

XK0-004.VCEup.223q

Number: XK0-004  
Passing Score: 800  
Time Limit: 120 min



XK0-004

CompTIA Linux+ Certification Exam



**Exam A****QUESTION 1**

Which of the following would be the BEST solution for a systems administrator to access the graphical user environment of a Linux machine remotely?

- A. VNC
- B. KDE
- C. X11
- D. RPC

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.sfu.ca/computing/about/support/tips/remote-to-linux-with-gui.html>

**QUESTION 2**

A technical support engineer receives a ticket from a user who is trying to create a 1KB file in the `/tmp` directory and is getting the following error: `No space left on device`. The support engineer checks the `/tmp` directory, and it has 20GB of free space.

Which of the following BEST describes a possible cause for this error?

- A. The `/tmp` directory is not mounted.
- B. The filesystem is formatted with a 4MB block size.
- C. the filesystem ran out of inodes.
- D. The `/tmp` directory has been set with an immutable attribute.

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.maketecheasier.com/fix-linux-no-space-left-on-device-error/>

**QUESTION 3** Which of the following is the BEST reason for not storing database files in the `/var` directory?

- A. The `/var` filesystem is not fast enough for database files.
- B. The number of files in `/var` is limited by the available inodes.
- C. Files in `/var` do not have strict file permissions.
- D. If log files fill up `/var`, it might corrupt the database.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 4****SIMULATION**

A junior system administrator had trouble installing and running an Apache web server on a Linux server. You have been tasked with installing the Apache web server on the Linux server and resolving the issue that prevented the junior administrator from running Apache.

**INSTRUCTIONS**

Install Apache and start the service. Verify that the Apache service is running with the defaults. Typing "help" in the terminal will show a list of relevant commands.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

#### CentOS Command Prompt

```
[root@centos7]#
```

Correct Answer: See explanation below

Section: (none)

Explanation

#### Explanation/Reference:

Explanation:

```
[root@tecmint ~]#
[root@tecmint ~]# yum install httpd
Loaded plugins: fastestmirror, refresh-packagekit
Setting up Install Process
Loading mirror speeds from cached hostfile
 * base: centos.excellmedia.net
 * epel: epel.scopesky.iq
 * extras: centos.excellmedia.net
 * updates: centos-hn.viettelidc.com.vn
Resolving Dependencies
There are unfinished transactions remaining. You might consider running yum-comp
lete-transaction first to finish them.
-
[root@tecmint ~]#
[root@tecmint ~]# systemctl start httpd
[root@tecmint ~]#
[root@tecmint ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/ht
[root@tecmint ~]#
[root@tecmint ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2017-06-27 06:51:35 EDT; 14s ago
     Docs: man:httpd(8)
           man:apachectl(8)
   Main PID: 17981 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:  0 B/sec"
   CGroup: /system.slice/httpd.service
           └─17981 /usr/sbin/httpd -DFOREGROUND
             └─17982 /usr/sbin/httpd -DFOREGROUND
               └─17983 /usr/sbin/httpd -DFOREGROUND
                 └─17984 /usr/sbin/httpd -DFOREGROUND
                   └─17985 /usr/sbin/httpd -DFOREGROUND
                     └─17986 /usr/sbin/httpd -DFOREGROUND

Jun 27 06:51:35 tecmint systemd[1]: Starting The Apache HTTP Server...
Jun 27 06:51:35 tecmint httpd[17981]: AH00558: httpd: Could not reliably determine the server's fully qualif
Jun 27 06:51:35 tecmint systemd[1]: Started The Apache HTTP Server.
[root@tecmint ~]#
```

VCEUp

#### QUESTION 5 DRAG

DROP

The lead Linux admin has added a disk, /dev/sdd, to a VM that is running out of disk space. Place the following steps in the correct order from first (1) to last (4) to add the disk to the existing LVM.

Select and Place:

1

2

3

4

`lvextend -L +10GB /dev/mapper/vgdata-data`

`pvcreate /dev/sdd`

`resize2fs /dev/mapper/vgdata-data`

`vgextend vgdata /dev/sdd`

Correct Answer:

1 `pvcreate /dev/sdd`

2 `vgextend vgdata /dev/sdd`

3 `lvextend -L +10GB /dev/mapper/vgdata-data`

4 `resize2fs /dev/mapper/vgdata-data`

`lvextend -L +10GB /dev/mapper/vgdata-data`

`pvcreate /dev/sdd`

`resize2fs /dev/mapper/vgdata-data`

`vgextend vgdata /dev/sdd`

Section: (none)

Explanation

Explanation/Reference:

Reference: <https://www.rootusers.com/how-to-increase-the-size-of-a-linux-lvm-by-expanding-the-virtual-machine-disk/>

#### QUESTION 6

An administrator receives a warning about a filesystem filling up, and then identifies a large file located at `/tmp/largelogfile`. The administrator deletes the file, but no space is recovered on the filesystem.

Which of the following commands would BEST assist the administrator in identifying the problem?

- A. `lsof | grep largelogfile`
- B. `pkill /tmp/largelogfile`
- C. `pgrep largelogfile`
- D. `ps -ef | grep largelogfile`

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://access.redhat.com/solutions/2316>

#### QUESTION 7

Which of the following can be used to boot a DVD from a remote device to initialize a Linux system setup on bare metal hardware as if it is a local DVD?

- A. UEFI
- B. PXE
- C. NFS
- D. GRUB

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html/installation\\_guide/ch-boot-x86](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/installation_guide/ch-boot-x86)

#### QUESTION 8

After starting a long-running script, a systems administrator needs to verify the frequency of what is filling up the /var partition and kill it because it is consuming too much space.

Which of the following is the correct sequence given only a terminal is available?

- A. 1. CTRL-C
  - 2. `bg`
  - 3. `watch df /var`
  - 4. CTRL-C
  - 5. `fg`
  - 6. CTRL-Z
- B. 1. CTRL-C
  - 2. `fg`
  - 3. `watch df /var`
  - 4. CTRL-Z
  - 5. `bg`
  - 6. CTRL-Z
- C. 1. CTRL-Z
  - 2. `bg`
  - 3. `watch df /var`
  - 4. CTRL-C
  - 5. `fg`
  - 6. CTRL-CD
- D. 1. CTRL-Z
  - 2. `bg`
  - 3. `watch df /var`
  - 4. CTRL-Z
  - 5. `fg`
  - 6. CTRL-C

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:****QUESTION 9**

A Linux administrator must identify a user with high disk usage. The administrator runs the `# du -s /home/*` command and gets the following output:

```
43    /home/User1
2701  /home/User2
133089 /home/User3
3611  /home/User4
```

Based on the output, User3 has the largest amount of disk space used. To clean up the file space, the administrator needs to find out more information about the specific files that are using the most disk space.

Which of the following commands will accomplish this task?

- A. `df -k /home/User3/files.txt`
- B. `du -a /home/User3/*`
- C. `du -sh /home/User/`
- D. `find . -name /home/User3 -print`

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://unix.stackexchange.com/questions/37221/finding-files-that-use-the-most-disk-space>

**QUESTION 10**

A Linux server has multiple IPs. A Linux administrator needs to verify if the HTTP server port is bound to the correct IP.

Which of the following commands would BEST accomplish this task?

- A. `route`
- B. `host`
- C. `nslookup`
- D. `netstat`
- E. `ip`

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.tecmint.com/find-listening-ports-linux/>

**QUESTION 11**

A systems administrator needs to append output of `ls -lha /opt` command to the contents of a `test.txt` file. Which of the following commands will accomplish this?

- A. `ls -lha /opt > test.txt`
- B. `ls -lha /opt < test.txt`
- C. `ls -lha /opt >> test.txt`
- D. `ls -lha /opt << test.txt`

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**Reference: <https://www.cyberciti.biz/faq/linux-append-text-to-end-of-file/>**QUESTION 12** A Linux administrator needs to remotely update the contents of the `www.comptia.org/contacts` URL.

Which of the following commands would allow the administrator to download the current contents of the URL before updating?

- A. `curl www.comptia.org/contacts`
- B. `dig www.comptia.org/contacts`
- C. `apt-get www.comptia.org/contacts`
- D. `yum list www.comptia.org/contacts`

**Correct Answer:** A**Section:** (none)**Explanation****Explanation/Reference:**Reference: <https://www.thegeekstuff.com/2012/04/curl-examples/>**QUESTION 13** Which of the following BEST describes containers running on a Linux system?

- A. Containers only need the namespaces functionality to run on a Linux system available since kernel 2.6.
- B. Containers need a hypervisor to run on a Linux system. Cgroups namespaces are functionalities used for the kernel but not for running containers.
- C. Containers only need the cgroups functionality for running on a Linux system. Namespaces is not a Linux kernel functionality needed for creating and managing containers.
- D. Containers use the cgroups and namespaces functionalities to isolate processes and assign hardware resources to each of those isolated processes.

**Correct Answer:** D**Section:** (none)**Explanation****Explanation/Reference:**Reference: <https://www.linuxjournal.com/content/everything-you-need-know-about-linux-containers-part-ii-working-linux-containers-lxc>**QUESTION 14** A networked has been crashing intermittently. A Linux administrator would like to write a shell script that will attempt to ping the server and email an alert if the server fails to respond. The script will later be scheduled via cron job.

Which of the following scripts would BEST accomplish this task? A.

```
SERVER='192.168.1.50'
RESULT='ping -C 2 $SERVER'
if [ ! $RESULT ]; then
    echo "Server is down" | mail -s "Server down" admin@email_address.com
fi
SERVER="192.168.1.50"
ping -c 2 $SERVER >/dev/null 2>/dev/null
if [ $? -ge 1 ]; then
    echo "Server is down" | mail -s "Server down" admin@email_address.com
fi
```

B.

```
SERVER="192.168.1.50"
RESULT='ping -c 2 $SERVER >/dev/null 2>/dev/null'
while [ $RESULT != 1 ];
do
    echo "Server is down" | mail -s "Server down" admin@email_address.com
done
SERVER="192.168.1.50"
ping -c 2 $SERVER >/dev/null 2>/tmp/fail.log
if [ -f /tmp/fail/log ]; then
    echo "Server is down" | mail -s "Server down" admin@email_address.com
fi
```

C.

C.

D.

VCEUp

**Correct Answer: D****Section: (none)****Explanation****Explanation/Reference:****QUESTION 15**

A Linux administrator is testing connectivity to a remote host on a shared terminal. The administrator wants to allow other users to access the terminal while the command is executing.

Which of the following commands should the administrator use?

- A. `bg ping remotehost`
- B. `fg ping remotehost`
- C. `ping remotehost < results`
- D. `ping remotehost &`

**Correct Answer: C****Section: (none)****Explanation****Explanation/Reference:****QUESTION 16**

A Linux administrator needs to switch from text mode to GUI. Which of the following runlevels will start the GUI by default?

- A. Runlevel 3
- B. Runlevel 4
- C. Runlevel 5
- D. Runlevel 6

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [http://www.linfo.org/runlevel\\_def.html](http://www.linfo.org/runlevel_def.html)

#### QUESTION 17

A junior systems administrator is configuring localization option environment variables. The administrator is given a checklist of tasks with the following requirements:

- View current settings of the `LC_ALL` environment variable only.
- Modify the `LANG` environment variable to US English Unicode.

Given this scenario, which of the following should be performed to meet these requirements? (Choose two.)

- A. `echo $LC_ALL`
- B. `locale`
- C. `cat $LC_ALL`
- D. `export LANG = en_US.UTF-8`
- E. `export $LANG = en_US.UTF`
- F. `stty`

**Correct Answer:** BD

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.tecmint.com/set-system-locales-in-linux/>

#### QUESTION 18

An administrator needs to change the IP address on a server remotely. After updating the configuration files, a network restart is needed. However, the administrator fears that when the network connection drops, the network restart script will be killed before the new IP address has been set.

Which of the following commands would prevent the script from being killed?

- A. `nohup service network restart`
- B. `service network restart &`
- C. `echo "service network restart" | at now`
- D. `bg service network restart`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 19

A Linux administrator is testing a new web application on a local laptop and consistently shows the following 403 errors in the laptop's logs:

```
type=AVC msg=audit(126552035:37232):avc:denied {read} for pid=24941 com=nginx nme="/home/user1" /dev/sda1
ino=2 scontext=unconfined_u:system_r:httpd_t:s0 tcontext=system_u:object_r:httpd_sys_content:s0
```

The web server starts properly, but an error is generated in the audit log. Which of the following settings should be enabled to prevent this audit message?

- A. `httpd_can_network_connect = 1`
- B. `httpd_enable_scripting = 1`
- C. `httpd_enable_homedirs = 1`
- D. `httpd_enable_cgi = 1`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 20

Which of the following BEST describes the purpose of the X11 system?

- A. X11 provides graphical display capabilities
- B. X11 provides command line capabilities
- C. X11 provides networking capabilities
- D. X11 provides telephony capabilities.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [https://en.wikipedia.org/wiki/X\\_Window\\_System](https://en.wikipedia.org/wiki/X_Window_System)

**QUESTION 21** An administrator is analyzing a Linux server which was recently hacked.

Which of the following will the administrator use to find all unsuccessful login attempts?

- A. `nsswitch`
- B. `faillock`
- C. `pam_tally2`
- D. `passwd`

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 22** A junior administrator needs to unload an older video kernel module.

Which of the following commands would BEST accomplish this task?

- A. `modprobe`
- B. `insmod`
- C. `rmmmod`
- D. `chmod`
- E. `depmod`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Enterprise\\_Linux/7/html/Kernel\\_Administration\\_Guide/sec-Unloading\\_a\\_Module.html](https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Kernel_Administration_Guide/sec-Unloading_a_Module.html)

**QUESTION 23**

An administrator is attempting to block SSH connections to 192.168.10.24 using the Linux firewall. After implementing a rule, a connection refused error is displayed when attempting to SSH to 192.168.10.24.

Which of the following rules was MOST likely implemented?

- A. `iptables -A -p tcp -d 192.168.10.24 --dport 22 -j REJECT`
- B. `iptables -A -p tcp -d 192.168.10.24 --dport 22 -j DROP`
- C. `iptables -A -p tcp -d 192.168.10.24 --dport 22 -j FORWARD`
- D. `iptables -A -p tcp -d 192.168.10.24 --dport 22 -j REFUSE`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.golinuxhub.com/2014/03/how-to-allowblock-ssh-connection-from.html>

**QUESTION 24**

A junior Linux administrator is setting up system-wide configuration settings. The goal is to ensure the PATH environment variable includes the following locations for all users who log into a Linux system:

`/usr/local/bin`

`/usr/local/sbin`

The administrator issues the following commands at the terminal:

```
echo $PATH
```

```
cat /etc/profile
```

Respectively, the output of these commands is as follows:

```
/usr/bin:/usr/sbin:/sbin:/bin
```

```
# /etc/profile: system-wide .profile file for the Bourne shell (sh(1))
```

```
# and Bourne compatible shells (bash(1), ksh(1), ash(1), ...).
```

```
if [ `id -u` -eq 0 ]; then
```

```
PATH="/usr/bin:/usr/sbin:/sbin:/bin"
```

```
else
```

```
PATH="/usr/local/games"
```

```
fi
```

```
export PATH
```

Given this output, which of the following would be the BEST action for the administrator to perform to address this issue?

- A. Update the `/etc/profile.d` file using a text editor, navigate to the PATH element, add the missing locations, and run the `bash_completion.sh` script to update the changes.
- B. Update the `/etc/profile` file using a text editor, navigate to the PATH element, add the missing locations and run the `. /etc/profile` command to update the changes.
- C. Update the `/etc/profile.d` file using a text editor, navigate to the PATH element, add the missing locations, and reboot to update the changes.
- D. Update the `/etc/profile` file using a text editor navigate to the PATH element, add the missing locations, and restart the bash process to update the changes.

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### QUESTION 25

A Linux systems administrator needs to provision multiple web servers into separate regional datacenters. The systems architect has instructed the administrator to define the server infrastructure using a specific tool that consumes a textbased file.

Which of the following is the BEST reason to do this?

- A. To document the infrastructure so it can be included in the system security plan
- B. To ensure the administrator follows the planning phase of the systems development life cycle
- C. To define the infrastructure so it can be provisioned consistently with minimal manual tasks
- D. To validate user requirements have been met within each regional datacenter for compliance

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 26** A Linux administrator needs to set permissions on an application with the following parameters:

- The owner of the application should be able to read, write, and execute the application.
  - Members of the group should be able to read and execute the application. ▪
- Everyone else should not have access to the application.

Which of the following commands would BEST accomplish these tasks?

- A. `chmod 710 <application name>`
- B. `chmod 730 <application name>`
- C. `chmod 750 <application name>`
- D. `chmod 760 <application name>`

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### QUESTION 27

A junior Linux administrator is trying to verify connectivity to the remote host `host1` and display round-trip statistics for ten ICMP requests.

