Free Questions for XK0-005 by dumpssheet

Shared by Russell on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

An administrator accidentally installed the httpd RPM package along with several dependencies. Which of the following options is the best way for the administrator to revert the package

installation?

Options:

A) dnf clean all

B) rpm -e httpd

C) apt-get clean

D) yum history undo last

Answer:

D

Explanation:

The yum history undo last command will undo the last transaction, which in this case is the installation of the httpd RPM package and its dependencies. This will remove the packages that were installed and restore the previous state of the system. SeeHow to undo or redo yum transactionsandyum history. Reference 1: https://www.redhat.com/sysadmin/undo-redo-yum-transactions 2: https://man7.org/linux/man-pages/man8/yum.8.html#HISTORY

Question 2

Question Type: MultipleChoice

A user is attempting to log in to a Linux server that has Kerberos SSO enabled. Which of the following commands should the user run to authenticate and then show the ticket grants? (Select TWO).

Options:

A) kinit

B) klist

C) kexec

D) kioad

E) pkexec

F) realm

Answer:

A, B

Explanation:

The following commands can help the user to authenticate and show the ticket grants using Kerberos SSO on a Linux server:

kinit: This command obtains and caches an initial ticket-granting ticket (TGT) for the user from the Kerberos key distribution center (KDC).The user needs to enter their password or use a keytab file to authenticate1.

klist: This command lists the cached tickets, including the TGT and any service tickets, for the user.It also shows the expiration time and flags for each ticket2.

For example, the user can run the following commands to log in and view their tickets:

$ kinit username@REALM

Password for username@REALM:

$ klist

Ticket cache: FILE:/tmp/krb5cc_1000

Default principal: username@REALM

Valid starting Expires Service principal

04/06/2023 16:06:59 04/07/2023 02:06:59 krbtgt/REALM@REALM

renew until 04/13/2023 16:06:59

kinit(1) - Linux man page, section "Description".

klist(1) - Linux man page, section "Description".

Question 3

Question Type: **MultipleChoice**

A systems administrator wants to list all local accounts in which the UID is greater than 500. Which of the following commands will give the correct output?

Options:

A) find /etc/passwd ---size +500

B) cut ---d: fl / etc/ passwd > 500

C) awk -F: '$3 > 500 {print $1}' /etc/passwd

D) sed '/UID/' /etc/passwd < 500

Answer:

C

Explanation:

The correct command to list all local accounts in which the UID is greater than 500 is:

awk -F: '$3 > 500 {print $1}' /etc/passwd

This command uses awk to process the /etc/passwd file, which contains information about the local users on the system. The -F: option specifies that the fields are separated by colons. The $3 refers to the third field, which is the UID. The condition $3 > 500 filters out the users whose UID is greater than 500. The action {print $1} prints the first field, which is the username.

The other commands are incorrect because:

find /etc/passwd ---size +500will search for files that are larger than 500 blocks in size, not users with UID greater than 500.

cut ---d: fl / etc/ passwd > 500will cut the first field of the /etc/passwd file using colon as the delimiter, but it will not filter by UID or print only the usernames. The > 500 part will redirect the output to a file named 500, not compare with the UID.

sed '/UID/' /etc/passwd < 500will use sed to edit the /etc/passwd file and replace any line that contains UID with 500, not list the users with UID greater than 500. The < 500 part will redirect the input from a file named 500, not compare with the UID.

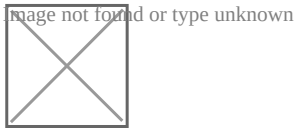
Linux List All Users In The System Command - nixCraft, section "List all users in Linux using /etc/passwd file".

Unix script getting users with UID bigger than 500 - Stack Overflow, section "Using awk".

Question 4

Question Type: MultipleChoice

A user reported issues when trying to log in to a Linux server. The following outputs were received:



Given the outputs above. which of the following is the reason the user is unable to log in to the server?

Options:

A) User1 needs to set a long password.

B) User1 is in the incorrect group.

C) The user1 shell assignment incorrect.

D) The user1 password is expired.

Answer:

D

Explanation:

The user1 password is expired. This can be inferred from the output of the chage -l user1 command, which shows the password expiration information for user1. The output shows that the password expired on 2020-10-01, and the account expired on 2020-10-08. This means that user1 cannot log in to the server unless the password and account are reactivated by the system administrator.

The other options are not correct based on the outputs above. User1 does not need to set a long password, because the output of the passwd -S user1 command shows that the password has a minimum length of 5 characters, which is met by user1's password. User1 is not in the incorrect group, because the output of the groups user1 command shows that user1 belongs to the app group, which is presumably the correct group for accessing the server. The user1 shell assignment is not incorrect, because the output of the grep user1 /etc/passwd command shows that user1 has /bin/bash as the default shell, which is a valid and common shell for Linux users.

