as root locally, which is not affected by this SSH configuration. To allow SSH access as root, the administrator must use an SSH key instead of a password.
Other options:
A. MaxSessions controls the number of simultaneous SSH sessions but is not causing the login denial here.
B. PAM (Pluggable Authentication Modules) is disabled, but enabling it is not required for basic SSH authentication.
C. Changing the SSH port is unrelated to the authentication method issue.
Reference: CompTIA Linux+ Study Guide: Exam XK0-006, Sybex, Chapter 11: "Securing Linux", Section: "Securing SSH Access"
CompTIA Linux+ XK0-006 Objectives, Domain 3.0: Security

4.Which of the following is a protocol for accessing distributed directory services containing a hierarchy of users, groups, machines, and organizational units?
A. SMB
B. TLS
C. LDAP

D. KRB-5

Answer: C

Explanation:

Directory services are a key part of enterprise Linux environments and are covered under the Security domain in Linux+ V8. The Lightweight Directory Access Protocol (LDAP) is specifically designed to access and manage distributed directory information.

LDAP directories store structured, hierarchical data such as users, groups, computers, and organizational units. Linux systems commonly use LDAP for centralized authentication, authorization, and identity management. LDAP is also the foundation for services like Active Directory and FreeIPA.

The other options are incorrect. SMB is a file and printer sharing protocol. TLS is an encryption protocol used to secure communications. Kerberos (KRB-5) is an authentication protocol often used alongside LDAP but does not store directory information itself.

Linux+ V8 documentation highlights LDAP as the primary protocol for directory-based identity services. Therefore, the correct answer is C.

5.Users report that a Linux system is unresponsive and simple commands take too long to complete. The Linux administrator logs in to the system and sees the following:

Output 1: 10:06:29 up 235 day, 19:23, 2 users, load average: 8.71, 8.24, 7.71

Output 2:

```
Linux 6.8.0-31-generic (host) 05/10/2024 _x86_64_ (4 CPU)
```

10:07:42	AM	CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	%guest	%gnice	%idle
10:07:42	AM	all	65.88	0	20.54	5.65	0	7.93	0	0	0	0

Which of the following is the system experiencing?

A. High latency

B. High uptime

C. High CPU load

D. High I/O wait times

Answer: C

Explanation:

This scenario is a classic performance troubleshooting case covered under the Troubleshooting domain of the CompTIA Linux+ V8 objectives. The key indicators to analyze are the load average values and the CPU utilization statistics.

The uptime command shows load averages of 8.71, 8.24, and 7.71 over the 1-, 5-, and 15-minute intervals. Load average represents the average number of processes that are either running on the CPU or waiting to run. On a system with 4 CPU cores, a healthy load average would typically be close to or below 4. Load averages consistently near or above 8 indicate that there are significantly more runnable processes than available CPU resources, causing processes to wait and resulting in poor system responsiveness.

The CPU output further confirms this condition. The %idle value is 0, meaning the CPU has no idle time available. The majority of CPU time is spent in user space (65.88%) and system/kernel space (20.54%), indicating heavy computational and kernel activity. While %iowait is present at 5.65%, it is not high enough to suggest that disk I/O is the primary bottleneck.

Option C, high CPU load, best explains the symptoms. High CPU load causes commands to execute slowly because processes are competing for limited CPU time. This directly matches the observed

behavior of the system being unresponsive.
The other options are incorrect. High uptime simply indicates how long the system has been running and does not cause performance issues by itself. High latency is a general term and not a specific diagnosis shown by the metrics provided. High I/O wait times would require a significantly higher %iowait value. According to Linux+ V8 documentation, correlating load averages with CPU core count and utilization is essential for accurate performance diagnosis. Therefore, the correct answer is C. High CPU load.