XK0-005Q&As

CompTIA Linux+ Certification Exam

Pass CompTIA XK0-005 Exam with 100% Guarantee

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

https://www.pass2lead.com/xk0-005.html

100% Passing Guarantee
100% Money Back Assurance

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

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

A Linux administrator would like to use systemd to schedule a job to run every two hours. The administrator creates timer and service definitions and restarts the server to load these new configurations. After the restart, the administrator checks the log file and notices that the job is only running daily. Which of the following is MOST likely causing the issue?

A. The checkdiskspace.service is not running.

B. The checkdiskspace.service needs to be enabled.

C. The OnCalendar schedule is incorrect in the timer definition.

D. The system-daemon services need to be reloaded.

Correct Answer: C

C. The OnCalendar schedule is incorrect in the timer definition.

The issue of the job only running daily is likely due to an incorrect OnCalendar schedule in the timer definition. The OnCalendar directive is used in the timer definition to specify the schedule on which the timer should run. If the schedule is

incorrect, the timer will not run as expected.

For example, if the administrator wants the job to run every two hours, the OnCalendar directive in the timer definition should be set to *:0/2.

To resolve the issue, the administrator should check the timer definition and make sure that the OnCalendar schedule is set correctly. After making the necessary changes, the administrator should reload the timer and service definitions and

check the log file again to see if the job is running as expected.

QUESTION 2

Using AD Query, the security gateway connections to the Active Directory Domain Controllers using what protocol?

A. Windows Management Instrumentation (WMI)

B. Hypertext Transfer Protocol Secure (HTTPS)

C. Lightweight Directory Access Protocol (LDAP)

D. Remote Desktop Protocol (RDP)

Correct Answer: C

When using AD Query, the security gateway connections to the Active Directory Domain Controllers using the Lightweight Directory Access Protocol (LDAP).

AD Query is a feature of Check Point security gateways that enables administrators to perform queries against Active Directory Domain Controllers. These queries can be used for a variety of purposes, such as user authentication and authorization, group policy enforcement, and other security-related tasks. To perform these queries, the security

gateway needs to communicate with the Active Directory Domain Controllers. This communication is typically done using the Lightweight Directory Access Protocol (LDAP), which is a client-server

protocol used for accessing directory services. LDAP is a widely used protocol for accessing Active Directory and is used by many different applications and services for authentication, authorization, and other directory-related functions. Therefore, the correct answer is: C. Lightweight Directory Access Protocol (LDAP).

QUESTION 3

A Linux administrator is installing a web server and needs to check whether web traffic has already been allowed through the firewall. Which of the following commands should the administrator use to accomplish this task?

A. firewalld query-service-http

B. firewall-cmd --check-service http

C. firewall-cmd --query-service http

D. firewalld --check-service http

Correct Answer: C

Correct answer option C. This command queries the firewall daemon (firewalld) to check if the "http" service is currently enabled in the firewall. If the service is enabled, the command will return "yes"; otherwise, it will return "no".

QUESTION 4

Users have reported that the interactive sessions were lost on a Linux server. A Linux administrator verifies the server was switched to rescue.target mode for maintenance. Which of the following commands will restore the server to its usual target?

A. telinit 0

B. systemctl reboot

C. systemctl get-default

D. systemctl emergency

Correct Answer: B

When the system is restarted, the systemd init system will automatically start the services required for the default target. This will include services such as the graphical user interface, networking, and other essential services.

QUESTION 5

A systems administrator created a new Docker image called test. After building the image, the administrator forgot to version the release. Which of the following will allow the administrator to assign the v1 version to the image?

A. docker image save test test:v1

B. docker image build test:vl

C. docker image tag test test:vl

D. docker image version test:v1

Correct Answer: C

To assign a version to a Docker image that has already been built and tagged, the systems administrator should use the docker image tag command. Therefore, the correct option is C, docker image tag test test:v1. The docker image tag command is used to assign a new tag (including a version number) to an existing Docker image.

QUESTION 6

A junior systems administrator has just generated public and private authentication keys for passwordless login. Which of the following files will be moved to the remote servers?