Which of the following commands should the administrator execute?

- A. `ping -c 10 host1`
- B. `traceroute -c 10 host1`
- C. `netstat host1`
- D. `pathping -c 10 host1`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://shaped.com/unix-ping/>

#### QUESTION 28

A junior Linux administrator is updating local name resolution to support IPv6. The administrator issues the command `cat /etc/hosts` and receives the following output:

```
127.0.0.1 localhost
```

Which of the following actions should the administrator perform to accomplish this task?

- A. Modify the `/etc/hosts` file, and add the `ipv6 localhost` entry to the file.
- B. Modify the `/etc/hosts` file, and add the `::1 localhost` entry to the file.
- C. Modify the `/etc/hosts` file, and add the `ipv4 localhost` entry to the file.
- D. Modify the `/etc/hosts` file, and add the `0.0.0.0 localhost` entry to the file.

**Correct Answer: B**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 29

A Linux systems administrator needs to copy the contents of a directory named “working” on the local working system to a folder `/var/www/html` on a server named “corporate-web”.

Which of the following commands will allow the administrator to copy all the contents to the web server?

- A. `scp -r working/* webuser@corporate-web:/var/www/html`
- B. `tar working/* webuser@corporate-web:/var/www/html`
- C. `cp -r working/* webuser@corporate-web:/var/www/html`
- D. `mv working webuser@corporate-web:/var/www/html`

**Correct Answer: A**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://unix.stackexchange.com/questions/232946/how-to-copy-all-files-from-a-directory-to-a-remote-directory-using-scp>

**QUESTION 30** A systems administrator has received reports of intermittent network connectivity to a particular website. Which of the following is the BEST command to use to characterize the location and type of failure over the course of several minutes?

- A. `mtr www.comptia.org`
- B. `tracert www.comptia.org` C. `ping www.comptia.org`
- D. `netstat www.comptia.org`

**Correct Answer: B**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.lifewire.com/traceroute-linux-command-4092586>

#### QUESTION 31

A Linux administrator has configured a Linux system to be used as a router. The administrator confirms that two network adapters are properly installed and functioning correctly. In addition, the output of the `iptables -L` command appears to contain a complete firewall configuration.

Which of the following commands does the administrator need to issue for the router to be fully functional?

- A. `echo "1" > /proc/sys/net/ipv4/ip_forward`
- B. `echo "0" > /proc/sys/net/ipv4/tcp_abort_on_overflow`
- C. `echo "0" > /proc/sys/net/ipv4/max_connections`
- D. `echo "1" > /proc/sys/net/ipv4/ip_default_ttl`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

### QUESTION 32

A systems administration team has decided to treat their systems as immutable instances. They keep the desired state of each of their systems in version control and apply automation whenever they provision a new instance. If there is an issue with one of their servers, instead of troubleshooting the issue, they terminate the instance and rebuild it using automation.

Which of the following is this an example of?

- A. Inventory
- B. Orchestration
- C. Infrastructure as code
- D. Agentless deployment

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 33** A systems administrator wants to deploy several applications to the same server quickly. Each application should be abstracted from the host with its own dependencies and libraries and utilize a minimal footprint.

Which of the following would be BEST in this scenario?

- A. Virtual machines
- B. Type 2 hypervisor
- C. Chroot jails
- D. Containers

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 34** An operator finds a user is having issues with opening certain files.

Which of the following commands would allow the security administrator to list and check the SELinux context?

- A. `ls -D`
- B. `ls -a`
- C. `ls -Z`
- D. `ls -l`

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html/security-enhanced\\_linux/sect-security-enhanced\\_linux-working\\_with\\_selinux-selinux\\_contexts\\_labeling\\_files](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/security-enhanced_linux/sect-security-enhanced_linux-working_with_selinux-selinux_contexts_labeling_files)

### QUESTION 35

A new corporate policy states that Bluetooth should be disabled on all company laptops. Which of the following commands would disable the use of Bluetooth?

- A. `echo "blacklist bluetooth" > /etc/modprobe.d/blacklist-bluetooth`
- B. `echo "kill bluetooth" > /etc/modprobe.d/kill-bluetooth`
- C. `echo "modprobe bluetooth" > /etc/modprobe.d/modporbe-bluetooth`
- D. `echo "rmmod bluetooth" > /etc/modprobe.d/rmmod-bluetooth`

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

### QUESTION 36

A junior Linux administrator is installing a new application with CPU architecture requirements that have the following specifications:

- x64 bit
- 3.0GHz speed
- Minimum quad core

The administrator wants to leverage existing equipment but is unsure whether the requirements of these systems are adequate. The administrator issues the following command `cat /proc/cpuinfo`. The output of the command is as follows:

```
processor:      0
vendor_id:     GenuineIntel
cpu_family:    x64
model:         58
model name:    Intel (R) Core(TM) i7-3687U @2.10 GHz
stepping:      9
microcode:     0x1c
cpu MHz:       2593.8%
cache size:    4096KB
siblings:      1
core id:       0
cpu cores:     4
```

Which of the following is the recommended course of action the administrator should take based on this output?

- A. Install the application, as the system meets the application requirements B. Procure new equipment that matches the recommended specifications
- C. Recompile the Linux kernel to support the installation.
- D. Reconfigure `lib` modules to support the new application.

**Correct Answer: A**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 37** A Linux systems administrator wants the ability to access systems remotely over SSH using RSA authentication. To which of the following files should the RSA token be added to allow this access?

- A. authorized\_keys
- B. ~/.ssh/ssh\_config
- C. id\_rsa.pub
- D. known\_hosts

**Correct Answer: C**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.digitalocean.com/community/tutorials/how-to-configure-ssh-key-based-authentication-on-a-linux-server>

**QUESTION 38**

A Linux server needs to be accessed, but the root password is not available.

Which of the following would BEST allow an administrator to regain access and set a new known password at the same time?

- A. Boot into single-user mode and reset the password via the `passwd` command.
- B. Boot into single-user mode and reset the password by editing the `/etc/passwd` file.
- C. Boot into single-user mode and reset the password by editing the `/etc/shadow` file.
- D. Boot into single-user mode and reset the password via the `chage` command.

**Correct Answer: A**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://phoenixnap.com/kb/how-to-change-root-password-linux>

**QUESTION 39** A Linux administrator wants to fetch a Git repository from a remote Git server.

Which of the following is the BEST command to perform this task?

- A. `git checkout`
- B. `git clone`
- C. `git merge`
- D. `git config`

**Correct Answer: B**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://git-scm.com/book/en/v2/Git-Basics-Working-with-Remotes>

**QUESTION 40**

An administrator needs to create a shared directory in which all users are able to read, write, and execute its content but none of the regular users are able to delete any content.

Which of the following permissions should be applied to this shared directory?

- A. rwxrwxrwt
- B. rwxrwxrws
- C. rwxrwxrwx
- D. rwxrwxrw\*

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 41** A systems administrator has finished building a new feature for the monitoring software in a separate Git branch.

Which of the following is the BEST method for adding the new feature to the software's master branch?

- A. Merge the changes from the feature branch to the master branch.
- B. Save the changes to the master branch automatically with each Git commit.
- C. Clone the feature branch into the master branch.
- D. Pull the changes from the feature branch into the master branch.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://git-scm.com/book/en/v2/Git-Branching-Basic-Branching-and-Merging>

**QUESTION 42** Which of the following will provide a list of all flash, external, internal, and SSD drives?

- A. lspci
- B. lsmod
- C. lsblk
- D. lsusb

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.linux.com/learn/intro-to-linux/2017/3/how-format-storage-devices-linux>

**QUESTION 43** Which of the following configuration management tools is considered agentless?

- A. Puppet
- B. Salt
- C. Ansible
- D. Chef

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.intigua.com/blog/puppet-vs.-chef-vs.-ansible-vs.-saltstack>

**QUESTION 44**

An administrator reviews the following configuration file provided by a DevOps engineer:

```
Tasks:
- name:Install php-fpm from repo
  yum:
    name: php-fpm
    state: present
- name:Install mysql from repo
  yum:
    name: mysql-server
    state: present
```

Which of the following would the application parsing this file MOST likely have to support?

- A. YAML
- B. AJAX
- C. JSON
- D. SOAP

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 45** Which of the following is a difference between YAML and JSON?

- A. Users can comment in YAML but not in JSON
- B. JSON only uses curly brackets, while YAML only uses square brackets
- C. JSON is used in web development, while YAML is used solely in back-end systems.
- D. YAML has been deprecated for JSON.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.json2yaml.com/yaml-vs-json>

**QUESTION 46**

A junior administrator of a physical server receives log messages indicating the out-of-memory killer has been active. All memory slots are in use on the motherboard, but additional disk space is available. Space has been allocated for a swap file.

Which of the following should the administrator use to reduce the output of memory messages?

- A. free : swapoff / swapfile ; swapon -a
- B. mkswap /swapfile; swapon -a
- C. fallocate -l 2G /swapfile && swapon -a
- D. echo "1" > /proc/meminfo ; swapon / swapfile

**Correct Answer: B**

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 47

A junior Linux administrator is optimizing a system in which an application needs to take priority 0 when running the process. The administrator runs the ps command and receives the following output:

```
PID  PPID  TTY    Time    CMD
8481  2     pts/17 16:40:00 app
9854  0     pts/17 16:40:00 ps
```

Given this scenario, which of the following steps will address this issue?

- A. Issue the command `renice -n 0 -p 8481`
- B. Issue the command `renice -p 8481`
- C. Issue the command `renice -p 0 -n 8481`
- D. Issue the command `renice -n 8481`

Correct Answer: A

Section: (none)

Explanation

Explanation/Reference:

#### QUESTION 48

An administrator needs to mount the shared NFS file system `testhost:/testvolume` to mount point `/mnt/testvol` and make the mount persistent after reboot.

Which of the following BEST demonstrates the commands necessary to accomplish this task? A.

```
# mkdir -p /mnt/testvol
# echo "testhost:/testvolume /mnt/testvol nfs defaults 0 0" >> /etc/fstab
# mount -a

# mkdir /mnt/testvol
# mount testhost:/testvolume /mnt/testvol

# mkdir testhost:/testvolume at /mnt/testvol
# mount -a

# mkdir /mnt/testvol
# echo "testhost:/testvolume /mnt/testvol" >> /mnt/mnttab
# mount -a
```

B.

C.

D.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 49

A systems administrator has deployed a Linux server based on an Anaconda process with all packages and custom configurations necessary to install a web server role.

Which of the following could be used to install more Linux servers with the same characteristics?

- A. `/etc/sysconfig/anaconda.cfg`
- B. `/root/anaconda.auto`
- C. `/root/anaconda-ks.cfg`
- D. `/etc/sysconfig/installation.cfg`

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html/installation\\_guide/sn-automating-installation](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/installation_guide/sn-automating-installation)

#### QUESTION 50

A Linux administrator is using a Linux system as a router. During the tests, the administrator discovers that IP packets are not being sent between the configured interfaces.

Which of the following commands enables this feature for IPv4 networks?

- A. `cat /proc/sys/net/ipv4/ip_route > 1`
- B. `echo "1" > /proc/sys/net/ipv4/ip_forward`
- C. `echo "1" > /proc/sys/net/ipv4/ip_route`
- D. `echo "1" > /proc/sys/net/ipv4/ip_net`

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 51

A systems administrator wants to know the current status of a series of `dd` jobs that were started in the background three hours ago.

Which of the following commands will achieve this task?

- A. `sudo killall -HUP dd`
- B. `sudo killall dd`
- C. `sudo killall -TERM dd`
- D. `sudo killall -USR1 dd`

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://askubuntu.com/questions/215505/how-do-you-monitor-the-progress-of-dd>

**QUESTION 52** A Linux administrator needs the “tech” account to have the option to run elevated commands as root.

Which of the following commands would BEST meet this goal?

- A. \$ su - tech -c “/bin/bash”
- B. # usermod -aG wheel tech
- C. # sudo -i tech
- D. # groupadd -u tech -g root

**Correct Answer: B**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 53** Which of the following is the purpose of the vmlinuz file on a Linux system?

- A. To prevent a Linux kernel panic
- B. To start a Linux virtual machine
- C. To provide the executable kernel for the system
- D. To enable resource access to the network

**Correct Answer: C**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://en.wikipedia.org/wiki/Vmlinuz>

**QUESTION 54**

Ann, a junior systems administrator, is required to add a line to the `/etc/yum.conf` file. However, she receives the following error message when she tries to add the line:

```
root@comptia:~# echo "line" > /etc/yum.conf
-su: /etc/yum.conf: Operation not permitted
```

Ann performs some diagnostics to attempt to find the root cause:

```
root@comptia:~# ls -l /etc/yum.conf
-rw-r--r-- 1 root root 970 Jan 30 2018 /etc/yum.conf
```

```
root@comptia:~# lsattr /etc/yum.conf
----i-----e-- /etc/yum.conf
```

```
root@comptia:~# df -i /etc/yum/conf
Filesystem  Inodes  IUsed  IFree  IUse%  Mounted on
/dev/sda1  524288  192861  331427  37%    /
```

VCEUp

Which of the following commands should Ann execute to write content to `/etc/yum?`

- A. `chmod 755 /etc/yum.conf`
- B. `setfacl -m m:rw /etc/yum.conf`
- C. `chattr -i /etc/yum.conf`
- D. `setenforce 0`

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 55** A Linux administrator needs to take stock of USB devices attached to the system.

Which of the following commands would be BEST to complete this task?

- A. `lspci`
- B. `lsusb`
- C. `cat /proc/USB`
- D. `modprobe --usb`

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://linuxhint.com/list-usb-devices-linux/>

**QUESTION 56**

Given the output below:

```
drwxr-xr-x. 4096 user1 user1 Documents
drwxr-xr-x. 4096 user1 user1 Music
lrwxrwxrwx. 1 root root MyPhoto.jpg ->/Pictures/photo.jpg
drwxr-xr-x. 4096 user1 user1 Pictures
-rw-r--r--. 256 user1 user1 text.txt
-rw-r--r--. 35 user1 user1 tmp.tmp
```

Which of the following commands can be used to remove `MyPhoto.jpg` from the current directory?

- A. `unlink ./MyPhoto.jpg`
- B. `del Pictures/photo.jpg`
- C. `rm -rf ./Pictures`
- D. `rm -f MyPhoto.jpg`
- E. `ln -rm ./Pictures/photo.jpg`

**Correct Answer: E**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 57** Which of the following server roles would assign a host IP address?

- A. DHCP
- B. NTP
- C. DNS
- D. SSH

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 58** Which of the following commands would show the default printer on a Linux system?

- A. lpr
- B. lpq
- C. lpstat
- D. lspci

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://superuser.com/questions/123576/show-default-linux-printer>

**QUESTION 59**

A systems administrator has set up third-party log aggregation agents across several cloud instances. The systems administrator wants to create a dashboard of failed SSH attempts and the usernames used.

Which of the following files should be watched by the agents?

- A. /var/log/audit/audit.log
- B. /var/log/kern.log C. /var/log/monitor
- D. /etc/rsyslog.conf

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 60**

A systems administrator must clean up all application files in the directory /var/log/app. However, the company's security policy requires the files to be kept on the backup server for one year. The Linux server has only the tar and bzip2 packages installed.

Which of the following commands will package and compress the files?

- A. tar -zcvf applicationfiles.tar.bz2 /var/log/app/\*
- B. tar -jcvf applicationfiles.tar.bz2 /var/log/app/\*
- C. tar -cvf applicationfiles.tar.bz2 /var/log/app/\*
- D. tar -xvf applicationfiles.tar.bz2 /var/log/app/\*

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### QUESTION 61

In order to comply with new security policies, an administrator needs to prevent the SSH server from using insecure algorithms.

Which of the following files should be edited to accomplish this?

- A. /etc/ssh/sshd\_config
- B. /etc/ssh/ssh\_config
- C. ~/.ssh/ssh\_config
- D. /etc/ssh/known\_hosts

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 62** Which of the following configuration files should be modified to disable Ctrl+Alt+Del in Linux?

- A. /etc/inittab
- B. ~/.bash\_profile
- C. /etc/securetty
- D. /etc/security/limits.conf

**Correct Answer:** A  
**Section:** (none)  
**Explanation**  
**Explanation/Reference:**

Reference: <https://www.linuxtechi.com/disable-reboot-using-ctrl-alt-del-keys/>

**QUESTION 63** Joe, a user, is unable to log in to the server and contracts the systems administrator to look into the issue. The administrator examines the /etc/passwd file and discovers the following entry:

```
joe:x:505:505:~/home/joe:/bin/false
```

Which of the following commands should the administrator execute to resolve the problem?

