Free Questions for XK0-005

Shared by Hammond on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

After connecting to a remote host via SSH, an administrator attempts to run an application but receives the following error:

[user@workstation ~]$ ssh admin@srv1

Last login: Tue Mar 29 18:03:34 2022

[admin@srvl ~] $ /usr/local/bin/config_manager

Error: cannot open display:

[admin@srv1 ~] $

Which of the following should the administrator do to resolve this error?

Options:

A- Disconnect from the SSH session and reconnect using the ssh -x command.
B- Add Options X11 to the /home/admin/.ssh/authorized_keys file.
C- Open port 6000 on the workstation and restart the firewalld service.
D- Enable X11 forwarding in /etc/ssh/ssh_config and restart the server.

Answer:

A

Explanation:

The error indicates that the application requires an X11 display, but the SSH session does not forward the X11 connection. To enable X11 forwarding, the administrator needs to use the ssh -X option, which requests X11 forwarding with authentication spoofing. This will set the DISPLAY environment variable on the remote host and allow the application to open a window on the local display.

Reference

CompTIA Linux+ (XK0-005) Certification Study Guide, page 314

Open a window on a remote X display (why ''Cannot open display'')?, answer by Gilles 'SO- stop being evil'

Question 2

Question Type: MultipleChoice

A Linux administrator is reviewing changes to a configuration file that includes the following section:

```
tls:
    certificates:
        - certFile: /etc/ssl/cert.cer
          keyFile: /etc/ssl/cert.key
          stores: default
        - certFile: /etc/ssl/expired.cer
          keyFile: /etc/ssl/expired.key
          stores: expired
```

The Linux administrator is trying to select the appropriate syntax formatter to correct any issues with the configuration file. Which of the following should the syntax formatter support to meet this goal?

Options:

A- Markdown
B- XML
C- YAML
D- JSON

Answer:

C

Explanation:

The configuration file shown in the image is written in YAML format, so the syntax formatter should support YAML to correct any issues with the file. YAML stands for YAML Ain't Markup Language, and it is a human-readable data serialization language that uses indentation and colons to define key-value pairs. YAML supports various data types, such as scalars, sequences, mappings, anchors, aliases, and tags. The configuration file follows the rules and syntax of YAML, while the other options do not. Markdown is a lightweight markup language that uses plain text formatting to create rich text documents. XML is a markup language that uses tags to enclose elements and attributes. JSON is a data interchange format that uses curly braces to enclose

objects and square brackets to enclose arrays.Reference:CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 21: Automating Tasks with Ansible, page 591.

Question 3

Question Type: MultipleChoice

The development team created a new branch with code changes that a Linux administrator needs to pull from the remote repository. When the administrator looks for the branch in Git, the branch in question is not visible. Which of the following commands should the Linux administrator run to refresh the branch information?

Options:

A- git fetch
B- git checkout
C- git clone
D- git branch

Answer:

A

Explanation:

git fetch is the command used to refresh the list of branches from the remote repository. It retrieves any new branches and updates the local metadata about the remote repository, making the branch visible locally. It does not change the working directory or merge any changes but updates the references.

Question 4

Question Type: MultipleChoice

An administrator is provisioning an Apache web server. When the administrator visits the server website, the browser displays a message indicating the website cannot be reached. Which of the following commands should the administrator use to verify whether the service Is running?

Options:

A- systemctl status httpd
B- systemctl mask httpd
C- systemctl reload httpd
D- systemctl restart httpd

Answer:

A

Explanation:

systemctl status httpd is the correct option to check if the Apache web server (httpd) is running. The systemctl status command provides detailed information about the service, including whether it is active and running.

Question 5

Question Type: MultipleChoice

An application developer received a file with the following content:

##This is a sample Image ##

FROM ubuntu:18.04

MAINTAINER demohut@gtmail.com.hac

COPY . /app

RUN make /app

CMD python /app/app.py

RUN apt-get update

RUN apt-get install -y nginx

CMD ["echo","Image created"]

The developer must use this information to create a test bed environment and identify the image (myimage) as the first version for testing a new

application before moving it to production. Which of the following commands will accomplish this task?