A. id_dsa.pem

B. id_rsa

C. id_ecdsa

D. id_rsa.pub

Correct Answer: D

D. id_rsa.pub

The public authentication key, id_rsa.pub, is typically used to set up passwordless login, also known as SSH key-based authentication. In this scenario, the junior administrator has generated public and private authentication keys, and they need to be moved to the remote servers to set up passwordless login.

The public key, id_rsa.pub, is usually copied to the remote server and added to the ~/.ssh/authorized_keys file on the remote server. This allows the local system to authenticate with the remote server using the private key, id_rsa, without requiring a password.

QUESTION 7

An administrator recently updated the BIND software package and would like to review the default configuration that shipped with this version. Which of the following files should the administrator review?

A. /etc/named.conf.rpmnew

B. /etc/named.conf.rpmsave

C. /etc/named.conf

D. /etc/bind/bind.conf

Correct Answer: C

QUESTION 8

While inspecting a recently compromised Linux system, the administrator identified a number of processes that should not have been running:

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
5545	joe	30	-10	5465	56465	8254	R	0.5	1.5	00:35.3	upload.sh
2567	joe	30	-10	6433	75544	9453	R	0.7	1.8	00:25.1	upload_passwd.sh
8634	joe	30	-10	3584	74537	6435	R	0.3	1.1	00:17.6	uploadpw.sh
4846	joe	30	-10	6426	63234	9683	R	0.8	1.9	00:22.2	upload_shadow.sh

Which of the following commands should the administrator use to terminate all of the identified processes?

A. pkill -9 -f "upload*.sh"

B. kill -9 "upload*.sh"

C. killall -9 -upload*.sh"

D. skill -9 "upload*.sh"

Correct Answer: C

QUESTION 9

Which of the following commands will display the operating system?

A. uname -n

B. uname -s

C. uname -o

D. uname -m

Correct Answer: C

The correct command to display the operating system is C. uname -o.

The uname command is used to print system information. It has several options that can be used to print different types of information.

Here\\'s what each option does in the context of the given question:

A. uname -n: prints the hostname of the machine.

B. uname -s: prints the kernel name of the machine.

C. uname -o: prints the operating system of the machine.

D. uname -m: prints the machine hardware name.

Therefore, the correct option to display the operating system is C (uname -o).

QUESTION 10

A Linux administrator needs to create an image named sda.img from the sda disk and store it in the /tmp directory. Which of the following commands should be used to accomplish this task?

A. dd of=/dev/sda if=/tmp/sda.img

B. dd if=/dev/sda of=/tmp/sda.img

C. dd --if=/dev/sda --of=/tmp/sda.img

D. dd --of=/dev/sda --if=/tmp/sda.img

Correct Answer: B

The correct command is B: dd if=/dev/sda of=/tmp/sda.img.

The dd command is used to create an image of a disk or partition, and the syntax is as follows: dd if=input-file of=output-file. In this case, the input file is the sda disk /dev/sda and the output file is the image file in the /tmp directory /tmp/sda.img.

QUESTION 11

A systems administrator created a web server for the company and is required to add a tag for the API so end users can connect. Which of the following would the administrator do to complete this requirement?

A. hostnamectl status --no-ask-password

B. hostnamectl set-hostname "$(perl -le "print" "A" x 86)"

C. hostnamectl set-hostname Comptia-WebNode -H root@192.168.2.14

D. hostnamectl set-hostname Comptia-WebNode --transient

Correct Answer: C

The hostnamectl set-hostname Comptia-WebNode -H root@192.168.2.14 command sets the hostname of a Linux system.

Here\\'s what each option does:

set-hostname Comptia-WebNode: The set-hostname option sets the hostname of the system to "Comptia-WebNode".

-H root@192.168.2.14: The -H option is used to specify the remote host to connect to. In this case, the administrator is connecting to the remote host with the IP address 192.168.2.14 as the root user.

This command sets the hostname of the remote host with IP address 192.168.2.14 to "Comptia-WebNode" as the root user. The new hostname will persist across reboots unless the administrator changes it again in the future.