Question 5

Question Type: MultipleChoice

Which of the following can be used as a secure way to access a remote terminal?

Options:

A) TFTP

B) SSH

C) SCP

D) SFTP

Answer:

B

Explanation:

SSH, or Secure Shell, is a protocol that allows you to access a remote terminal or virtual machine securely over an encrypted connection. You can use SSH to run commands, transfer files, or tunnel network traffic on a remote system. To use SSH, you need an SSH client program on your local system and an SSH server program on the remote system. You also need to authenticate yourself

using a username and password or a public/private key pair. SSH is widely used by system administrators, developers, and engineers to remotely manage Linux servers and other devices.

The other options are not correct answers. TFTP, or Trivial File Transfer Protocol, is a simple protocol that allows you to transfer files between systems, but it does not provide any security or encryption features. SCP, or Secure Copy Protocol, is a protocol that uses SSH to securely copy files between systems, but it does not provide a remote terminal access. FTP, or File Transfer Protocol, is another protocol that allows you to transfer files between systems, but it also does not provide any security or encryption features.

Question 6

Question Type: **MultipleChoice**

A Linux systems administrator is troubleshooting an I/O latency on a single CPU server. The administrator runs a top command and receives the following output:

%Cpu(s): 0.2 us, 33.1 sy, 0.0 ni, 0.0 id, 52.4 wa, 0.0 hi, 0.2 si, 0.0 st

Which of the following is correct based on the output received from the executed command?

Options:

A) The server's CPU is taking too long to process users' requests.

B) The server's CPU shows a high idle-time value.

C) The server's CPU is spending too much time waiting for data inputs.

D) The server's CPU value for the time spent on system processes is low.

Answer:

C

Explanation:

The server's CPU is spending too much time waiting for data inputs. This can be inferred from the output of the top command, which shows the percentage of CPU time spent in different states. The wa state stands for wait, and it indicates that the CPU is idle while waiting for an I/O operation to complete. In this case, the wa state is 52.4%, which means that more than half of the CPU time is wasted on waiting for data inputs. This can cause a high I/O latency and affect the performance of the server.

The other options are not correct based on the output received from the executed command. The server's CPU is not taking too long to process users' requests, because the us state, which stands for user, is only 0.2%, which means that the CPU is barely used by user processes. The server's CPU does not show a high idle-time value, because the id state, which stands for idle, is 0.0%, which means that the CPU is not idle at all. The server's CPU value for the time spent on system processes is not low, because the sy state, which stands for system, is 33.1%, which means that the CPU is heavily used by system processes.

Question 7

Question Type: MultipleChoice

A systems administrator wants to list all local accounts in which the UID is greater than 500. Which of the following commands will give the correct output?

Options:

A) find /etc/passwd ---size +500

B) cut ---d: fl / etc/ passwd > 500

C) awk -F: '$3 > 500 {print $1}' /etc/passwd

D) sed '/UID/' /etc/passwd < 500

Answer:

C

Explanation:

The correct command to list all local accounts in which the UID is greater than 500 is:

awk -F: '$3 > 500 {print $1}' /etc/passwd

This command uses awk to process the /etc/passwd file, which contains information about the local users on the system. The -F: option specifies that the fields are separated by colons. The $3 refers to the third field, which is the UID. The condition $3 > 500 filters out the users whose UID is greater than 500. The action {print $1} prints the first field, which is the username.

The other commands are incorrect because:

find /etc/passwd ---size +500will search for files that are larger than 500 blocks in size, not users with UID greater than 500.

cut ---d: fl / etc/ passwd > 500will cut the first field of the /etc/passwd file using colon as the delimiter, but it will not filter by UID or print only the usernames. The > 500 part will redirect the output to a file named 500, not compare with the UID.

sed '/UID/' /etc/passwd < 500will use sed to edit the /etc/passwd file and replace any line that contains UID with 500, not list the users with UID greater than 500. The < 500 part will redirect the input from a file named 500, not compare with the UID.

Linux List All Users In The System Command - nixCraft, section "List all users in Linux using /etc/passwd file".

Unix script getting users with UID bigger than 500 - Stack Overflow, section "Using awk".

Question 8

Question Type: **MultipleChoice**

An administrator accidentally installed the httpd RPM package along with several dependencies. Which of the following options is the best way for the administrator to revert the package

installation?