- A. usermod -s /bin/bash joe
- B. passwd -u joe
- C. useradd -s /bin/bash joe
- D. chage -E -1 joe

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 64**

A server is almost out of free memory and is becoming unresponsive. Which of the following sets of commands will BEST mitigate the issue?

- A. free, fack, partprobe
- B. lsof, lvcreate, mdadm
- C. df, du, rmmmod
- D. fdisk, mkswap, swapon -a

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 65**

A Linux administrator is using a public cloud provider to host servers for a company's website. Using the provider's tools, the administrator wrote a JSON file to define how to deploy the servers. Which of the following techniques did the administrator use?

- A. Infrastructure as code
- B. Build automation
- C. Platform as a service
- D. Automated configuration

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://cloud.google.com/cloud-build/docs/build-config>

**QUESTION 66**

A Linux system is running normally when the systems administrator receives an alert that one application spawned many processes. The application is consuming a lot of memory, and it will soon cause the machine to become unresponsive. Which of the following commands will stop each application process?

- A. kill `pidof application`
- B. killall application
- C. kill -9 `ps -aux | grep application`
- D. pkill -9 application

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.tecmint.com/how-to-kill-a-process-in-linux/>

**QUESTION 67** A systems administrator configured a new kernel module, but it stopped working after reboot. Which of the following will allow the systems administrator to check for module problems during server startup?

- A. lsmod
- B. modprobe
- C. modinfo
- D. dmesg

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html/deployment\\_guide/sec-displaying\\_information\\_about\\_a\\_module](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/sec-displaying_information_about_a_module)

**QUESTION 68** A junior Linux administrator is installing patches using YUM. The administrator issues the following command:

```
yum list installed
```

The output of the command is as follows:

```
Loaded plugins: fastmirror, langpacks
Existing lock /var/run/yum.pid: another copy is running as pid 5180.
Another app is currently holding the yum lock; waiting for it to exit...
The other application is yum
Memory: 26 M RSS (r415 MB VSZ)
Started: Fri Jun 15 08:05:15 2018 - 2:18:48 ago
State: Traced/Stopped pid: 5180
```

Given this scenario and the output, which of the following should the administrator do to address this issue?

- A. `renice -n 9 -p 5180`
- B. `killall yum`
- C. `ps -ef | grep yum`
- D. `top | grep yum`

**Correct Answer: C**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.thegeekdiary.com/yum-command-fails-with-another-app-is-currently-holding-the-yum-lock-in-centos-rhel-7/>

**QUESTION 69**

A systems administrator needs to retrieve specific fields from a CSV file. Which of the following tools would accomplish this task?

- A. `awk`
- B. `sort`
- C. `print`
- D. `echo`

**Correct Answer: A**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://stackoverflow.com/questions/19602181/how-to-extract-one-column-of-a-csv-file>

**QUESTION 70** Two specific users need access to a directory owned by root where backups are located. Which of the following commands would BEST ensure the specified users can access the backup files?

- A. `umask`
- B. `chcon`
- C. `chmod`
- D. `setfacl`

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 71** Which of the following is the purpose of the monitoring server role?

- A. To aggregate web traffic to watch which websites employees are visiting
- B. To collect status and performance information about the servers in an environment
- C. To provide user authentication services to a network
- D. To provide real-time analysis of potential threats to the organization

**Correct Answer:** B  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 72** A junior administrator is migrating a virtual machine from a Type 1 hypervisor to a Type 2 hypervisor. To ensure portability, which of the following formats should the administrator export from the Type 1 hypervisor to ensure compatibility?

- A. OWASP
- B. VDI
- C. VMDK
- D. OVA

**Correct Answer:** D  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

Reference: <https://docs.vmware.com/en/VMware-Fusion/11/com.vmware.fusion.using.doc/GUID-16E390B1-829D-4289-8442-270A474C106A.html>

**QUESTION 73**

A junior systems administrator is upgrading a package that was installed on a Red Hat-based system. The administrator is tasked with the following:

- Update and install the new package.

- Verify the new package version is installed.

Which of the following should be done to BEST accomplish these task? (Choose two.)

- A. `yum install <package name>`
- B. `yum upgrade`
- C. `rpm -e <package name>`
- D. `rpm -qa`
- E. `apt-get <package name>`
- F. `apt-get upgrade`

**Correct Answer:** AD  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

Reference: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/6/html/deployment\\_guide/ch-yum](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/ch-yum)

**QUESTION 74** Which of the following is the template for the grub.cfg file?

- A. /etc/default/grub
- B. /etc/grub2.cfg
- C. /etc/sysctl.conf
- D. /boot/efi

**Correct Answer: A**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://geek-university.com/linux/grub-version-2/>

**QUESTION 75**

A Linux administrator implemented a new HTTP server using the default configuration. None of the users on the network can access the server. If there is no problem on the network or with the users' workstations, which of the following steps will BEST analyze and resolve the issue?

- A. Run `netstat` to ensure the port is correctly bound, and configure the firewall to allow access on ports 80 and 443
- B. Run `route` to ensure the port is correctly bound, and configure the firewall to allow access on ports 80 and 443
- C. Run `netcat` to ensure the port is correctly bound, and configure a static route to the web to allow access on ports 80 and 443
- D. Run `route` to ensure the port is correctly bound, and configure SELinux to allow access on ports 80 and 443

**Correct Answer: C**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.varonis.com/blog/netcat-commands/>

**QUESTION 76**

A Linux storage administrator wants to create a logical volume group. Which of the following commands is required to start the process?

- A. `pvcreate`
- B. `vgcreate`
- C. `lvcreate`
- D. `mkfs.xfs`

**Correct Answer: B**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.thegeekstuff.com/2010/08/how-to-create-lvm/>

**QUESTION 77**

A Linux administrator built a GitLab server. Later that day, a software engineer tried to access the server to upload the repository during the final step of installation. The software engineer could not access the website. Which of the following firewall rules would allow access to this site?

- A. `iptables -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack -cstate NEW, ESTABLISHED -j ACCEPT`
- B. `iptables -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack -cstate ESTABLISHED -j ACCEPT`
- C. `iptables -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack -cstate RELATED, ESTABLISHED -j ACCEPT`
- D. `iptables -A INPUT -p tcp -m multiport --dports 80,443 -m conntrack -cstate NEW, ESTABLISHED -j REJECT`

**Correct Answer: C**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://serverfault.com/questions/578730/when-using-iptables-firewall-rules-why-assert-new-state-on-all-allowed-ports>

**QUESTION 78**

While creating a file on a volume, the Linux administrator receives the following message: No space left on device. Running the `df -m` command, the administrator notes there is still 50% of usage left. Which of the following is the NEXT step the administrator should take to analyze the issue without losing data?

- A. Run the `df -i` command and notice the inode exhaustion
- B. Run the `df -h` command and notice the space exhaustion
- C. Run the `df -B` command and notice the block size
- D. Run the `df -k` command and notice the storage exhaustion

**Correct Answer: A**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.tecmint.com/how-to-check-disk-space-in-linux/>

**QUESTION 79** A user attempts to use the `mount -a` command but gets the following error:

```
mount: mount point /mnt/test does not exist
```

Which of the following commands best describes the action the Linux administrator should take NEXT?

- A. `mount -a /mnt/test`
- B. `mkdir -p /mnt/test`
- C. `mdadm -p /mnt/test`
- D. `mkfs /mnt/test`
- E. `touch /mnt/test`

**Correct Answer: B**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://serverfault.com/questions/751113/mount-point-does-not-exist-despite-creating-it>

**QUESTION 80**

Which of the following is modified to reconfigure the boot environment?

- A. `grub-mkconfig`
- B. `grub.cfg`
- C. `update-grub`
- D. `grub2-mkconfig`

**Correct Answer: B**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 81** A company wants to ensure that all newly created files can be modified only by their owners and that all new directory content can be changed only by the creator of the directory. Which of the following commands will help achieve this task?

- A. `umask 0022`
- B. `umask 0012`
- C. `chmod -R 0644 /`
- D. `chmod -R 0755 /`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.computerhope.com/unix/uumask.htm>

**QUESTION 82**

A Linux administrator needs to back up the folder `/usr/domain`, and the output must be a gzip compressed tar. Which of the following commands should be used?

- A. `tar -cv domain.tar.gz /usr/domain`
- B. `tar -cvf /usr/domain domain.tar.gz`
- C. `tar -czvf domain.tar.gz /usr/domain`
- D. `tar -cxzv /usr/domain domain.tar.gz`

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://help.ubuntu.com/community/BackupYourSystem/TAR>

**QUESTION 83** A Linux administrator needs every new file created on a directory to maintain the group permissions of the same directory. Which of the following commands would satisfy this requirement?

- A. `chmod o+s <directory>`
- B. `chmod u+s <directory>` C. `chmod +s <directory>`
- D. `chmod g+s <directory>`

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://unix.stackexchange.com/questions/115631/getting-new-files-to-inherit-group-permissions-on-linux>

**QUESTION 84**

Which of the following statements BEST represents what the term “agentless” means regarding orchestration?

- A. Installation of a tool is not required on the remote system to perform orchestration tasks
- B. It facilitates version control when using infrastructure as code during orchestration
- C. It automatically removes malware from the remote system during orchestration
- D. A tool can only be accessed remotely to perform orchestration tasks

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://whatistechtarget.com/definition/agentless>

**QUESTION 85** Given that a company's policy states that users cannot install third-party tools on Windows servers, which of the following protocols will allow a Linux GUI to connect to a Windows server?

- A. VNC
- B. NX
- C. RDP
- D. X11

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://phoenixnap.com/kb/ssh-to-connect-to-remote-server-linux-or-windows>

**QUESTION 86**

Ann, a junior Linux administrator, needs to copy software from her local machine to assist in developing a software application on a remote machine with the IP address 192.168.3.22. The file needs to be placed on the `/tmp` directory. After downloading the RPM to the local machine, which of the following commands would be BEST to use to copy the software?

- A. `scp ~/software.rpm USER@192.168.3.22:/tmp`
- B. `scp ~/software.rpm USER@192.168.3.22: /tmp`
- C. `wget USER@192.168.3.22:/tmp -f ~/software.rpm`
- D. `scp USER@192.168.3.22 ~/software.rpm :/tmp`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

VCEUp

**QUESTION 87**

An administrator is tasked with increasing the size of the volume `/dev/vg/lv` to 20GB. Which of the following BEST illustrates the steps the administrator should take?

- A. `vgextend -L20G /dev/vg/lv; resizelv /dev/vg/lv`
- B. `parted -L20G /dev/vg/lv; remount /dev/vg/lv`
- C. `mkfs -L20G /dev/vg/lv; tune2fs /dev/vg/lv`
- D. `lvextend -L20G /dev/vg/lv; resize2fs /dev/vg/lv`

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 88** A systems administrator observes high latency values when reaching a remote web server. Which of the following commands will help determine and isolate issues on the network side?

- A. `mtr`
- B. `dig`
- C. `netstat`
- D. `route`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.keycdn.com/support/what-is-latency>

**QUESTION 89**

A Linux administrator wants to obtain a list of files and subdirectories in the `/etc` directory that contain the word “services”. Once the files and subdirectories are discovered, they should be listed alphabetically in the `/var/tmp/foundservices` file. Which of the following shell scripts will accomplish this task?

A. `#!/bin/bash find /etc -name services | sort > /var/tmp/foundservices`  
B. `#!/bin/bash locate /etc -sort -name services > /var/tmp/foundservices`  
C. `#!/bin/bash find -name services -sort </var/tmp/foundservices`  
D. `#!/bin/bash find /etc -name services -sort > /var/tmp/foundservices`

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 90**

A systems administrator is enabling quotas on the `/home` directory of a Linux server. The administrator makes the appropriate edits to the `/etc/fstab` file and attempts to issue the commands to enable quotas on the desired directory. However, the administrator receives an error message stating the filesystem does not support quotas. Which of the following commands should the administrator perform to proceed?

A. `mount -o remount /home`  
B. `quotacheck -cg`  
C. `edquota /home`  
D. `quotaon /home`

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.tecmint.com/set-filesystem-disk-quotas-on-ubuntu/>

**QUESTION 91**

A systems administrator needs to install a new piece of hardware that requires a new driver. The driver should be manually installed. Which of the following describes the order of commands required to obtain module information, install the module, and check the log for any errors during module installation?

A. `lsmod, modprobe, modinfo`  
B. `modinfo, insmod, modprobe`  
C. `modinfo, insmod, dmesg`  
D. `lsmod, insmod, dmesg`

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 92** A new HTTPS web service is being deployed on a server. Which of the following commands should the Linux administrator use to ensure traffic is able to flow through the system firewall to the new service?

A. `iptables -I OUTPUT -p tcp --sport 443 -j ACCEPT`  
B. `iptables -A INPUT -p tcp --dport 443 -j ACCEPT`

- C. iptables -I INPUT --dport 443 -j ACCEPT  
 D. iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.linode.com/docs/security/firewalls/control-network-traffic-with-iptables/>

**QUESTION 93** An administrator has modified the configuration file for a service. The service is still running but is not using the new configured values. Which of the following will BEST remediate this issue?

- A. kill -HUP  
 B. init 0  
 C. service start  
 D. renice -10

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 94**

An administrator needs to see a list of the system user's encrypted passwords. Which of the following Linux files does the administrator need to read?

- A. /etc/shadow  
 B. /etc/skel  
 C. /etc/passwd  
 D. /etc/pw

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 95**

A Linux administrator is setting up a testing environment and needs to connect to a separate testing server using the production server name. The administrator needs to override the hostname that the DNS is returning in order to use the test environment. Which of the following commands should be run on each of the testing systems to BEST meet this goal?

- A. # hostnamectl set-hostname "192.168.1.100 production.company.com"  
 B. # grep -i IP "\${ip addr show} production.company.com" > /etc/resolv.conf  
 C. # ip addr add 192.168.1.100/24 dev eth0 && rndc reload production.company.com D. # echo "192.168.1.100 production.company.com" >> /etc/hosts

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/networking\\_guide/sec\\_configuring\\_host\\_names\\_using\\_hostnamectl](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/networking_guide/sec_configuring_host_names_using_hostnamectl)

**QUESTION 96**

A Linux administrator opens a ticket to have an external hard drive mounted. As a security policy, external storage kernel modules are disabled.

Which of the following is the BEST command for adding the proper kernel module to enable external storage modules?

- A. `rmmod /lib/modules/3.6.12-100-generic/kernel/drivers/usb/storage/usb-storage.ko`
- B. `modinfo /lib/modules/3.6.12-100-generic/kernel/drivers/usb/storage/usb-storage.ko`
- C. `depmod /lib/modules/3.6.12-100-generic/kernel/drivers/usb/storage/usb-storage.ko`
- D. `insmod /lib/modules/3.6.12-100-generic/kernel/drivers/usb/storage/usb-storage.ko`

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cyberciti.biz/faq/linux-how-to-load-a-kernel-module-automatically-at-boot-time/>

**QUESTION 97** Which of the following are Linux desktop managers? (Choose two.)

- A. KDE
- B. GNOME
- C. GUI
- D. VNC
- E. X11
- F. SPICE

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 98**

A systems administrator is configuring options on a newly installed Linux VM that will be deployed to the Pacific time zone. Which of the following sets of commands should the administrator execute to accurately configure the correct time settings?

- A. `cd /etc ln -s /usr/share/zoneinfo/US/Pacific localtime`
  - B. `cd /usr/local ln -s /usr/share/zoneinfo/US/Pacific zoneinfo`
  - C. `cd /etc/local ln -s /usr/share/zoneinfo/US/Pacific localtime`
  - D. `cd /usr/share/local ln -s /usr/share/zoneinfo/US/Pacific localectl`
- Correct**

**Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 99** A user has connected a Bluetooth mouse to a computer, but it is not working properly. Which of the following commands should the systems administrator use to fix the issue?

- A. `lsmod -i bluetooth`
- B. `insmod bluetooth`
- C. `modprobe -r bluetooth`
- D. `depmod -i bluetooth`

**Correct Answer:** C  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### QUESTION 100

An administrator notices that a long-running script, `/home/user/script.sh`, is taking up a large number of system resources. The administrator does not know the script's function. Which of the following commands should the administrator use to minimize the script's impact on system resources?

- A. `renice`
- B. `kill`
- C. `bg`
- D. `nohup`

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

**QUESTION 101** An administrator needs to deploy 100 identical CentOS workstations via PXE boot. Which of the following should the administrator use to minimize the amount of interaction with the consoles needed?

- A. Kickstart script
- B. Ghost image on a distribution server
- C. Hard disk duplicator
- D. Hard disk duplicator
- E. Ubiquity script

**Correct Answer:** A  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

#### QUESTION 102

A user, `jsmith`, needs access to database files located on a server. Which of the following will add `jsmith` to the "dba" group and preserve existing group memberships?