Options:

A- docker build -t myimage:1.0 .
B- docker build -t myimage: .
C- docker build -t myimage-1.0 .
D- docker build -i myimage:1.0 .

Answer:

A

Explanation:

The docker build command is used to build an image from a Dockerfile and a context1.The Dockerfile is a text file that contains the instructions for creating the image, and the context is a set of files that can be used in the image creation process1. The file that the developer received is an example of a Dockerfile.

The -t option is used to specify a name and an optional tag for the image1.The name and tag are separated by a colon (:), and the tag is usually used to indicate the version of the image2. For example, -t myimage:1.0 means that the image will be named myimage and tagged as 1.0.

The last argument of the docker build command is the path to the context, which can be a local directory or a URL1.The dot (.) means that the current working directory is the context2. Therefore, docker build -t myimage:1.0 . means that the image will be built from the Dockerfile and the files in the current working directory, and it will be named myimage and tagged as 1.0.

Question 6

Question Type: MultipleChoice

A Linux administrator has been tasked with installing the most recent versions of packages on a RPM-based OS. Which of the following commands will accomplish this task?

Options:

A- apt-get upgrade
B- rpm -a
C- yum updateinfo
D- dnf update

E- yum check-update

Answer:

D

Explanation:

The dnf update command will accomplish the task of installing the most recent versions of packages on a RPM-based OS. This command will check for available updates from the enabled repositories and apply them to the system. The apt-get upgrade command is used to install updates on a Debian-based OS, not a RPM-based OS. The rpm -a command is invalid, as -a is not a valid option for rpm. The yum updateinfo command will display information about available updates, but it will not install them. The yum check-update command will check for available updates, but it will not install them.Reference:CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 19: Managing Packages and Software, page 559.

Question 7

Question Type: MultipleChoice

User1 is a member of the accounting group. Members of this group need to be able to execute but not make changes to a script maintained by User2. The script should not be accessible to other users or groups. Which of the following will give proper access to the script?

Options:

A- chown user2:accounting script.sh
chmod 750 script.sh
B- chown user1:accounting script.sh
chmod 777 script.sh
C- chown accounting:user1 script.sh
chmod 057 script.sh
D- chown user2:accounting script.sh
chmod u+x script.sh

Answer:

A

Explanation:

The commands that will give proper access to the script are:

chown user2:accounting script.sh: This command will change the ownership of the script to user2 as the owner and accounting as the group. Thechowncommand is a tool for changing the owner and group of files and directories on Linux systems. Theuser2:accountingis the user and group name that the command should assign to the script. Thescript.shis the name of the script that the command should modify. The commandchown user2:accounting script.shwill ensure that user2 is the owner of the script and accounting is the group of the script, which will allow user2 to maintain the script and the accounting group to access the script.

chmod 750 script.sh: This command will change the permissions of the script to 750, which means read, write, and execute for the owner; read and execute for the group; and no access for others. Thechmodcommand is a tool for changing the permissions of files and directories on Linux systems. The permissions are represented by three digits in octal notation, where each digit corresponds to the owner, group, and others. Each digit can have a value from 0 to 7, where each value represents a combination of read, write, and execute permissions. The 750 is the permission value that the command should assign to the script. Thescript.shis the name of the script that the command should modify. The commandchmod 750 script.shwill ensure that only the owner and the group can execute the script, but not make changes to it, and that the script is not accessible to other users or groups.

The commands that will give proper access to the script arechown user2:accounting script.shandchmod 750 script.sh. This is the correct answer to the question. The other options are incorrect because they either do not give proper access to the script (chown user1:accounting script.shorchown accounting:user1 script.sh) or do not change the permissions of the script (chmod 777 script.shorchmod u+x script.sh).Reference:CompTIA Linux+ (XK0-005) Certification Study Guide, Chapter 11: Managing File Permissions and Ownership, pages 346-348.

To Get Premium Files for XK0-005 Visit
https://www.p2pexams.com/products/xk0-005

For More Free Questions Visit
https://www.p2pexams.com/comptia/pdf/xk0-005

