RHCE Q&As

Red Hat Certified Engineer — RHCE

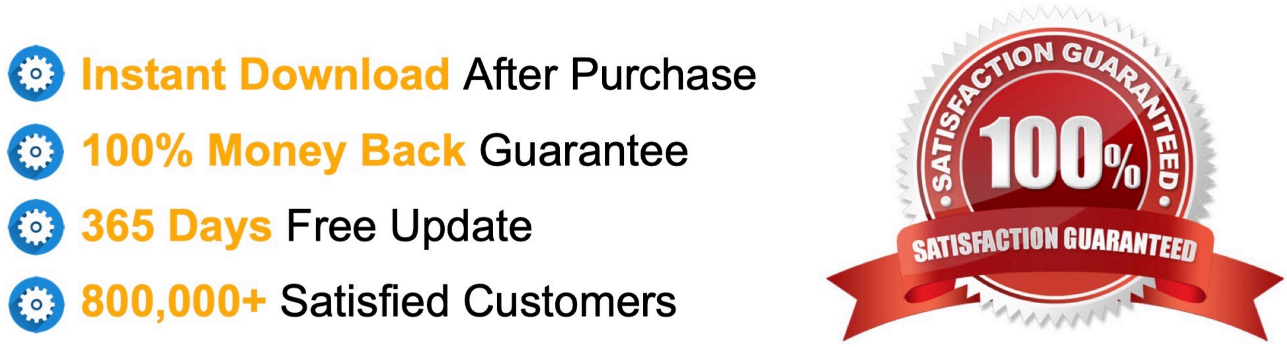
Pass RedHat RHCE Exam with 100% Guarantee

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

https://www.leads4pass.com/rhce.html

100% Passing Guarantee
100% Money Back Assurance

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


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

QUESTION 1

SIMULATION

Add a cron schedule to take full backup of /home on every day at 5:30 pm to /dev/st0 device.

A. explanation

Correct Answer: A

1.

 vi /var/schedule 30 17 * * * /sbin/dump -0u /dev/st0 /dev/hda7

2.

 crontab /var/schedule

3.

 service crond restart

We can add the cron schedule either by specifying the scripts path on /etc/crontab file or by creating on text file on crontab pattern. cron helps to schedule on recurring events. Pattern of cron is: Minute Hour Day of Month Month Day of Week

Commands

0-59 0-23 1-31 1-12 0-7 where 0 and 7 mean Sunday.

Note * means every. To execute the command on every two minutes */2.

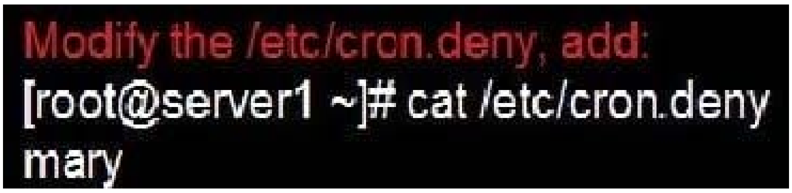
QUESTION 2

SIMULATION

Prevent Mary from performing user configuration tasks in your system.

A. explanation

Correct Answer: A



Modify the /etc/cron.deny, add:

```
[root@server1 ~]# cat /etc/cron.deny
mary
```

Conclusions:

1. I find that it is common to add various service access limits in the exam RHCE. The exercises like: require one network segment can be accessed another network segments can not be accessed, the following are some conclusions for

various service:

tcp_wrappers:/etc/hosts.allow,/etc/hosts.deny

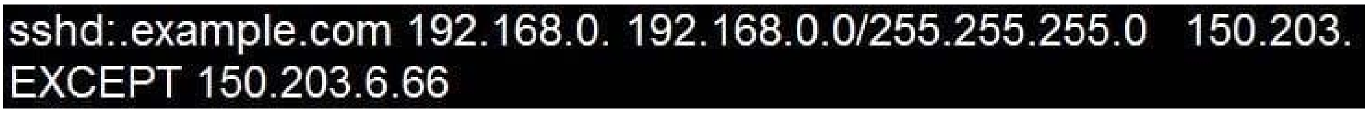
tcp_wrappers can filter the TCP\\'s accessing service. TCP whether has the filtering function which depends on this service whether use the function library of tcp_wrappers, or this service whether has the xinetd process of starting function of

tcp_wrappers. tcp_wrappers\\'s main configuration file is /etc/hosts.allow,/etc/ hosts.deny.