QUESTION 12

An administrator needs to make some changes in the IaC declaration templates. Which of the following commands would maintain version control?

A. git clone https://github.com/comptia/linux+-.git git push origin

B. git clone https://qithub.com/comptia/linux+-.git git fetch New-Branch

C. git clone https://github.com/comptia/linux+-.git git status

D. git clone https://github.com/comptia/linuxt+-.git git checkout -b

Correct Answer: D

D. git clone https://github.com/comptia/linux+.git git checkout -b

The git clone command is used to clone a remote Git repository, which in this case is the repository located at https://github.com/comptia/linux+.git. This command will download the entire repository to the local machine.

After cloning the repository, the administrator should create a new branch using the git checkout -b command. This will create a new branch in the Git repository and make it the current branch. The administrator can then make changes to the IaC declaration templates in this branch without affecting the main branch.

QUESTION 13

An administrator is trying to diagnose a performance issue and is reviewing the following output: System Properties: CPU: 4 vCPU Memory: 40GB Disk maximum IOPS: 690 Disk maximum throughput: 44Mbps | 44000Kbps Based on the above output, which of the following BEST describes the root cause?

```
avg-cpu:  %user  %nice  %system  %iowait  %steal  %idle
          2.00   0.00   3.00     32.00    0.00    63.00

Device            tps   kB_read/s   kB_wrtn/s     kB_read     kB_wrtn
sdb            345.00         0.02        0.04 4739073123    23849523
sdb1           345.00     32102.03    12203.01 4739073123    23849523
```

A. The system has reached its maximum IOPS, causing the system to be slow.

B. The system has reached its maximum permitted throughput, therefore iowait is increasing.

C. The system is mostly idle, therefore the iowait is high.

D. The system has a partitioned disk, which causes the IOPS to be doubled.

Correct Answer: B

QUESTION 14

An administrator deployed a Linux server that is running a web application on port 6379/tcp.

SELinux is in enforcing mode based on organization policies.

The port is open on the firewall.

Users who are trying to connect to a local instance of the web application receive Error 13, Permission denied.

The administrator ran some commands that resulted in the following output:

```
# semanage port -l | egrep '(^http_port_t|6379)'
http_port_t tcp 80, 81, 443, 488, 8008, 8009, 8443, 9000

# curl http://localhost/App.php
Cannot connect to App Server.
```

Which of the following commands should be used to resolve the issue?

A. semanage port -d -t http_port_t -p tcp 6379

B. semanage port -a -t http_port_t -p tcp 6379

C. semanage port -a http_port_t -p top 6379

D. semanage port -l -t http_port_tcp 6379

Correct Answer: B

The semanage command is used to manage SELinux policy settings on Linux systems. In this case, the semanage port -a -t http_port_t -p tcp 6379 command is adding a new SELinux port type for the TCP protocol and port number 6379.

Here\\'s what each option does:

-a: The -a option stands for "add", and it is used to add a new SELinux port type.

-t http_port_t: The -t option is used to specify the SELinux type for the new port, in this case, http_port_t.

-p tcp 6379: The -p option is used to specify the protocol and port number, in this case, TCP protocol and port number 6379.

With this command, the SELinux policy is updated to allow the TCP protocol to listen on port number 6379 with the http_port_t type. This is useful in cases where the application requires the use of a non-standard port number for HTTP traffic.

QUESTION 15

Which of the following commands is used to configure the default permissions for new files?

A. setenforce

B. sudo

C. umask

D. chmod

Correct Answer: C

C. umask

umask is a command in Linux that sets the default file permissions for newly created files and directories.

The default permissions are calculated by subtracting the umask value from 777 for files and 666 for directories. The result is the default permission for each bit (r, w, and x).

For example, a umask value of 022 would result in file permissions of 644 (666 - 022) and directory permissions of 755 (777 - 022).

Option A (setenforce) is used to set the enforcement mode of SELinux, the security module in Linux. It is not used to configure the default permissions for new files.

Option B (sudo) is used to run commands with administrative privileges. It is not used to configure the default permissions for new files.

Option D (chmod) is used to change the permissions of existing files and directories, but not to configure the default permissions for new files.