- A. `usermod -a -G dba jsmith`
- B. `usermod -g dba jsmith`
- C. `useradd -g dba jsmith`
- D. `groupmod dba -u jsmith`

**Correct Answer:** AC  
**Section:** (none)  
**Explanation**

**Explanation/Reference:**

Explanation:

According to the reference given below. Both AC is correct. Reference:

<https://www.cyberciti.biz/faq/howto-linux-add-user-to-group/>

#### QUESTION 103

A Linux administrator installed a new network adapter and temporarily disabled the network service from starting on boot. The partial output of `chkconfig` is as follows:

```
network 0:off 1:off 2:off 3:off 4:off 5:off 6:off
```

Which of the following commands BEST describes how the administrator should re-enable the network service?

- A. `chkconfig --level 0 network on`
- B. `chkconfig --level 0-6 network on`
- C. `chkconfig --level 6 network on`
- D. `chkconfig --level 12 network on`
- E. `chkconfig --level 345 network on`

**Correct Answer:** E

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.thegeekdiary.com/how-to-enable-or-disable-service-on-boot-with-chkconfig/>

#### QUESTION 104

An engineer is working on a production application deployment that requires changing a web application property file called `server.property` that is managed by the Git version control system. A cloned copy of the remote repository in which the `server.property` file exists is on the local desktop computer. The engineer makes appropriate changes to the files, saves it as `server.property`, and executes `git commit -m "changed the property file" server.property`. Which of the following commands did the engineer fail to perform?

- A. `git init server.property`
- B. `git merge server.property`
- C. `git add server.property`
- D. `git push server.property`

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.earthdatascience.org/workshops/intro-version-control-git/basic-git-commands/>

#### QUESTION 105

A Linux administrator retrieved a repository of files from a Git server using `git clone`. The administrator wants to see if a configuration file was added to the repository. Which of the following Git arguments should be used to see the recent modifications?

- A. `fetch`
- B. `log`
- C. `init`
- D. `pull`

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 106

A systems administrator is unable to reach other devices on the network and the Internet. The server is configured with the IP address 192.169.1.50/24 on `eth0`. The server's router is 192.168.1.1. The administrator reviews the output of `route -n`:

## Kernel IP routing table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.2.1	0.0.0.0	UG	1024	0	0	eth0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

Which of the following commands should the administrator run to correct the issue?

- A. route del default gw 192.168.2.1 eth0; route add default gw 192.168.1.1 eth0
- B. route add -net 192.168.10.0 netmask 255.255.255.0 gw 192.168.2.1 eth0
- C. route add 192.168.1.1 default 192.168.1.50 eth0
- D. route host gw 192.168.1.1 eth0

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 107** A junior Linux administrator needs to access production servers using a secure SSH protocol. Which of the following files should contain the public key to gain remote access to the server?

- A. ~/ssh/authorized-keys
- B. /etc/authorized\_keys
- C. /etc/sshd/ssh.conf
- D. ~/.ssh/authorized\_keys

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.linode.com/docs/security/securing-your-server/>

**QUESTION 108**

An administrator needs to see the type of CPU that a server is running. Which of the following files contains this information?

- A. /proc/cpuinfo
- B. /etc/devices/info.conf
- C. /dev/proc/cpu
- D. /sys/dev/cpuinfo

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.binarytides.com/linux-cpu-information/>

**QUESTION 109**

A junior systems administrator is creating a cron job. The cron job requirements are as follows:

- Run the `hello.sh` script every hour (24 times in one day).
- Run it on Monday only.

Given this scenario, which of the following crontab options should be configured to meet these requirements?

- A. 0 \*\*\* 1 hello.sh
- B. 0 24 \*\* Monday hello.sh
- C. 24 \*\*\* Monday hello.sh
- D. 1 \*\*\* 0 hello.sh

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 110

A Linux systems administrator is setting up SSH access with PKI for several using their newly created RSA keys. Which of the following MOST securely achieves this task?

- A. Use `curl` to copy each user's public key file to the respective system
- B. Use `cp` to copy each user's public key file to the respective system
- C. Use `ssh-copy-id` to copy each user's public key file to the respective system
- D. Use `ssh-copy-id` to copy each user's private key file to the respective system

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.linode.com/docs/security/authentication/use-public-key-authentication-with-ssh/>

#### QUESTION 111

The development team has automated their software build process so each time a change is submitted to the source code repository, a new software build is compiled. They are requesting that the Linux operations team look into automating the deployment of the software build into the test environment. Which of the following is the benefit to the development team for implementing deployment automation?

- A. To ensure the build commits are also deployed to the test environment
- B. To enable notifications when builds are deployed to the test environment
- C. To ensure software builds in test are not accidentally deployed to production
- D. To streamline the deployment process for deploying builds into test environments

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 112

A Linux administrator needs to schedule a cron job to run at 1:15 p.m. every Friday to report the amount of free disk space on the system and to send the output to a file named "freespace". Which of the following would meet this requirement?

- A. 13 15 \* \* 5 df > /freespace
- B. 15 13 \* \* 5 df > /freespace
- C. 15 1 \* \* 6 df > /freespace
- D. 15 13 6 \* \* df > /freespace

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 113**

A technician wants to secure a sensitive workstation by ensuring network traffic is kept within the local subnet. To accomplish this task, the technician executes the following command:

```
echo 0 > /proc/sys/net/ipv4/ip_default_ttl
```

Which of the following commands can the technician use to confirm the expected results? (Choose two.)

- A. tcpdump
- B. traceroute
- C. route
- D. iperf
- E. ip
- F. arp

**Correct Answer:** BC

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 114**

A junior Linux administrator needs to ensure a service will start on system boot. Which of the following commands should be used to accomplish this task?

- A. chkconfig <service> on
- B. systemctl <service> bootup
- C. service <service> enable
- D. crontab install <service>

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://geekflare.com/how-to-auto-start-services-on-boot-in-linux/>

**QUESTION 115**

SIMULATION

Find the file named *core* and remove it from the system.

**INSTRUCTIONS**

Type "help" to display a list of available commands.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

Linux Shell

```
[comptia@localhost ~]$
```

**Correct Answer:** See explanation below.

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Explanation:

```
root@tryit-sought:~# find . -type f -name "FILE-TO-FIND" -exec rm -f {} \;  
root@tryit-sought:~# find . -type f -core "FILE-TO-FIND" -exec rm -f {} \;
```

Reference: <https://www.cyberciti.biz/faq/linux-unix-how-to-find-and-remove-files/>

**QUESTION 116 DRAG**

**DROP**

As a Systems Administrator, to reduce disk space, you were tasked to create a shell script that does the following:

Add relevant content to /tmp/script.sh, so that it finds and compresses rotated files in /var/log without recursion.

**INSTRUCTIONS**

Fill the blanks to build a script that performs the actual compression of rotated log files.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

**Select and Place:**

**Snippets**

tar	until	zip
egrep	awk	\$log
"\$6"	pgrep	repeat
/tmp/tempfile	locate	filename
rar	then	"log.[1-6]\$"
in	done	/var/log
for	xz	"\$1"
sed	gzip	"\$log.[1-6]\$"
while		

```
#!/bin/bash
#name: script.sh
find /var/log -type f -maxdepth 1 | grep [?] > /tmp/tempfile
[?] filename [?] $(cat [?])
do
[?] $filename
[?]
```

Correct Answer:

**Snippets**

tar	until	zip
egrep	awk	\$log
"\$6"	pgrep	repeat
/tmp/tempfile	locate	filename
rar	then	"log.[1-6]\$"
in	done	/var/log
for	xz	"\$1"
sed	gzip	"\$log.[1-6]\$"
while		

```
#!/bin/bash
#name: script.sh
find /var/log -type f -maxdepth 1 | grep "$1" > /tmp/tempfile
for filename in $(cat /tmp/tempfile)
do
gzip $filename
done
```

Section: (none)  
 Explanation  
 Explanation/Reference:

**QUESTION 117 HOTSPOT**

After installing a new web server, you are unable to browse to the default web page.

**INSTRUCTIONS**

Review all the command output and select the command needed to remediate the issue.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

Hot Area:

Commands	Answer
<pre>[root@webserver log]# getenforce [root@webserver log]# getsebool -a   grep httpd [root@webserver log]# netstat -antp [root@webserver log]# ss -antp [root@webserver log]# ps -ef   grep nginx [root@webserver log]# grep avc /var/log/audit/audit.log [root@webserver log]# more /var/log/web/access_log [root@webserver log]# more /var/log/web/error_log [root@webserver log]# ls -la [root@webserver log]# journalctl -u nginx -1 [root@webserver log]# systemctl status webserver [root@webserver log]# sealert</pre>	<pre>[root@webserver log]# systemctl restart nginx setsebool -P httpd_read_user_content =1 restorecon -rv /home/comptia/html kill -HUP 3431 sysctl -w net.ipv4 ip_forward = 1 chown -R comptia: /home/comptia/html/ firewall-cmd --zone=public --service=http --permanent chmod 777 /home/comptia/html/ setfacl -m g:comptia:rwX /home/comptia/html/ cp -R /home/comptia/html /var/www/html</pre>

Output

VCEUp

Correct Answer:

Commands	Answer
<pre>[root@webserver log]# getenforce [root@webserver log]# getsebool -a   grep httpd [root@webserver log]# netstat -antp [root@webserver log]# ss -antp [root@webserver log]# ps -ef   grep nginx [root@webserver log]# grep avc /var/log/audit/audit.log [root@webserver log]# more /var/log/web/access_log [root@webserver log]# more /var/log/web/error_log [root@webserver log]# ls -la [root@webserver log]# journalctl -u nginx -1 [root@webserver log]# systemctl status webserver [root@webserver log]# sealert</pre>	<pre>[root@webserver log]# systemctl restart nginx setsebool -P httpd_read_user_content =1 restorecon -rv /home/comptia/html kill -HUP 3431 sysctl -w net.ipv4 ip_forward = 1 chown -R comptia: /home/comptia/html/ firewall-cmd --zone=public --service=http --permanent chmod 777 /home/comptia/html/ setfacl -m g:comptia:rwX /home/comptia/html/ cp -R /home/comptia/html /var/www/html</pre>
Output	

Section: (none)  
Explanation

Explanation/Reference:

#### QUESTION 118

A Linux administrator has installed a web application firewall in front of a web server running on HTTP port 8080 and successfully started the HTTP server. However, after opening the application URL in an Internet browser, the administrator discovered that the application does not work. The administrator performed the following diagnostic steps:

Output of `sysctl -a` command:

```
kernel.sched_child_runs_first = 0
kernel.panic = 0
kernel.ftrace_enabled = 1
kernel.sysrq = 1
net.ipv4.icmp_echo_ignore_all = 0
```

Output of `iptables -L` command:

```
Chain INPUT (policy ACCEPT)
```

```
target prot opt source destination
ACCEPT tcp -- anywhere anywhere tcp dpt:webcache
```

```
Chain FORWARD (policy ACCEPT)
```

```
target prot opt source destination
ACCEPT tcp -- anywhere anywhere dpt:webcache
```

```
Chain OUTPUT (policy ACCEPT)
```

```
target prot opt source destination
```

Output of `netstat -nltop | grep "8080"`:

```
tcp 0.0.0.0:8080 0.0.0.0* Listen 12801/httpd
```

Which of the following is the NEXT step the administrator should perform to permanently fix the issue at the kernel level?

- A. `sysctl -w net.ipv4.ip_forward=1` then run `sysctl -w /etc/sysctl.conf` to enable the change
- B. Edit `/etc/sysctl.conf` file and add `net.ipv4.ip_forward = 1` then run `sysctl -p /etc/sysctl.conf` to enable the change
- C. Add iptables rule `iptables -A INPUT -m state --state NEW -p tcp --dport 8080 -j` then restart httpd daemon
- D. Add iptables rule `iptables -A FORWARD -m state --state NEW -p tcp --dport 8080 -j ACCEPT` then restart httpd daemon

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 119** A member of the production group issues the following command:

```
echo "Monday through Friday" > /production_docs/days
```

The command fails to execute, so the user obtains the following output:

```
drwxr--r-- root production 0 Jun 16 2018 production
-rw-r--r-- production production 4096 Jun 14 2018 days
```

Which of the following commands should the user execute to BEST fix the issue?

- A. `chmod g+w production` to change the permissions on the `days` file
- B. `chgrp root production_docs/days` to change the group ownership of the `production_docs/days` file
- C. `chmod g+S production` to set the GUID on the `production_docs` directory
- D. `chown production` to change the ownership of the `production_docs` directory

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 120**

A junior systems administrator created a new filesystem `/dev/sda1` with mountpoint `/data` and added it to the `/etc/fstab` for auto-mounting.

When the systems administrator tries to mount the file system, the system refuses. Given the output below:

```
/dev/mapper/VolGroup00-Log-Vol100 / xfs defaults 0 0
/dev/sda1 /data xfs noauto,dev,sync,ro,nosuid 0 0
/dev/mapper/VolGroup00-Log-Vol101 swap swap defaults0 0
/dev/sda2 /mine ext4 auto,suid,sync,rw,dev 0 0
```

Which of the following steps is necessary?

- A. Change the filesystem from `/dev/sda1` to `/dev/sda2` and reboot.
- B. Change the options to `auto,dev,sync,rw,nosuid` and run the `mount -a` command.
- C. Change the mount point to `data` and reboot.
- D. Change the dump column to 1 and run the `mount -a` command.

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 121** A user wants to list the lines of a log, adding a correlative number at the beginning of each line separated by a set of dashes from the actual message. Which of the following scripts will complete this task? A.

```
#!/bin/bash
LOG='/var/log/auth.log'
nrlines=0
while read LINE
do
    nrlines=$((nrlines + 1))
    echo $nrlines --- ${LINE}
done < ${LOG}

#!/bin/bash
LOG='/var/log/auth.log'
nrlines=0
while read LINE
do
    nrlines=$((nrlines + 1))
    echo $nrlines --- ${LINE}
done

#!/bin/bash
LOG='/var/log/auth.log'
nrlines=0
while read LINE
do
    nrlines=$((nrlines + 1))
    echo $nrlines --- ${LINE}
done < ${LOG}

#!/bin/bash
LOG='/var/log/auth.log'
nrlines=0
while read LINE
do
    nrlines=$((nrlines + 1))
    echo $nrlines --- ${LINE}
done < ${LOG}
```

B.

C.

D.

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 122

An analyst is trying to determine which public IP addresses are managed by Company A, but the script is not working correctly.

```
for ip in $(cat ip-list.txt)
do whois $ip | grep "Company A" > /dev/null
    if [ $? -ne 0 ]
        then echo "$ip"
    fi
done
```

Which of the following explains what is wrong with the script?

- A. `$(cat ip-list.txt)` should be changed to ``cat ip-list.txt`` in the `for` statement.
- B. The `for` should be changed to `while` in the loop.
- C. The `>` should be changed to `2>` in the `do` statement.
- D. The `-ne` flag should be changed to `-eq` in the `if` statement.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 123

All users are reporting that they cannot connect to the SFTP server. The administrator runs a scan:

```
starting nmap 4.11 at 2018-06-16 EST
not shown: 1456 closed ports
```

```
PORT      STATE  SERVICE
53/tcp    open   dns
80/tcp    open   http
957/tcp   open   unknown
```

```
MAC Address 08:00:00:00:00:00 ( computer systems )
nmap finished = 1 ip address ( 1 host up ) scanned in 1.497 seconds
You have mail in /var/spool/mail/root
```

Which of the following would allow the administrator to fix the problem?

- A. Allow SFTP connections on port 22 using `/etc/sysconfig/iptables`.
- B. Allow SFTP connections on port 20 and 21 using `/etc/sysconfig/iptables`.
- C. Allow SFTP connections on port 25 using `/etc/sysconfig/iptables`.
- D. Allow SFTP connections on port 1456 using `/etc/sysconfig/iptables`.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 124

A Linux systems administrator installed a new web server, which failed while attempting to start. The administrator suspects that SELinux is causing an issue and wants to temporarily put the system into permissive mode. Which of the following would allow the administrator to accomplish this?

- A. `echo SELINUX=PERMISSIVE >> /etc/sysconfig/selinux`
- B. `setenforce 0`
- C. `sestatus 0`
- D. `chcon httpd_sys_content_t /var/`

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 125** A configuration management tool running every minute is enforcing the service HTTPd to be started. To perform maintenance, which of the following series of commands can be used to prevent the service from being started?

- A. `systemctl stop httpd && systemctl mask httpd`
- B. `systemctl disable httpd && systemctl mask httpd` C. `systemctl stop httpd && systemctl hide httpd`
- D. `systemctl disable httpd && systemctl hide httpd`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 126**

An administrator has written the following Bash script:

```
/home/user/test.sh
```

```
#!/usr/bin/sh
for i in `cat /home/user/iplist.txt`
do
    nslookup $i
done
echo
```

All necessary files exist in the correct locations. However, when the administrator executes `/home/user/test.sh` the following error is received: No

```
such file or directory
```

Which of the following is the MOST likely cause of the error?