And the priority of the documents in hosts. allow is higher than hosts. deny. Visit will be passed if no match was found.

sshd,vsftpd can use the filtering service of tcp_wrappers.

Configuration example:

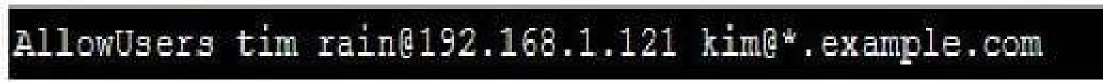


```
sshd:.example.com 192.168.0. 192.168.0.0/255.255.255.0   150.203.
EXCEPT 150.203.6.66
```

Notice:

The two configuration files\\' syntax can refer to hosts_access (5) and hosts_options(5) sshd_config There are four parameters in this configuration file: DenyUsers, AllowUsers, DenyGroups, AllowGroups, they are used to limit some users or

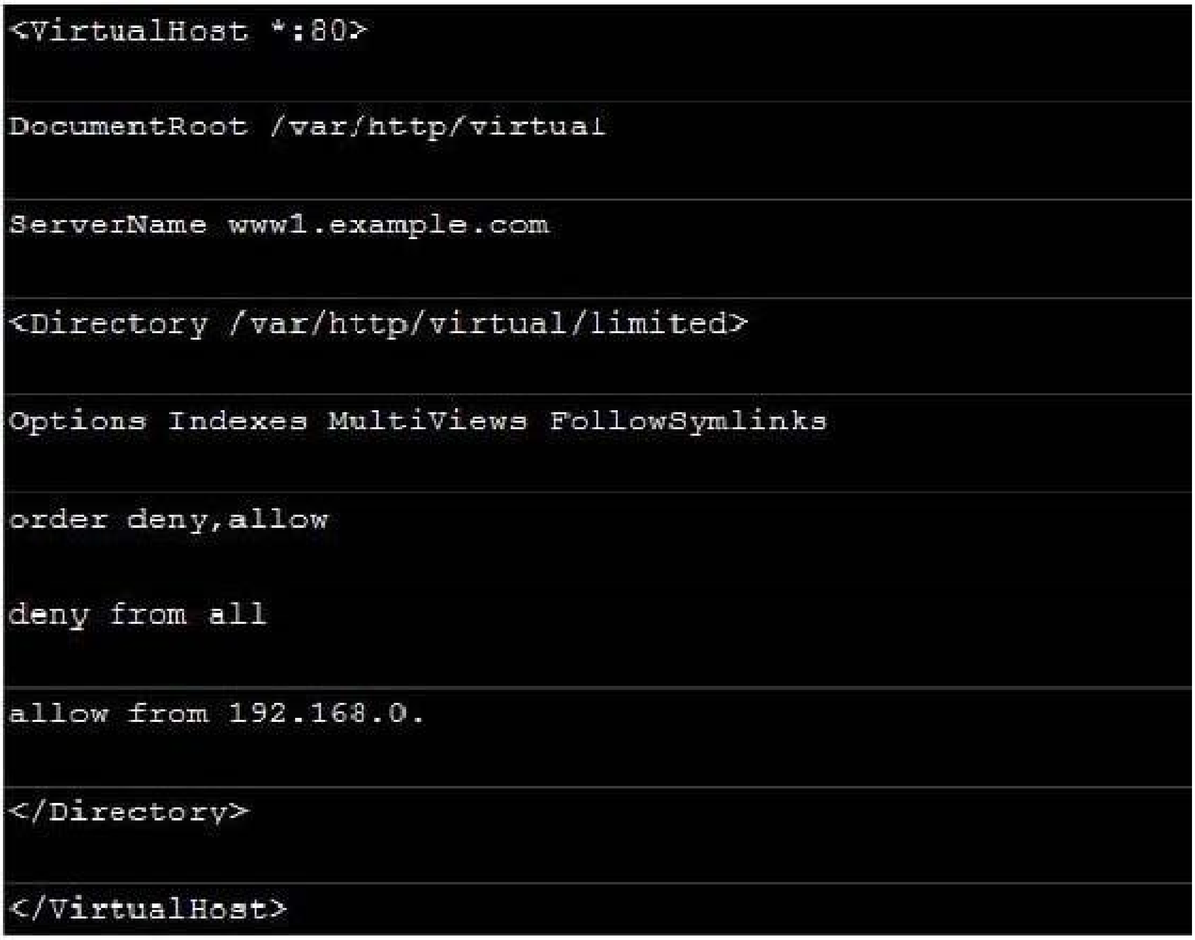
user groups to proceed Remote Login through the SSH. These parameters\\' priority level is DenyUsers->AllowUsers->DenyGroups->AllowGroups Configuration example:



```
AllowUsers tim rain@192.168.1.121 kim@*.example.com
```

httpd Service

Through the /etc/httpd/conf/httpd.conf in parameters, can add to control the url access. Just as:



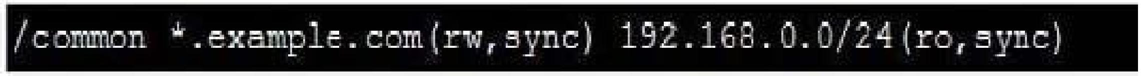
```
<VirtualHost *:80>

DocumentRoot /var/http/virtual

ServerName www1.example.com

<Directory /var/http/virtual/limited>

Options Indexes MultiViews FollowSymlinks

order deny,allow

deny from all

allow from 192.168.0.

</Directory>

</VirtualHost>
```

Notice:

So pay attention, deny\\'s and allow\\'s priority level in order deny,allow is: the backer has the higher priority level. But here, allow\\'s priority has a higher priority level.

nfs Service

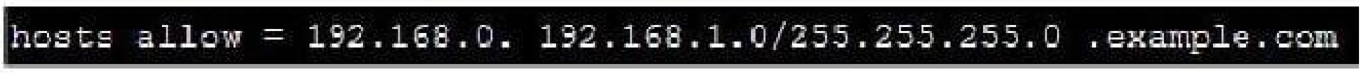
nfs service directly control the visits through file /etc/exports, just as:



```
/common *.example.com(rw,sync) 192.168.0.0/24(ro,sync)
```

samba Service

Parameter hosts allow in /etc/samba/smb.conf which is used as Access Control, just as:



```
hosts allow = 192.168.0. 192.168.1.0/255.255.255.0 .example.com
```

2.

Paying attention to use Mount parameters: _netdev,defaults when you are mounting ISCSI disk.

3.

Stop the NetworkManager /etc/init.d/NetworkManager stop chkconfig NetworkManager off

4.

When you are deploying ifcfg-ethX, add parameters: PEERDNS=no

5.

Empty the firewall in RHCSA RHCE:

6.

Narrow lv steps:

7.

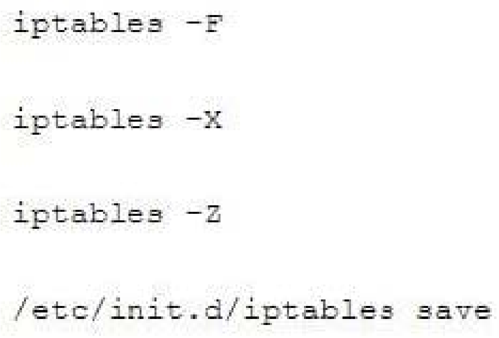
Mount the using command - swap which is newly added in /etc/fstab

8.

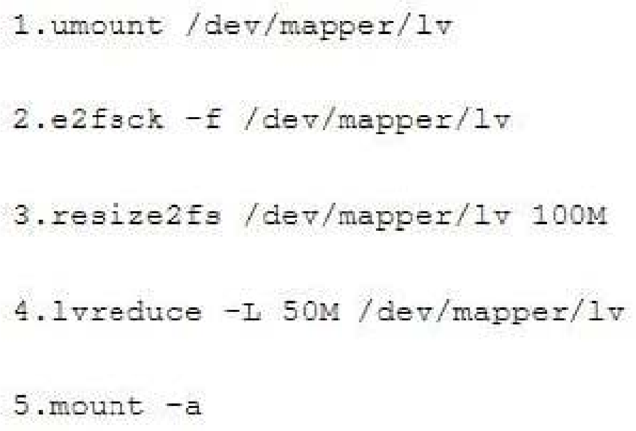
If Verification is not passed when you are installing software, can import public key: rpm import /etc/pki/rpm.../...release and so on. In yum.repo, you also can deploy gpgkey, for example, gpgkey=/etc/pki/rpm.../...release

9.