Options:

A) dnf clean all

B) rpm -e httpd

C) apt-get clean

D) yum history undo last

Answer:

D

Explanation:

The yum history undo last command will undo the last transaction, which in this case is the installation of the httpd RPM package and its dependencies. This will remove the packages that were installed and restore the previous state of the system. SeeHow to undo or redo yum transactionsandyum history. Reference 1: https://www.redhat.com/sysadmin/undo-redo-yum-transactions 2: https://man7.org/linux/man-pages/man8/yum.8.html#HISTORY

Question 9

Question Type: MultipleChoice

A Linux systems administrator is troubleshooting an I/O latency on a single CPU server. The administrator runs a top command and receives the following output:

%Cpu(s): 0.2 us, 33.1 sy, 0.0 ni, 0.0 id, 52.4 wa, 0.0 hi, 0.2 si, 0.0 st

Which of the following is correct based on the output received from the executed command?

Options:

A) The server's CPU is taking too long to process users' requests.

B) The server's CPU shows a high idle-time value.

C) The server's CPU is spending too much time waiting for data inputs.

D) The server's CPU value for the time spent on system processes is low.

Answer:

C

Explanation:

The server's CPU is spending too much time waiting for data inputs. This can be inferred from the output of the top command, which shows the percentage of CPU time spent in different states. The wa state stands for wait, and it indicates that the CPU is idle while waiting for an I/O operation to complete. In this case, the wa state is 52.4%, which means that more than half of the CPU time is wasted on waiting for data inputs. This can cause a high I/O latency and affect the performance of the server.

The other options are not correct based on the output received from the executed command. The server's CPU is not taking too long to process users' requests, because the us state, which stands for user, is only 0.2%, which means that the CPU is barely used by user processes. The server's CPU does not show a high idle-time value, because the id state, which stands for idle, is 0.0%, which means that the CPU is not idle at all. The server's CPU value for the time spent on system processes is not low, because the sy state, which stands for system, is 33.1%, which means that the CPU is heavily used by system processes.

Question 10

Question Type: MultipleChoice

Which of the following can be used as a secure way to access a remote terminal?

Options:

A) TFTP

B) SSH

C) SCP

D) SFTP

Answer:

B

Explanation:

SSH, or Secure Shell, is a protocol that allows you to access a remote terminal or virtual machine securely over an encrypted connection. You can use SSH to run commands, transfer files, or tunnel network traffic on a remote system. To use SSH, you need an SSH client program on your local system and an SSH server program on the remote system. You also need to authenticate yourself using a username and password or a public/private key pair. SSH is widely used by system administrators, developers, and engineers to remotely manage Linux servers and other devices.

The other options are not correct answers. TFTP, or Trivial File Transfer Protocol, is a simple protocol that allows you to transfer files between systems, but it does not provide any security or encryption features. SCP, or Secure Copy Protocol, is a protocol that uses SSH to securely copy files between systems, but it does not provide a remote terminal access. FTP, or File Transfer Protocol, is another protocol that allows you to transfer files between systems, but it also does not provide any security or encryption features.

Question 11

Question Type: MultipleChoice

An administrator accidentally deleted the /boot/vmlinuz file and must resolve the issue before the server is rebooted. Which of the following commands should the administrator use to identify the correct version of this file?

Options:

A) rpm -qa | grep kernel; uname -a

B) yum -y update; shutdown -r now

C) cat /etc/centos-release; rpm -Uvh --nodeps

D) telinit 1; restorecon -Rv /boot

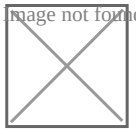
Answer:

A

Question 12

Question Type: MultipleChoice

A user reported issues when trying to log in to a Linux server. The following outputs were received:



Given the outputs above. which of the following is the reason the user is unable to log in to the server?

Options:

A) User1 needs to set a long password.

B) User1 is in the incorrect group.

C) The user1 shell assignment incorrect.

D) The user1 password is expired.

Answer:

D

Explanation:

The user1 password is expired. This can be inferred from the output of the chage -l user1 command, which shows the password expiration information for user1. The output shows that the password expired on 2020-10-01, and the account expired on 2020-10-08. This means that user1 cannot log in to the server unless the password and account are reactivated by the system administrator.

The other options are not correct based on the outputs above. User1 does not need to set a long password, because the output of the passwd -S user1 command shows that the password has a minimum length of 5 characters, which is met by user1's password. User1 is not in the incorrect group, because the output of the groups user1 command shows that user1 belongs to the app group, which is presumably the correct group for accessing the server. The user1 shell assignment is not incorrect, because the output of the grep user1 /etc/passwd command shows that user1 has /bin/bash as the default shell, which is a valid and common shell for Linux users.