- A. The shebang points to the wrong path.
- B. The script is not executable.
- C. The formatting of the file is incorrect.
- D. Nslookup is not installed.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 127**

An administrator is troubleshooting an application that has failed to start after the server was rebooted. Noticing the data volume is not mounted, the administrator attempts to mount it and receives this error:

```
[root@localhost comptia]# mount /dev/datavg/datalv /data
mount: special device /dev/datavg/datalv does not exist
```

Upon checking the logical volume status, the administrator receives this information:

```
[root@localhost comptia]# lvs
LV VG Attr LSize Pool Origin Data% Meta% Move Log Cpy%Sync Convert
root centos -wi-ao---- <6.20g
swap centos -wi-ao---- 820.00m
datalv datavg -wi----- 500.00m
[root@localhost comptia]#
```

Which of the following can be said about the data logical volume, and how can this problem be resolved?

- A. The logical volume is not active. The administrator should make it active with `lvchange -ay /dev/datavg/datalv` and then mount it.
- B. The logical volume file system has become corrupted. The administrator should repair it with `xfs_repair /dev/datavg/datalv` and then mount it.
- C. The logical volume is OK but the `/dev` special files are missing. The administrator should recreate them by running `/dev/MAKEDEV`.
- D. The file system is read-only. The administrator should remount it as read-write with the command `mount -o remount,rw /data`.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 128**

A four-drive Linux NAS has been improperly configured. Each drive has a capacity of 6TB, for a total storage capacity of 24TB. To reconfigure this unit to be not pluggable for drive replacement and provide total storage of 11TB to 12TB, which of the following would be the correct RAID configuration?

- A. RAID 01
- B. RAID 03
- C. RAID 10
- D. RAID 50

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 129**

A systems administrator suspects a process with a PID of 2864 is consuming resources at an alarming rate. The administrator uses the command `renice -n -5 -p2864`, but it does not solve the issue. Which of the following commands should the administrator execute to correct the issue?

- A. `nice -n 5 -p 2864`
- B. `nice -n -5 -p 2864`
- C. `renice -n 10 -p 2864`
- D. `renice -n -10 -p 2864`

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

VCEUp

**QUESTION 130 DRAG**

DROP

You have been asked to parse a log file of logins to determine various information about who is logging in and when.

**INSTRUCTIONS**

Open and inspect the Login log file.

Drag and drop the correct commands onto the output that was generated from that command.

Tokens can be used only once and not all will be used.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

**Select and Place:**

## Command Output

View Login Log

## Commands

```
grep "Mar 13" lastlog
tr "[A-Z]" "[a-z]" < lastlog | grep -i "mar 12"
awk '{ print toupper($0) }' lastlog
tr "[a-z]" "[A-Z]" < lastlog | grep -i "mar 12"
awk '{ print $1 }' lastlog | sort | uniq
awk '{ print $1 }' lastlog | uniq
awk '{ print $2 }' lastlog | sort | uniq
grep lastlog "Mar 13"
grep Mar 13 lastlog
awk '{ print $1 }' lastlog | sort | uniq -c
grep "Mar13" lastlog
grep -i "mar 12" lastlog | sed 's/[a-z]/[A-Z]/g'
```

[comptia@localhost exercise]\$

```
eric pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
david pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
ann pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
chris pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
carl pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
joe pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
lee pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
```

[comptia@localhost exercise]\$

```
COMPTIA PTS/1 :0 Sun Mar 12 14:20 - 09:48 (1+19:28)
CHRIS PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
REBOOT SYSTEM BOOT 3.10.0-693.21.1. Sun Mar 12 11:01 - 13:26 (2+02:24)
LEE PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
COMPTIA PTS/0 :0 Sun Mar 12 14:14 - 14:22 (00:07)
ERIC PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
COMPTIA PTS/0 :0 Sun Mar 12 11:37 - 11:58 (00:20)
REBOOT SYSTEM BOOT 3.10.0-693.21.1. Sun Mar 12 11:02 - 13:26 (2+02:23)
DAVID PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
COMPTIA PTS/0 :0 Sun Mar 12 09:53 - 10:59 (01:05)
COMPTIA :0 :0 Sun Mar 12 11:01 - 11:01 (00:00)
REBOOT SYSTEM BOOT 3.10.0-693.21.1. Sun Mar 12 10:59 - 13:26 (2+02:26)
COMPTIA :0 :0 Sun Mar 12 11:03 - 13:26 (2+02:22)
COMPTIA PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
ANN PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
CARL PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
REBOOT SYSTEM BOOT 3.10.0-693.EL7.X Sun Mar 12 09:39 - 10:59 (01:19)
JOE PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
COMPTIA :0 :0 Sun Mar 12 09:43 - DOWN (01:15)
COMPTIA PTS/0 :0 Sun Mar 12 11:04 - 11:34 (00:30)
```

[comptia@localhost exercise]\$

```
ann
carl
chris
comptia
david
eric
joe
lee
reboot
```

Correct Answer:

Command Output

View Login Log

---

**Commands**

```
awk '{ print toupper($0) }' lastlog
tr "[a-z]" "[A-Z]" < lastlog | grep -i "mar 12"
awk '{ print $1 }' lastlog | sort | uniq

awk '{ print $2 }' lastlog | sort | uniq
grep lastlog "Mar 13"
grep Mar 13 lastlog
awk '{ print $1 }' lastlog | sort | uniq -c
grep "Mar13" lastlog
grep -i "mar 12" lastlog | sed 's/[a-z]/[A-Z]/g'
```

```
[comptia@localhost exercise]$ awk '{ print $1 }' lastlog | uniq
eric pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
david pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
ann pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
chris pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
carl pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
joe pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
lee pts/3 :0 Mon Mar 13 10:52 - 08:48 (1+12:50)
```

```
[comptia@localhost exercise]$ grep "Mar 13" lastlog

COMPTIA PTS/1 :0 Sun Mar 12 14:20 - 09:48 (1+19:28)
CHRIS PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
REBOOT SYSTEM BOOT 3.10.0-693.21.1. Sun Mar 12 11:01 - 13:26 (2+02:24)
LEE PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
COMPTIA PTS/0 :0 Sun Mar 12 14:14 - 14:22 (00:07)
ERIC PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
COMPTIA PTS/0 :0 Sun Mar 12 11:37 - 11:58 (00:20)
REBOOT SYSTEM BOOT 3.10.0-693.21.1. Sun Mar 12 11:02 - 13:26 (2+02:23)
DAVID PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
COMPTIA PTS/0 :0 Sun Mar 12 09:53 - 10:59 (01:05)
COMPTIA :0 :0 Sun Mar 12 11:01 - 11:01 (00:00)
REBOOT SYSTEM BOOT 3.10.0-693.21.1. Sun Mar 12 10:59 - 13:26 (2+02:26)
COMPTIA :0 :0 Sun Mar 12 11:03 - 13:26 (2+02:22)
COMPTIA PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
ANN PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
CARL PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
REBOOT SYSTEM BOOT 3.10.0-693.EL7.X Sun Mar 12 09:39 - 10:59 (01:19)
JOE PTS/2 :0 Sun Mar 12 14:52 - 09:48 (1+18:56)
COMPTIA :0 :0 Sun Mar 12 09:43 - DOWN (01:15)
COMPTIA PTS/0 :0 Sun Mar 12 11:04 - 11:34 (00:30)
```

```
[comptia@localhost exercise]$ tr "[A-Z]" "[a-z]" < lastlog | grep -i "mar 12"
ann
carl
chris
comptia
david
eric
joe
lee
reboot
```

Section: (none)  
 Explanation

Explanation/Reference:

**QUESTION 131**

A systems administrator wants to download a package from a remote server. Which of the following are the BEST commands to use for this task? (Choose two.)

- A. curl
- B. wget

- C. make
- D. tar
- E. zip
- F. nc

**Correct Answer:** BF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.linuxtechi.com/nc-ncat-command-examples-linux-systems/> <https://www.unifiedremote.com/tutorials/how-to-install-unified-remote-server-deb-via-terminal>

**QUESTION 132** An administrator is logged into a server remotely and wants to determine if the system is a VM. Which of the following commands would assist with this?

- A. dmesg
- B. ps
- C. top
- D. vmstat

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://ostechnix.com/check-linux-system-physical-virtual-machine/>

**QUESTION 133**

Ann, a Linux administrator, wants to edit a configuration management file. When she opens the file to edit, her text editor reports that the file has been opened in read-only mode. She then tries to edit the file as root by elevating via sudo and is still unable to save any changes. The error message in her text editor says that the read-only option is set on the file. Ann checks the permissions on the file and sees the following:

```
-rw-rw-r-- 1 root wheel 30 Jun 13 15:38 infrastructure.yml
```

Which of the following commands is the BEST option to allow her to successfully modify the file?

- A. `chmod 600 infrastructure.yml`
- B. `chown root: infrastructure.yml`
- C. `chattr -i infrastructure.yml`
- D. `chmod o+w infrastructure.yml`

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://cets.seas.upenn.edu/answers/chmod.html>

**QUESTION 134**

Joe, a member of the accounting group on a Linux system, is unable to write a file called "taxes" in the accounting shared directory. The ownership and permissions on the directory and file are as follows:

```
accounting drwxrw-r-- user = ann, group = accounting
taxes -rw-r--r-- , user = ann, group = accounting
```

Which of the following commands would allow Joe to write to the file? (Choose two.)

- A. `chmod g+x accounting`
- B. `chmod 777 taxes`

- C. chgrp taxes accounting
- D. chgrp accounting taxes
- E. chmod 774 accounting
- F. chmod u+x accounting

**Correct Answer:** AF

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.pluralsight.com/blog/it-ops/linux-file-permissions>

**QUESTION 135** An administrator needs to generate a list of services that are listening on TCP and/or UDP ports. Which of the following tools should the administrator use?

- A. ethtool
- B. route
- C. netstat
- D. portmap

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.tecmint.com/find-open-ports-in-linux/>

**QUESTION 136**

Ann, a user, has created a new directory and noticed that permissions on the new directory are as follows:

```
drwx-----. 1 ann ann 0 Jun 11 08:20 work
```

Which of the following should the administrator do to restore default permissions for newly created directories?

- A. Change umask value in /etc/profile.
- B. Run chmod command to update permissions.
- C. Modify directory ownership to ann:ann with chown.
- D. Execute chattr command to restore default access.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://geek-university.com/linux/set-the-default-permissions-for-newly-created-files/>

**QUESTION 137**

A Linux engineer is troubleshooting a newly added SCSI device for a Linux server that needed more disk space without rebooting. The engineer discovers that the new device is not visible by the Linux kernel in `fdisk -l` output. Which of the following commands should be used to rescan the entire SCSI bus?

- A. echo "-- --" > /sys/class/scsi\_host/host0/scan
- B. echo ' ' > /sys/class/scsi\_host/host0/scan
- C. echo "-- --" > /sys/scsi/scsi\_host/host0/scan
- D. echo "scan" > /sys/class/scsi\_host/host0/scan

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://geekpeek.net/rescan-scsi-bus-on-linux-system/>

**QUESTION 138**

A systems administrator is troubleshooting an intermittent network connection at the IP address 192.168.1.23. The administrator wishes to monitor the connection at five-minute intervals for one hour. Which of the following commands will accomplish this task?

- A. `ping -i 5 192.168.1.23`
- B. `ping -c 12 192.168.1.23`
- C. `ping -c 12 -i 300 192.168.1.23`
- D. `ping -c 60 -i 100 192.168.1.23`

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://linuxize.com/post/linux-ping-command/>

**QUESTION 139**

A systems administrator wants to mount an ISO to access its content. Using `/mnt` as a mount point, which of the following is the correct syntax?

- A. `mount -o iso9660 /dev/sr0 /mnt`
- B. `mount -o loop -t iso /mnt`
- C. `mount -o loop /tmp/image.iso /mnt`
- D. `mount -o loop /dev/kvm /mnt`

VCEUp

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.cyberciti.biz/tips/how-to-mount-iso-image-under-linux.html>

**QUESTION 140**

An administrator is uncomfortable allowing users to log in as root. Which of the following ensures that root logins are disallowed?

- A. `usermod -L root`
- B. `usermod -G root`
- C. `usermod -B root`
- D. `usermod -U root`

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-en-4/s1-wstation-privileges.html>

**QUESTION 141**

A systems administrator installs a simple package, but the Linux system returns the following error: `rpmdb open fails`. To verify if there is a problem in the RPM database, the systems administrator runs the following command:

```
# yum check
error: db4 error(11) from dbenv->open: Resource temporarily unavailable
error: cannot open Packages index using db4 - Resource temporarily unavailable (11)
error cannot open Packages database in /var/lib/rpm
CRITICAL:yum:main:
Error: rpmdb open fails
```

Which of the following commands should the systems administrator run NEXT to resolve this issue?

- A. cd/var/lib/rpm; rpm --rebuilddb ; rm -f \_db\*; yum clean all
- B. cd/var/lib/rpm; rpm -qd; rpm --rebuilddb; yum clean all
- C. cd/var/lib/rpm; rpm -qa; rm -f \_db\*; yum clean all
- D. cd/var/lib/rpm; rm -f \_db\*; rpm --rebuilddb; yum clean all

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

#### QUESTION 142

Joe, a user, reports that he is no longer able to write files to his home directory. Upon inspection, the Linux administrator discovers that attempting to create a new file gives the following error: No space left on device. However, the disk and partition are not full. Which of the following commands would be BEST for the administrator to use to continue troubleshooting this problem?

- A. rm -Rf ~/.\*
- B. fsck -y /dev/sda1
- C. df -i
- D. fdisk /dev/sda

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.linuxtechi.com/11-df-command-examples-in-linux/>

#### QUESTION 143

A Linux administrator is adding a static IP address to a network interface on a Linux system. The administrator modifies the ifcfg-eth0 configuration file with the following settings:

```
DEVICE:      ETH0
BOOTPROTO:   DHCP
IPADDR:      192.16.20.10
NETMASK:     255.255.255.0
ONBOOT:      No
USERCTL:     No
```

After the administrator restarts the Linux server, the system is not connected to the network. Which of the following configuration settings needs to be changed?

- A. Set BOOTPROTO to BOOTP and USERCTL to yes.
- B. Set BOOTPROTO to NONE and ONBOOT to yes.
- C. Set USERCTL to yes and ONBOOT to no.
- D. Set NETMASK to 255.255.0.0 and ONBOOT to yes.

**Correct Answer: D**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.tecmint.com/set-add-static-ip-address-in-linux/>

**QUESTION 144**

A company wants to provide internal identity verification services for networked devices. Which of the following servers should be installed?

- A. SSH
- B. VPN
- C. CA
- D. DHCP
- E. DNS

**Correct Answer: C**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 145** An administrator notices a directory on a web server named `/var/www/html/old_reports` that should no longer be accessible on the web. Which of the following commands will accomplish this task?

- A. `chmod 000 /var/www/html/old_reports`
- B. `chgrp root /var/www/html/old_reports`
- C. `chown apache /var/www/html/old_reports`
- D. `setenforce apache /var/www/html/old_reports`

**Correct Answer: D**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 146**

A Linux administrator wants to configure log messages of critical or higher severity levels from the cron utility to be logged to the console. Which of the following will accomplish this objective?

- A. Edit the `/etc/logrotate.d/cron` file to include the line `cron.emerg.* /dev/console`
- B. Edit the `/etc/rsyslog.conf` file to include the line `cron.emerg.* /dev/console`
- C. Edit the `/etc/logrotate.conf` file to include the line `cron.emerg.* /dev/console`
- D. Edit the `/etc/rsyslog.d/conf` file to include the line `cron.emerg.* /dev/console`

**Correct Answer: B**

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 147**

A file server is sharing a directory called `/share` between team members inside a company. The fileshare needs to be moved from serverA to `/newshare` located on serverB with all permissions and attributes preserved. Which of the following commands would BEST achieve this task?

- A. `rsync -aHAX /share/* serverB:/newshare`

- B. `dd if=/share/* of=serverB:/newshare` C. `tar -cvf /share/* serverB:/newshare`  
 D. `mirrorlv /share/* serverB:/newshare`

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 148** An administrator needs to look at a log for an application on a `systemd`-based system. There is no log for this application in `/var/log`. Which of the following is another way to view the application log on this system?

- A. `tail -f /var/log/secure`  
 B. `journalctl -u application`  
 C. `systemctl application.service`  
 D. `watch /var/lib/application/`

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 149** Which of the following is true about Type 2 hypervisors?