When you are using "Find" command to search and keep these files, paying attention to use cp -a to copy files if you use user name and authority as your searching methods.



```
iptables -F

iptables -X

iptables -Z

/etc/init.d/iptables save
```



```
1.umount /dev/mapper/lv

2.e2fsck -f /dev/mapper/lv

3.resize2fs /dev/mapper/lv 100M

4.lvreduce -L 50M /dev/mapper/lv

5.mount -a
```

QUESTION 3

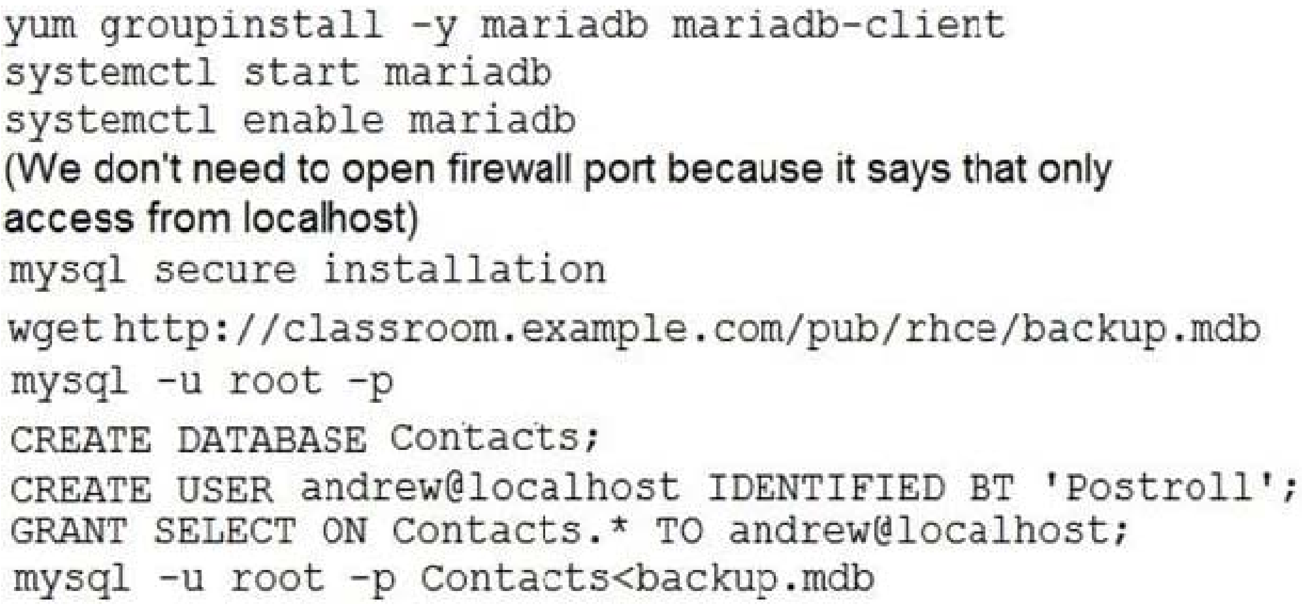
SIMULATION

There were two systems: system1, main system on which most of the configuration take place system2, some configuration here

MariaDB Restore a database on serverX from the backup file http://classroom.com/pub/rhce/backup.mdb The database name should be Contacts. It should be access only within the localhost Set a password for root user as "Postroll". Other than the root user, the user Andrew is able to read the query from the above mentioned database. The user should be authenticated with the password as "Postroll".

A. explanation

Correct Answer: A



```
yum groupinstall -y mariadb mariadb-client
systemctl start mariadb
systemctl enable mariadb
(We don't need to open firewall port because it says that only
access from localhost)
mysql secure installation
wget http://classroom.example.com/pub/rhce/backup.mdb
mysql -u root -p
CREATE DATABASE Contacts;
CREATE USER andrew@localhost IDENTIFIED BT 'Postroll';
GRANT SELECT ON Contacts.* TO andrew@localhost;
mysql -u root -p Contacts<backup.mdb
```

QUESTION 4

SIMULATION

You access the iscsi shared storage. The storage server ip is 172.24.30.100. Separate of 1500M space, format as ext3 file system, mount under /mnt/data, and make sure the root-start automatically mount.

A. explanation

Correct Answer: A

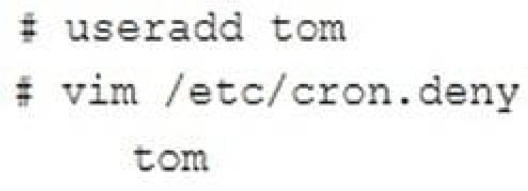
QUESTION 5

SIMULATION

Configure cron and don\\'t allow the user tom to use.

A. explanation

Correct Answer: A



```
# useradd tom
# vim /etc/cron.deny
     tom
```

RHCE Practice Test RHCE Study Guide RHCE Braindumps