- A. Type 2 hypervisors run on top of another general purpose OS.  
 B. Type 2 hypervisors are often called bare-metal or native hypervisors.  
 C. Type 2 hypervisors offer a performance increase to the guests in comparison to a Type 1 hypervisor.  
 D. Only Type 2 hypervisors allow direct access to CPU virtualization features.

**Correct Answer: A**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.sciencedirect.com/topics/computer-science/hypervisors>

**QUESTION 150**

A security administrator wants to display a warning banner before a user logs in. Which of the following files must be edited to make this happen?

- A. `/etc/services`  
 B. `/etc/issue`  
 C. `/etc/hosts`  
 D. `/etc/motd`

**Correct Answer: D**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://kerneltalks.com/tips-tricks/how-to-configure-login-banners-in-linux/>

**QUESTION 151**

Using which of the following control mode commands is the correct way to substitute all occurrences of `/dev/sdc` with `/dev/sdd` while editing a file in `vi`?

- A. `:s//dev/sdc//dev/sdd`
- B. `:s\/dev\/sdc\/dev\/sdd/g`
- C. `:s\/dev\/sdc\/dev\/sdd`
- D. `:%s\/dev\/sdc\/dev\/sdd`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 152

A user needs to modify the IP address of a laptop. Which of the following files can be used to configure the network interface named `eth0`?

- A. `/etc/sysconfig/network/interfaces.cnf`
- B. `/system/config/interfaces`
- C. `/etc/sysconfig/network-scripts/ifcfg-eth0`
- D. `/system/networking/ifconfig`
- E. `/etc/interfaces/eth0.conf`

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://opensource.com/life/16/6/how-configure-networking-linux>

**QUESTION 153** A user wants to use terminal services from a Windows workstation to manage a Linux server. Which of the following should be installed on the Linux server to enable this functionality?

- A. VNC
- B. rdesktop
- C. SPICE
- D. XRDP

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.netadmintools.com/art237.html>

#### QUESTION 154

On a UEFI-based system, which of the following invokes GRUB2 from the EFI command prompt?

- A. `boot//EFI/grub2.efi`
- B. `EFI/grub2.efi`
- C. `/boot/EFI/grub2.efi`
- D. `/grub2.efi`

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://docs.pagure.org/docs-fedora/the-grub2-bootloader.html>

**QUESTION 155** A systems administrator notices a large number of autoloaded device modules are no longer needed and decides to do a cleanup of them. Which of the following commands will accomplish this task?

- A. `rmmmod -c`
- B. `depmod -r`
- C. `insmod -c`
- D. `modprobe -r`

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <http://ccrma.stanford.edu/planetccrma/man/man8/modprobe.8.html>

**QUESTION 156** A Linux administrator looks at the `/etc/timezone` file and determines the need to change the time zone from California to New York temporarily. Which of the following commands will accomplish this?

- A. `sed -f TZ=America/New_York`
- B. `cat TZ=America/New_York`
- C. `export TZ=America/New_York`
- D. `printf TZ=America/New_York`

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.thegeekstuff.com/2010/09/change-timezone-in-linux/>

**QUESTION 157**

A user has been locked out of an account due to too many failed password attempts. Which of the following commands will unlock the user's account?

- A. `pam_tally2 --user=user --reset`
- B. `passwd -u user -G root`
- C. `usermod -u user -G root`
- D. `chage -1 user=user --reset`

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [https://www.tecmint.com/use-pam\\_tally2-to-lock-and-unlock-ssh-failed-login-attempts/](https://www.tecmint.com/use-pam_tally2-to-lock-and-unlock-ssh-failed-login-attempts/)

**QUESTION 158**

A systems administrator receives a report that the web server is not running after a planned system reboot. After starting the web server manually, which of the following commands should the administrator issue to ensure the web server starts at boot time?

- A. `systemctl service on`
- B. `systemctl enable <name>.service`
- C. `systemctl service enable`
- D. `systemctl on <name>.service`

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**Reference: <https://geekflare.com/how-to-auto-start-services-on-boot-in-linux/>**QUESTION 159**

An administrator is reviewing updates in the master online Git repository and notices a file named `.htaccess`. The file contains passwords and should only be in the administrator's local repository, not the online one. Which of the following would prevent this file from appearing online in the future?

- A. `git commit -m "File Update" -x .htaccess`
- B. `sed -i 's/#Preserve Hidden=True/Preserve Hidden=True/g' .git/config`
- C. `chown nobody:nobody .htaccess`
- D. `echo ".htaccess" >> .gitignore`

**Correct Answer:** D**Section:** (none)**Explanation****Explanation/Reference:****QUESTION 160**

A technician wants to secure a sensitive workstation by ensuring network traffic is kept within the local subnet. To accomplish this task, the technician executes the following command:

```
echo 0 > /proc/sys/net/ipv4/ip_default_ttl
```

Which of the following commands can the technician use to confirm the expected results? (Choose two.)

- A. `tcpdump`
- B. `traceroute`
- C. `route`
- D. `iperf`
- E. `ip`
- F. `arp`

**Correct Answer:** CF**Section:** (none)**Explanation****Explanation/Reference:**

**QUESTION 161** An administrator needs to create a file named `hello` in the home directory that contains the following text:

```
it's me!
```

Which of the following commands would accomplish this goal?

- A. `mkdir ~/hello touch`
- ~/ "it's me!" B. `touch`
- ~/hello `echo "it's me!" >`
- ~/hello C. `mv ~/hello cp`
- "it's me!" > ~/hello D.
- `type ~/hello print "it's`
- `me!"`

**Correct Answer:** A**Section:** (none)**Explanation**

**Explanation/Reference:**

**QUESTION 162** Which of the following commands will let a Linux user know the PCI devices that are installed in the system?

- A. `cat /proc/devices/pci`
- B. `lspci`
- C. `lsdev`
- D. `cat /proc/sys/dev`

**Correct Answer: B Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://opensource.com/article/19/9/linux-commands-hardware-information>

**QUESTION 163** A Linux administrator is updating iptables rules and is given the following tasks:

- Output a list of iptables rules.
- Remove all iptables rules.

Which of the following actions should be performed from the terminal console to accomplish these tasks? (Choose two.)

- A. `iptables -F`
- B. `iptables -L`
- C. `iptables -I`
- D. `iptables -C`
- E. `iptables -A`
- F. `iptables -N`

**Correct Answer: AB**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

Reference: <https://www.digitalocean.com/community/tutorials/how-to-list-and-delete-iptables-firewall-rules>

**QUESTION 164**

A junior Linux administrator is performing version control on a Git repository. The administrator is given a list of tasks to complete:

- List the currently installed Git release.
- Show the status reporting of the clone.

Which of the following commands would allow the administrator to complete these tasks? (Choose two.)

- A. `git clone --progress`
- B. `git clone --recursive`
- C. `git --help`
- D. `git clone --dissociate`
- E. `git --version`
- F. `git clone --shared`

**Correct Answer: AC**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 165**

A systems administrator needs to allow the Linux server to receive HTTP connections from Internet hosts. By default, the port for HTTP connections is blocked. Which of the following rules should be added in the firewall to allow this type of connection?

- A. `firewall-cmd --zone=public --add-port=443/tcp --permanent`
- B. `firewall-cmd --zone=internal --add-port=80/tcp --permanent`
- C. `firewall-cmd --zone=public --add-port=80/tcp --permanent`
- D. `firewall-cmd --zone=internal --add-port=443/tcp --permanent`

**Correct Answer: C**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 166**

A Linux administrator attempts to install the package `newprogram.x86_64.rpm` using a package manager. The administrator receives a warning indicating the command that was run was using a deprecated package manager. Which of the following commands should the administrator use to avoid the warning and install the `newprogram.x86_64.rpm` program?

- A. `# dnf install newprogram.x86_64.rpm`
- B. `# rpm -e newprogram.x86_64.rpm`
- C. `# dpkg -i newprogram.x86_64.rpm`
- D. `# apt-get install newprogram.x86_64.rpm`

**Correct Answer: B**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

VCEUp

**QUESTION 167** Which of the following would allow remote users to access a corporate server? (Choose two.)

- A. VPN server
- B. SMTP server
- C. NTP server
- D. SSH server
- E. DHCP server
- F. File server

**Correct Answer: AD**

**Section: (none)**

**Explanation**

**Explanation/Reference:**

**QUESTION 168** A junior administrator is configuring local name lookups for fully qualified domain names in an isolated environment. The administrator is given a checklist and must accomplish the following tasks:

- Add localhost with loopback address.
- Add 192.168.192.12/24 to resolve to `database01.comptia.org`

Given this scenario, which of the following steps should the administrator perform to accomplish these tasks?

- A. Open the `/etc/nsswitch.conf` file with a file editor and add the following lines:

```
127.0.0.1 localhost
192.168.192.12 database01.comptia.org
```

B. Open the `/etc/dhcpd.conf` file with a file editor and add the following lines:

```
127.0.0.1 localhost
192.168.192.12 database01.comptia.org
```

C. Open the `/etc/hosts` file with a file editor and add the following lines:

```
127.0.0.1 localhost
192.168.192.12 database01.comptia.org
```

D. Open the `/etc/network` file with a file editor and add the following lines:

```
127.0.0.1 localhost
192.168.192.12 database01.comptia.org
```

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 169** An administrator is reviewing suspicious activity on a server and needs to determine which users logged into the system within the past 24 hours. Which of the following commands should the administrator run to determine this?

- A. `last`
- B. `who`
- C. `id`
- D. `usermod`

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [https://linuxhint.com/detect\\_linux\\_system\\_hacked/](https://linuxhint.com/detect_linux_system_hacked/)

**QUESTION 170**

During the final step of staging new Linux hardware, GRUB2 is installed to the system drive. Which of the following BEST describes the role of GRUB2 in a new Linux installation?

- A. It provides a menu for creating administrator task shortcuts.
- B. It provides a menu for running special shell scripts.
- C. It provides a method to partition a hard drive.
- D. It provides a method to pass parameters to the Linux kernel on startup.

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: [https://docs.fedoraproject.org/en-US/fedora/rawhide/system-administrators-guide/kernel-module-driver-configuration/Working\\_with\\_the\\_GRUB\\_2\\_Boot\\_Loader/](https://docs.fedoraproject.org/en-US/fedora/rawhide/system-administrators-guide/kernel-module-driver-configuration/Working_with_the_GRUB_2_Boot_Loader/)

**QUESTION 171**

A site reliability engineer updated the latest configuration management scripts and committed them to a workstream called either `test` or `patch`. A Linux administrator wants to ensure these latest workstreams are able to be retrieved to the server. Which of the following is the BEST Git attribute to use?

- A. `branch`
- B. `fetch`

- C. log
- D. pull

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

#### QUESTION 172

A systems administrator wants to disable the Linux Kernel WatchDog Timer Driver for security purposes. Which of the following will accomplish this task?

- A. Add `blacklist watchdog` to the `/etc/modprobe.d/blacklist` file.
- B. Rename the `/etc/modprobe.d/watchdog` file to `watchdog.off` instead.
- C. Remove the `watchdog=1` from the `/usr/modules/watchdog.conf` file.
- D. Add `watchdog=0` to the `/etc/modprobe.conf` file.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

**QUESTION 173** In which of the following Linux GUI environments would the Konsole application MOST likely be found?

- A. Gnome
- B. KDE
- C. Cinnamon
- D. Unity
- E. MATE

**Correct Answer:** B

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://opensource.com/life/17/10/top-terminal-emulators>

#### QUESTION 174

A new user has been added to a Linux machine. Which of the following directories would contain the user's default files?

- A. `/etc/login.defs`
- B. `/etc/passwd`
- C. `/etc/skel`
- D. `/etc/inittab`

**Correct Answer:** C

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://linuxize.com/post/how-to-create-users-in-linux-using-the-useradd-command/>

**QUESTION 175** An issue was discovered on a testing branch of a Git repository. A file was inadvertently modified and needs to be reverted to the master branch version. Which of the following is the BEST option to resolve the issue?

- A. `git branch -b master file`
- B. `git merge master testing`
- C. `git stash branch master`
- D. `git checkout master -- file`

**Correct Answer:** D

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://www.git-scm.com/book/en/v2/Git-Basics-Undoing-Things>

**QUESTION 176**

A junior systems administrator has generated a PKI certificate for SSH sessions. The administrator would like to configure authentication without passwords to remote systems. Which of the following should the administrator perform?

- A. Add the content of `id_rsa.pub` file to the remote system `~/.ssh/authorized_keys` location.
- B. Add the content of `id_rsa` file to the remote system `~/.ssh/authorized_keys` location.
- C. Add the content of `id_rsa` file to the remote system `~/.ssh/known_hosts` location.
- D. Add the content of `id_rsa.pub` file to the remote system `~/.ssh/known_hosts` location.

**Correct Answer:** A

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://kb.iu.edu/d/aews>

**QUESTION 177**

A junior systems administrator is scanning `archive.tar` files with an antivirus scanner. The administrator is given the following tasks:

- List all files that are in the `archive.tar` files. ▪

Extract all files from the `archive.tar` files.

Which of the following actions should be performed to meet these requirements? (Choose two.)

- A. `tar -tvf archive.tar`
- B. `tar -xf archive.tar` C. `tar -A archive.tar`
- D. `tar -av archive.tar`
- E. `tar -r archive.tar`
- F. `tar -uvz archive.tar`

**Correct Answer:** AB

**Section:** (none)

**Explanation**

**Explanation/Reference:**

Reference: <https://linuxize.com/post/how-to-create-and-extract-archives-using-the-tar-command-in-linux/>

**QUESTION 178**

**SIMULATION**

After installing a new web server, you are unable to browse to the default web page.

**INSTRUCTIONS**

Review all the command output and select the command needed to remediate the issue.

*If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.*

## Commands

```
[root@webserver log]# getenforce
[root@webserver log]# getsebool -a | grep httpd
[root@webserver log]# netstat -antp
[root@webserver log]# ss -antp
[root@webserver log]# ps -ef | grep nginx
[root@webserver log]# grep avc
/var/log/audit/audit.log
[root@webserver log]# more /var/log/web/access_log
[root@webserver log]# more /var/log/web/error_log
[root@webserver log]# ls -la
[root@webserver log]# journalctl -u nginx -1
[root@webserver log]# systemctl status webserver
[root@webserver log]# sealert
```

## Answer

```
[root@webserver log]#
```

## Output

## Commands

```
[root@webserver log]# getenforce
[root@webserver log]# getsebool -a | grep httpd
[root@webserver log]# netstat -antp
[root@webserver log]# ss -antp
[root@webserver log]# ps -ef | grep nginx
[root@webserver log]# grep avc
/var/log/audit/audit.log
[root@webserver log]# more /var/log/web/access_log
[root@webserver log]# more /var/log/web/error_log
[root@webserver log]# ls -la
[root@webserver log]# journalctl -u nginx -l
[root@webserver log]# systemctl status webserver
[root@webserver log]# systemctl
```

## Answer

```
[root@webserver log]#
```

```
systemctl restart nginx
```

```
[root@localhost log]# getsebool -a | grep httpd
httpd_anon_write --> off
httpd_builtin_scripting --> on
httpd_can_check_spam --> off
httpd_can_connect_ftp --> off
httpd_can_connect_ldap --> off
httpd_can_connect_mythtv --> off
httpd_can_connect_zabbix --> off
httpd_can_network_connect --> off
httpd_can_network_connect_cobbler --> off
httpd_can_network_connect_db --> off
httpd_can_network_memcache --> off
httpd_can_network_relay --> off
httpd_can_sendmail --> off
httpd_dbus_avahi --> off
httpd_dbus_sss --> off
httpd_dontaudit_search_dirs --> off
httpd_enable_cgi --> on
httpd_enable_ftp_server --> off
httpd_enable_homedirs --> off
httpd_execmem --> off
httpd_graceful_shutdown --> on
httpd_manage_ipa --> off
httpd_mod_auth_ntlm_winbind --> off
httpd_mod_auth_pam --> off
httpd_read_user_content --> off
httpd_run_ipa --> off
```

## Commands

```
[root@webserver log]# getenforce
[root@webserver log]# getsebool -a | grep httpd
[root@webserver log]# netstat -antp
[root@webserver log]# ss -antp
[root@webserver log]# ps -ef | grep nginx
[root@webserver log]# grep avc
/var/log/audit/audit.log
[root@webserver log]# more /var/log/web/access_log
[root@webserver log]# more /var/log/web/error_log
[root@webserver log]# ls -la
[root@webserver log]# journalctl -u nginx -l
[root@webserver log]# systemctl status webserver
[root@webserver log]# sealert
```

## Answer

```
[root@webserver log]#
systemctl restart nginx
```

```
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State PID/Program name
tcp 0 0 0.0.0.0:111 0.0.0.0:* LISTEN 1/systemd
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN 3431/nginx: master
tcp 0 0 192.168.122.1:53 0.0.0.0:* LISTEN 1517/dnsmasq
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN 1137/sshd
tcp 0 0 127.0.0.1:631 0.0.0.0:* LISTEN 1141/cupsd
tcp 0 0 127.0.0.1:25 0.0.0.0:* LISTEN 1387/master
tcp6 0 0 :::111 :::* LISTEN 1/systemd
tcp6 0 0 :::80 :::* LISTEN 3431/nginx: master
tcp6 0 0 :::22 :::* LISTEN 1137/sshd
tcp6 0 0 :::631 :::* LISTEN 1141/cupsd
tcp6 0 0 :::3128 :::* LISTEN 1138/squid
tcp6 0 0 :::25 :::* LISTEN 1387/master
```

## Commands

```
[root@webserver log]# getenforce
[root@webserver log]# getsebool -a | grep httpd
[root@webserver log]# netstat -antp
[root@webserver log]# ss -antp
[root@webserver log]# ps -ef | grep nginx
[root@webserver log]# grep avc
/var/log/audit/audit.log
[root@webserver log]# more /var/log/web/access_log
[root@webserver log]# more /var/log/web/error_log
[root@webserver log]# ls -la
[root@webserver log]# journalctl -u nginx -l
[root@webserver log]# systemctl status webserver
[root@webserver log]# sealert
```

## Answer

```
[root@webserver log]#
systemctl restart nginx
```

```
[root@localhost log]# ps -ef | grep nginx
root 3431 1 0 09:26 ? 00:00:00 nginx: master process /usr/sbin/nginx
nginx 3432 3431 0 09:26 ? 00:00:00 nginx: worker process
nginx 3433 3431 0 09:26 ? 00:00:00 nginx: worker process
root 5042 3087 0 09:57 pts/0 00:00:00 grep --color=auto nginx
```

VCEUp

<p><b>Commands</b></p> <pre>[root@webserver log]# getenforce [root@webserver log]# getsebool -a   grep httpd [root@webserver log]# netstat -antp [root@webserver log]# ss -antp [root@webserver log]# ps -ef   grep nginx [root@webserver log]# grep avc /var/log/audit/audit.log [root@webserver log]# more /var/log/web/access_log [root@webserver log]# more /var/log/web/error_log [root@webserver log]# ls -la [root@webserver log]# journalctl -u nginx -1 [root@webserver log]# systemctl status webserver [root@webserver log]# systemctl</pre>	<p><b>Answer</b></p> <pre>[root@webserver log]# systemctl restart nginx</pre>
---	---

```

type=AVC msg=audit(1524839402.317:210): avc: denied { rlimitinh } for pid=3537 comm="pkla-check-auth"
scontext=system_u:system_r:policykit_t:s0 tcontext=system_u:system_r:policykit_auth_t:s0 tclass=process
type=AVC msg=audit(1524839402.317:210): avc: denied { siginh } for pid=3537 comm="pkla-check-auth"
scontext=system_u:system_r:policykit_t:s0 tcontext=system_u:system_r:policykit_auth_t:s0 tclass=process
type=AVC msg=audit(1524839402.317:210): avc: denied { noatsecure } for pid=3537 comm="pkla-check-auth"
scontext=system_u:system_r:policykit_t:s0 tcontext=system_u:system_r:policykit_auth_t:s0 tclass=process
type=AVC msg=audit(1524839402.342:211): avc: denied { rlimitinh } for pid=3541 comm="pkla-check-auth"
scontext=system_u:system_r:policykit_t:s0 tcontext=system_u:system_r:policykit_auth_t:s0 tclass=process
type=AVC msg=audit(1524839402.342:211): avc: denied { siginh } for pid=3541 comm="pkla-check-auth"
scontext=system_u:system_r:policykit_t:s0 tcontext=system_u:system_r:policykit_auth_t:s0 tclass=process
type=AVC msg=audit(1524839402.342:211): avc: denied { noatsecure } for pid=3541 comm="pkla-check-auth"
scontext=system_u:system_r:policykit_t:s0 tcontext=system_u:system_r:policykit_auth_t:s0 tclass=process

```

<p><b>Commands</b></p> <pre>[root@webserver log]# getenforce [root@webserver log]# getsebool -a   grep httpd [root@webserver log]# netstat -antp [root@webserver log]# ss -antp [root@webserver log]# ps -ef   grep nginx [root@webserver log]# grep avc /var/log/audit/audit.log [root@webserver log]# more /var/log/web/access_log [root@webserver log]# more /var/log/web/error_log [root@webserver log]# ls -la [root@webserver log]# journalctl -u nginx -1 [root@webserver log]# systemctl status webserver [root@webserver log]# systemctl</pre>	<p><b>Answer</b></p> <pre>[root@webserver log]# systemctl restart nginx</pre>
---	---

```

3.10.0-693.21.1.el7.x86_64 #1 SMP Wed Mar 7
19:03:37 UTC 2018 x86_64 x86_64
Alert Count 4
First Seen 2018-04-27 09:32:39 CDT
Last Seen 2018-04-27 09:33:36 CDT
Local ID e60f1ef3-d3d6-4ae4-a3e1-0da75f87a3f9

Raw Audit Messages
type=AVC msg=audit(1524839616.973:219): avc: denied { read } for pid=3432 comm="nginx" name="404.html" dev="dm-0"
ino=6853183 scontext=system_u:system_r:httpd_t:s0 tcontext=unconfined_u:object_r:user_home_t:s0 tclass=file

Hash: nginx,httpd_t,user_home_t,file,read

```



**Correct Answer:** Systemctl restart nginx  
**Section:** (none) **Explanation**

**Explanation/Reference:**

**QUESTION 179** A corporate server security policy states, "Ensure password hashes are not readable by non-administrative users." The administrator should check the permissions on which of the following files to ensure the server satisfies this policy?

- A. /etc/shadow

- B. /etc/passwd
- C. /etc/group
- D. /etc/security/limits.conf

**Correct Answer: B**  
**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 180** A Linux systems administrator is implementing Source Code Management for the web application server configuration files located in /etc/httpd/. Which of the following steps should the administrator perform FIRST?

- A. Clone the remote repository using 'git clone'
- B. Create a new repository using 'git init'
- C. Retrieve the remote changes using 'git commit'
- D. Configure the directory for git using 'git config'

**Correct Answer: D**  
**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 181**

A junior systems administrator is tasked with providing the `network_administrators` group the ability to perform `sudo` without prompting for a password. Which of the following steps should the administrator perform to accomplish this task? (Choose two.)

- A. Use `visudo` to edit the `/etc/sudoers` file and add `network_administrators` to the "wheel" group
- B. Use `vi` to edit the `/etc/sudo` file and add `network_administrators` to the "wheel" group
- C. Provide all `network_administrators` with the "root" account password
- D. Add the `network_administrators ALL=(ALL) NOPASSWD: ALL` directive to the `/etc/sudoers` file
- E. Add the `network_administrators=(ALL) NOEXEC: ALL` directive to the `/etc/sudoers` file

**Correct Answer: CD**  
**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 182**

A storage administrator in a virtualized environment has been told by a user that there is no space left on the volume to which the user can write. However, a check reveals that there is 20GB of unused space. Which of the following explains the discrepancy?

- A. The drive is not formatted
- B. The drive is thin provisioned
- C. The drive is thick provision eager zeroed
- D. The drive space is overallocated

**Correct Answer: B**  
**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 183**

A systems administrator has scheduled a system update for a server. The update includes a resynchronization of the package database and updates to the current packages and the system distribution packages. Which of the following commands contains the proper order of this update?

- A. apt-get upgrade, apt-get dist-upgrade, apt-get update
- B. apt-get update, apt-get upgrade, apt-get dist-upgrade
- C. apt-get dist-upgrade, apt-get upgrade, apt-get update
- D. apt-get update, apt-get dist-upgrade, apt-get upgrade

**Correct Answer: B**

**Section: (none) Explanation**

**Explanation/Reference:**

#### QUESTION 184

An administrator receives the following message on a remote server: `Cannot open display`. Which of the following should the administrator have used to log in to the server?

- A. `xrdp -h server.company.com`
- B. `ssh -X server.company.com`
- C. `xvnc server.company.com`
- D. `rdesktop server.company.com`

**Correct Answer: B**

**Section: (none) Explanation**

**Explanation/Reference:**

#### QUESTION 185

A junior administrator is installing kernel modules. The administrator is given a checklist that outlines the following tasks to be completed:

- Display currently installed module version.
- Display which modules loaded at startup.

Which of the following commands would be used to accomplish these tasks? (Choose two.)

- A. `cat /etc/issue`
- B. `insmod`
- C. `lsmod`
- D. `rmmmod`
- E. `depmod`
- F. `dmesg`

**Correct Answer: CD**

**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://linuxize.com/post/lsmod-command-in-linux/>

#### QUESTION 186

An administrator wants to know the amount of memory installed on a Linux server. Which of the following commands can be used to accomplish this task?

- A. `cat /sys/proc/meminfo`
- B. `cat /proc/meminfo`
- C. `cat /proc/sys/meminfo`
- D. `cat /sys/meminfo`

**Correct Answer: D**

**Section: (none) Explanation**

**Explanation/Reference:**

Reference: [https://devconnected.com/how-to-check-ram-on-linux/#:~:text=The%20most%20popular%20command%20in,use%20the%20%20free%20command.&text=As%20you%20can%20see%2C%20the,\(also%20called%20virtual%20memory\)](https://devconnected.com/how-to-check-ram-on-linux/#:~:text=The%20most%20popular%20command%20in,use%20the%20%20free%20command.&text=As%20you%20can%20see%2C%20the,(also%20called%20virtual%20memory))

**QUESTION 187** A Linux administrator is helping the security team troubleshoot an SELinux policy violation incident. Which of the following would be the BEST utility command to display SELinux violation and AVC denial messages?

- A. journalctl | grep sealert
- B. sealert -a /var/log/audit/audit.log
- C. aureport | grep AVC
- D. cat /var/log/messages | grep selinux

**Correct Answer: B**  
**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 188** A systems administrator received a request to change the hostname to a new name. Which of the following file configurations should be changed to fix the hostname in the server?

- A. /etc/sysconfig/network
- B. /etc/hosts
- C. /etc/resolv.conf
- D. /etc/sysconfig/nsswitch.conf

**Correct Answer: B**  
**Section: (none) Explanation**

**Explanation/Reference:**

Reference <https://www.tecmint.com/set-hostname-permanently-in-linux/>

**QUESTION 189** An administrator notices the HISTSIZE variable is 50, using the commands below:

```
HISTSIZE=50
export HISTSIZE
```

The administrator rechecks the HISTSIZE value using `echo HISTSIZE` but gets no value. Which of the following commands should the administrator use to retrieve its value?

- A. printenv | grep \$HISTSIZE
- B. echo HISTSIZE
- C. printf HISTSIZE
- D. grep \$HISTSIZE

**Correct Answer: B**  
**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://superuser.com/questions/478926/histsize-not-being-set-in-bash>

**QUESTION 190**

Users in the payroll department are not configured to use DNS due to security concerns. The users ask the junior Linux administrator to configure their workstations to access the payroll server at 192.168.204.11 by the name "Payroll". Which of the following commands should the administrator issue to meet this request?

- A. echo "nameserver 192.168.204.11 #Payroll" >> /etc/resolv.conf
- B. echo "net.ipv4.ip\_dynaddr=192.168.204.11 Payroll" >> /etc/sysctl.conf
- C. echo "192.168.204.11 Payroll" >> /etc/hosts

```
D. echo `IPADDR="192.168.204.11" #Payroll' >> /etc/network/interface
```

**Correct Answer: C**

**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 191** A systems administrator downloads an application's source files, compiles the application, and installs it per the application's installation instructions. When trying to run the application, the system states:

```
$ occmd
bash: occmd: command not found..
```

Running the `locate` command shows it does exist in the following location:

```
/opt/occmd/bin/occmd
```

Which of the following should the administrator do to allow the command to run properly? (Choose two.)

- A. `sudo ln -s /opt/occmd/bin/occmd /usr/local/bin/occmd`
- B. `echo "export PATH=$PATH:/opt/occmd/bin" >> ~/.bashrc`
- C. `mv /opt/occmd ~/ && ln -s ~/occmd/bin/occmd ./occmd`
- D. `echo "#!/bin/bash \n ${which occmd}" > /usr/bin/occmd.sh`
- E. `sudo mv /opt/occmd/bin/occmd /etc/bin/`
- F. `cd /opt/occmd/bin && chmod +x ./occmd && restorecon -rv *`

**Correct Answer: EF**

**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 192**

A Linux administrator tries to ping a hostname in a network but receives the message: `hostname not found`. The administrator is sure the name exists on the network and wants to verify if the DNS server is correctly configured on the client. Which of the following files should the administrator use to verify this information?

- A. `/etc/named.conf`
- B. `/etc/resolv.conf`
- C. `/etc/nsswitch.conf`
- D. `/etc/network`

**Correct Answer: B**

**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://www.hostgator.com/help/article/error-your-hostname-could-not-be-resolved-to-an-ip-address>

**QUESTION 193**

Users are unable to connect to a server using HTTPS. The administrator runs the following command on the remote system:

```
$ netstat
tcp 0 0 0.0.0.0:80 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:443 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
```

Then, the administrator runs the following command from a local workstation:

```
$ nmap
PORT STATE
80    open
443   closed
22    open
```

Which of the following steps should the administrator take to address the issue?

- A. Start the application to run on port 443
- B. Configure the application to run on an active port
- C. Allow port 443 through the firewall
- D. Update the self-signed certificate

**Correct Answer: C**

**Section: (none) Explanation**

**Explanation/Reference:**

#### QUESTION 194

A Linux administrator is restoring the SELinux contexts on an entire system. Which of the following commands is the BEST option to complete this task?

- A. `setenforce 0 && reboot`
- B. `setfacl -bR / && reboot`
- C. `touch /.autorelabel && reboot`
- D. `restorecon / && reboot`

**Correct Answer: D**

**Section: (none) Explanation**

**Explanation/Reference:**

Reference: [https://access.redhat.com/documentation/en-us/red\\_hat\\_enterprise\\_linux/7/html/selinux\\_users\\_and\\_administrators\\_guide/sect-security-enhanced\\_linux-working\\_with\\_selinux-selinux\\_contexts\\_labeling\\_files](https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/selinux_users_and_administrators_guide/sect-security-enhanced_linux-working_with_selinux-selinux_contexts_labeling_files)

**QUESTION 195** An administrator has a CSV file named `hosts.csv`. The contents of `hosts.csv` include the following:

```
192.168.2.57,lnx1prd.example.com,Linux,Production
192.168.2.58,lnx2prd.example.com,Linux,Production
192.168.1.4,server15.example.com,Windows,Development
```

The administrator needs to create a second comma-separated list of only the Linux server IP addresses. Which of the following commands would achieve this need?

- A. `for ip in $(grep "Linux" hosts.csv | cut -d"," -f1); do echo -n "$ip,"; done`
- B. `for ip in $( cut -d"," -f1 hosts.csv | grep "Linux"); do echo -n "$ip,"; done`
- C. `for ip in $(grep "Linux" hosts.csv | sed "/$1//"); do echo -n "$ip,"; done`
- D. `for ip in $(awk -F, '{print $1}' hosts.csv | grep "Linux"); do echo -n "$ip,"; done`

**Correct Answer: C**

**Section: (none) Explanation**

**Explanation/Reference:**

#### QUESTION 196

An administrator is installing a Linux VM on a personal hypervisor. The administrator wants to have the VM's IP address on the same network as the hypervisor host so the VM has the same network properties as the physical interface of the host. To which of the following should the administrator set the network properties?

- A. Host-only network
- B. NAT network
- C. Bridge network
- D. Overlay network

**Correct Answer: C**

**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://www.nakivo.com/blog/virtualbox-network-setting-guide/>

#### QUESTION 197

A raw VM image is being compressed with bzip2 and copied to a flash drive at `/dev/hdb` for off-site use by the marketing department. Which of the following command lines accomplishes this task?

- A. `mv /vm/mkgt.img | bzip2 /dev/hdb/mkgt.img.bz2`
- B. `bzip2 -c /vm/mktg.img | dd of=/dev/hdb`
- C. `cp /vm/mktg.img | bzip2 /dev/hdb/mktg.img.bz2`
- D. `cp -a -r /vm/mktg.img bzip2 /dev/hdb/mktg.img.zip`

**Correct Answer: C**

**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 198** A systems administrator wants to install a new application that requires the `newmod` kernel module. Which of the following commands should the systems administrator use?

- A. `lsof newmod`
- B. `modinfo newmod`
- C. `lsmod newmod`
- D. `modprobe newmod`

**Correct Answer: B**

**Section: (none) Explanation**

**Explanation/Reference:**

#### QUESTION 199

A server, which is used to collect data about the network and datacenter environment via SNMP, is running out of space. Which of the following should the server administrator implement to reduce disk utilization?

- A. `journald`
- B. Snapshots
- C. `logrotate`
- D. `tar -cvf`

**Correct Answer: B**

**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 200** In which of the following directories is the `vmlinuz` file located?

- A. `/boot`
- B. `/etc`
- C. `/bin`
- D. `/proc`

**Correct Answer: A**  
**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://askubuntu.com/questions/452070/what-is-vmlinuz-file-on-live-ubuntu>

**QUESTION 201** A systems administrator is implementing disk quotas on `/home`. During the process, the administrator receives the following error:

```
Cannot find filesystem to check or filesystem not mounted with user quota option.
```

Which of the following is the correct order of steps the administrator should follow to resolve this error?

- A. 1. Verify if `/home` has quotas enabled in `/etc/fstab` and, if not, enable it.  
 2. Remount `/home`.  
 3. Create the quota database files and generate the disk usage table.  
 4. Assign user quota policies.
- B. 1. Create the quota database files and generate the disk usage table.  
 2. Verify if `/home` has quotas enabled in `/etc/fstab` and, if not, enable it.  
 3. Remount `/home`.  
 4. Assign user quota policies.
- C. 1. Verify if `/home` has quotas enabled in `/etc/fstab` and, if not, enable it.  
 2. Create the quota database files and generate the disk usage table.  
 3. Remount `/home`.  
 4. Assign user quota policies.
- D. 1. Assign user quota policies.  
 2. Verify if `/home` has quotas enabled in `/etc/fstab` and, if not, enable it.  
 3. Create the quota database files and generate the disk usage table.  
 4. Remount `/home`.

**Correct Answer: A**  
**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://www.howtoforge.com/community/threads/quotacheck-cannot-find-filesystem-to-check.25954/>

**QUESTION 202**

A Linux user wants to give read-only permissions to a directory and its contents. Which of the following commands will allow the user to accomplish this task?

- A. `chmod -R 400 /new_directory/`
- B. `chmod -R 600 /new_directory/`
- C. `chmod 400 /new_directory/`
- D. `chmod 600 /new_directory/`

**Correct Answer: D**  
**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://www.linode.com/docs/guides/modify-file-permissions-with-chmod/>

**QUESTION 203** A Linux administrator needs to remove a USB drive from a system. The `umount` command fails, stating the device is busy. Which of the following commands will show the reason for this error?

- A. `lsusb | grep /mnt/usb`
- B. `mount | grep /mnt/usb`
- C. `ps aux | grep /mnt/usb`
- D. `lsof | grep /mnt/usb`

**Correct Answer: D**

**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://www.systutorials.com/force-linux-umount-filesystem-reporting-device-busy/>

**QUESTION 204**

A Linux systems administrator is troubleshooting an issue with the `/home` directory running out of space. The administrator needs to determine which `/home` directories are using the most space. Which of the following commands should be used?

- A. `du`
- B. `lvs`
- C. `df`
- D. `fsck`

**Correct Answer: A**

**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://www.cs.washington.edu/lab/faq/home-directory-size>

**QUESTION 205** An administrator needs a bootable USB for installing a new Linux machine. The administrator downloaded the image file and named it as `Linux_OS.iso` in the `/tmp` directory. Which of the following commands will accomplish that task?

- A. `dd input=/tmp/Linux_OS.iso of=/dev/sda bs=512`
- B. `dd in=/tmp/Linux_OS.iso out=/dev/sdb bs=512`
- C. `dd if=/tmp/Linux_OS.iso of=/dev/sda bs=512`
- D. `dd if=/tmp/Linux_OS.iso out=/dev/sdb1 bs=512`

**Correct Answer: C**

**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://medium.com/the-blog-of-ehsan-nazim/how-to-make-linux-isos-bootable-from-usb-flash-drive-the-command-line-way-380fca04e096>

**QUESTION 206**

A junior Linux administrator needs to create 16 empty files quickly that will contain sales information for each quarter for the past four years. Which of the following commands will meet this requirement?

- A. `touch {2015,2016,2017,2018}. {q1,q2,q3,q4}`
- B. `touch [2015,2016,2017,2018]. [q1,q2,q3,q4]`
- C. `touch `2015,2016,2017,2018`. `q1,q2,q3,q4``
- D. `touch {2015.2016.2017.2018}. {q1.q2.q3.q4}`

**Correct Answer: C**

**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 207**

An administrator needs to change the DNS domain search order of a single Linux host to localize it better. Which of the following files should the administrator edit?

- A. /etc/resolv.conf
- B. /etc/hosts
- C. /etc/nsswitch.conf
- D. /etc/dhcpd.conf

**Correct Answer: C**

**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://www.cyberciti.biz/faq/howto-change-dns-search-order-in-linux/>

**QUESTION 208** A user issues the following command:

```
ls -l /var/log | egrep -e '^d[rwx]{3}.*[rw-]{3}.*'
```

The list of files in the system is shown below:

```
ls -l /var/log/
total 1156
-rw-r--r-- 1 root root 2877 Apr 24 14:14 alternatives.log
drwxr-xr-x 2 root root 4096 Apr 24 08:36 apt
-rw-r----- 1 syslog adm 37910 Jun 12 15:22 auth.log
-rw----- 1 root utmp 0 Apr 24 08:19 btmp
-rw-r--r-- 1 syslog adm 246139 Jun 12 15:21 cloud-init.log
-rw-r--r-- 1 root root 8872 Jun 12 15:21 cloud-init-output.log
drwxr-xr-x 2 root root 4096 Apr 9 14:25 dist-upgrade
-rw-r--r-- 1 root root 21326 Apr 24 14:14 dpkg.log
drwxr-xr-x 2 root root 4096 Apr 24 08:16 fsck
-rw-r----- 1 syslog adm 152618 Jun 12 15:21 kern.log
-rw-rw-r-- 1 root utmp 292876 Jun 12 15:21 lastlog
drwxr-xr-x 2 root root 4096 Dec 7 2017 lxd
-rw-r----- 1 syslog adm 388374 Jun 12 15:24 syslog
drwxr-x--- 2 root adm 4096 Apr 25 14:41 unattended-upgrades
drwxr-x--- 2 root adm 4096 Apr 25 15:41 attended-upgrades
-rw-r--r-- 1 root root 1 Apr 24 14:15 vboxadd-install.log
-rw-r--r-- 1 root root 255511 Apr 24 14:15 vboxadd-setup.log
-rw-rw-r-- 1 root utmp 10368 Jun 12 15:21 wtmp
```

VCEUp

Which of the following results matches the command issued?

- A. drwxr-x--- 2 root adm 4096 Apr 25 14:41 unattended-upgrades  
drwxr-x--- 2 root adm 4096 Apr 25 15:41 attended-upgrades
- B. drwxr-xr-x 2 root root 4096 Apr 24 08:36 apt  
drwxr-xr-x 2 root root 4096 Apr 9 14:25 dist-upgrade  
drwxr-x--- 2 root adm 4096 Apr 25 14:41 unattended-upgrades
- C. drwxr-xr-x 2 root root 4096 Apr 24 08:36 apt  
drwxr-xr-x 2 root root 4096 Apr 9 14:25 dist-upgrade  
drwxr-x--- 2 root adm 4096 Apr 25 15:41 attended-upgrades
- D. -rw-r--r-- 1 root root 2877 Apr 24 14:14 alternatives.log  
-rw-r--r-- 1 syslog adm 246139 Jun 12 15:21 cloud-init.log  
-rw-r--r-- 1 root root 8872 Jun 12 15:21 cloud-init-output.log

**Correct Answer: D**

**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 209** Which of the following BEST describes build automation?

- A. Automating the creation of software and related processes
- B. Automatically categorizing servers in the infrastructure
- C. Managing and provisioning servers via automatic templates
- D. Bringing systems in line with the desired automated configuration

**Correct Answer:** A

**Section:** (none) **Explanation**

**Explanation/Reference:**

Reference: [https://en.wikipedia.org/wiki/Build\\_automation](https://en.wikipedia.org/wiki/Build_automation)

**QUESTION 210**

A Linux administrator needs to configure a new firewall without an existing ACL to allow incoming web traffic. The firewall must log the allowed network traffic. Which of the following command sequences would accomplish this task when they are executed in order?

- A. iptables -A INPUT -p tcp --dport 80 -J LOG iptables -A INPUT -p tcp --dport 443 -J LOG iptables -I INPUT -p tcp --dport 80 -J ACCEPT iptables -I INPUT -p tcp --dport 443 -J ACCEPT
- B. iptables -I INPUT -m multiport -p tcp --dports 80,443 -J LOG iptables -I INPUT -m multiport -p tcp --dports 80,443 -J ACCEPT
- C. iptables -A INPUT -m multiport -p tcp --dports 80,443 -J LOG iptables -A INPUT -m multiport -p tcp --dports 80,443 -J ACCEPT
- D. iptables -A INPUT -p tcp --dport 80 -J ACCEPT iptables -A INPUT -p tcp --dport 443 -J ACCEPT iptables -A INPUT -p tcp --dport 80 -J LOG iptables -A INPUT -p tcp --dport 443 -J LOG

**Correct Answer:** A

**Section:** (none) **Explanation**

**Explanation/Reference:**

Reference: <https://www.linode.com/docs/guides/control-network-traffic-with-iptables/>

**QUESTION 211**

An organization wants to consolidate its entire user information in centralized storage using an X.500-based protocol. Which of the following protocols should be used for this implementation?

- A. RADIUS
- B. LDAP
- C. DNS
- D. DHCP

**Correct Answer:** B

**Section:** (none) **Explanation**

**Explanation/Reference:**

Reference: [https://en.wikipedia.org/wiki/Directory\\_service](https://en.wikipedia.org/wiki/Directory_service)

**QUESTION 212**

An administrator needs to kill the oldest Bash shell running in the system. Which of the following commands should be issued to accomplish this task?

- A. ps axjf | grep bash to obtain PID kill -9 PID
- B. ps -eo pid,etime,cmd | grep bash (to obtain PID) kill -9 PID

- C. `ps -eo pid,etime| grep bash (to obtain PID) killall -9 PID`
- D. `killall -15 -o bash`

**Correct Answer: D**  
**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://phoenixnap.com/kb/how-to-kill-a-process-in-linux>

**QUESTION 213**

Due to security policies, a restriction was implemented that forbids direct access to the database server. The junior administrator needs to connect using SSH tunneling. Which of the following commands allows the junior administrator to connect from a desktop?

- A. `ssh -L dbserver.local:5432:localhost:95432 postgres@dbserver.local`
- B. `ssh -L 5432:localhost dbserver.local:5432 postgres` C. `ssh -L 95432:localhost postgres@dbserver.local`
- D. `ssh -L 9432:localhost:5432 postgres@dbserver.local`

**Correct Answer: D**  
**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 214** Which of the following boot methods can a Linux administrator use to boot a Linux server remotely via a network interface card instead of a local disk?

- A. NTP
- B. PXE
- C. NFS
- D. Kickstart

**Correct Answer: B**  
**Section: (none) Explanation**

**Explanation/Reference:**

Reference: [https://en.wikipedia.org/wiki/Diskless\\_Remote\\_Boot\\_in\\_Linux](https://en.wikipedia.org/wiki/Diskless_Remote_Boot_in_Linux)

**QUESTION 215**

A user requested a USB serial device to be added to a desktop computer. The device has built-in kernel driver support. The administrator tested the device installation and access, but the user cannot access the serial port. Each time the user attempts to access the device, an error log is created that shows the user does not have permission to use the serial port. Which of the following will add a user to the group that has serial port capabilities?

- A. `usermod -a -G serialport $USER`
- B. `usermod -a -G modem $USER`
- C. `usermod -a -G dialout $USER`
- D. `usermod -a -G root $USER`

**Correct Answer: C**  
**Section: (none) Explanation**

**Explanation/Reference:**

Reference: <https://websistent.com/fix-serial-port-permission-denied-errors-linux/>

**QUESTION 216**

A system ran out of storage space on a particular mount and will not allow anything to be written to disk. The `df` command shows there are 6GB free on the mount, and there is no inode exhaustion. This issue has happened before due to a known large log file that was not being rotated. The administrator remembers the file name but cannot remember the location of the log file or which process is writing to it. Which of the following would be the BEST solution to correct this issue while maintaining availability?

- A. Use the `lsof` command to find where the large log file is located and truncate it
- B. Use the `locate` command to find where the large log file is located and delete it
- C. Use the `du` command to find where the large log file is located and delete it
- D. Use the `ps` command to find which process is writing to the log file, and then kill and restart the process

**Correct Answer:** D

**Section:** (none) **Explanation**

**Explanation/Reference:**

**QUESTION 217** A Linux administrator suspects unauthorized users are attempting to log in to the Linux server remotely. Which of the following should the administrator check FIRST?

- A. `/var/log/messages`
- B. `/var/log/secure`
- C. `/var/log/dmesg`
- D. `/var/log/kern.log`

**Correct Answer:** B

**Section:** (none) **Explanation**

**Explanation/Reference:**



**QUESTION 218**

A junior systems administrator is diagnosing an issue with latency. The administrator issues the command `mtr www.comptia.org` at a terminal and receives the following output:

Host	Packets			Pings			
	Loss %	Sent	Last	Avg	Best	Worst	StDev
1. 10.0.5.2	3 %	345	0.6	0.7	0.3	19.6	1.2
2. 192.168.0.1	30 %	345	0.6	45	0.1	0.2	0.04
3. 216.239.14.33	100 %	0	0	0	0	0	0

Given this scenario and the output, which of the following should be reported to the network team for investigation? (Choose two.)

- A. Host 1 is set to filter ICMP reply packets.
- B. Host 1 is set to filter ICMP echo packets.
- C. Host 2 is experiencing high packet loss, indicating the link is overloaded.
- D. Host 2 is experiencing low bandwidth, indicating the ISP is blocking traffic.
- E. Host 3 is set to filter ICMP reply packets.
- F. Host 3 is set to filter ICMP echo packets.

**Correct Answer:** CF

**Section:** (none) **Explanation**

**Explanation/Reference:**

**QUESTION 219** A user receives an `access_denied` error when trying to modify a file, even though the file permissions are set to 777. Which of the following commands should be used to view additional file permissions?

- A. `getsebool`
- B. `getenforce`

- C. `ls -z`
- D. `ps -z`

**Correct Answer: C**

**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 220**

A Linux administrator receives a call from the network operations team that one of the database applications is down on a Linux server. The Linux server is configured with RAID 1 for redundancy, and the array `/dev/md0` consists of two devices called `/dev/sda1` and `/dev/sdb1`. After looking at the status of the RAID 1 array in the `/proc/mdstat` file, the administrator discovers the RAID 1 array is degraded and the disk `/dev/sdb1` on which the database application was installed appears to have failed.

```
cat /proc/mdstat
```

```
Personalities : [linear] [multipath] [raid1]
md0 : active raid1 sda1[0] sdb1[2]
      233456177 blocks [2/1] [U ]
```

Which of the following steps should the administrator take to remove the device `/dev/sdb1` from the RAID array `md0`? (Choose two.)

- A. `mdadm /dev/md0 --remove /dev/sdb1`
- B. `mdadm /dev/sdb1 --fail /dev/md0`
- C. `mdadm /dev/md0 --fail /dev/sdb1`
- D. `mdadm /dev/sdb1 --remove /dev/md0`
- E. `racadm --remove /dev/sdb1`
- F. `racadm --fail /dev/sdb1`



**Correct Answer: AC**

**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 221**

A systems administrator needs to connect to a remote Linux machine to run system updates from within a graphical interface. Which of the following should the administrator use?

- A. MATE
- B. Wayland
- C. VNC
- D. Unity

**Correct Answer: C**

**Section: (none) Explanation**

**Explanation/Reference:**

**QUESTION 222**

When requesting SSH access to a remote system, a user accidentally emailed the `id_rsa` key to the administrator. Which of the following should the user do NEXT?

- A. Run the `ssh-add` command to add the remote system to `known_hosts`.
- B. Ask the administrator to run `chmod 600 id_rsa` on the remote system.
- C. Delete `id_rsa` key file and send the `id_rsa.pub` key file instead.
- D. Stop using that key and run `ssh-keygen` to generate a new key pair.

**Correct Answer:** D  
**Section:** (none) **Explanation**

**Explanation/Reference:**

**QUESTION 223** An administrator receives an alarm because the disk of one of the servers is running out of space. Which of the following commands can be used to see the space that each partition is using?

- A. `df -h`
- B. `du -scg /`
- C. `fdisk -l`
- D. `fsck /`

**Correct Answer:** A  
**Section:** (none) **Explanation**

**Explanation/Reference:**