



EX300^{Q&As}

Red Hat Certified Engineer (RHCE)

Pass RedHat EX300 Exam with 100% Guarantee

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

<https://www.pass4itsure.com/ex300.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



**QUESTION 1****SIMULATION**

There are two different networks 192.168.0.0/24 and 192.168.1.0/24. Where 192.168.0.254 and

192.168.1.254 IP Address are assigned on Server. Verify your network settings by pinging 192.168.1.0/24 Network\\'s Host.

Correct Answer: Please see explanation

Explanation:

```
1. vi /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=station?.example.com
GATEWAY=192.168.0.254
2. service network restart
Or
1. vi /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
ONBOOT=yes
BOOTPROTO=static
IPADDR=X.X.X.X
NETMASK=X.X.X.X
GATEWAY=192.168.0.254
2. ifdown eth0
3. ifup eth0
```

QUESTION 2**SIMULATION**

Make Secondary belongs the jeff and marion users on sysusers group. But harold user should not belongs to sysusers group.

Correct Answer: Please see explanation

Explanation:

1.

usermod -G sysusers jeff



2.

`usermod -G sysuser marion`

3.

Verify by reading `/etc/group` file

Note:

Using `usermod` command we can make user belongs to different group. There are two types of group one primary and another is secondary. Primary group can be only one but user can belong to more than one group as secondary.

`usermod -g groupname username` - To change the primary group of the user. `usermod -G groupname username` - To make user belongs to secondary group.

QUESTION 3

SIMULATION

RHCE Test Configuration Instructions

Information for the two systems you will use in test is the following:

`system1.group3.example.com`: is one of the main sever. `system2.group3.example.com`: mainly used as a client. Password for both of the two systems is `atenorth` System's IP is provided by DHCP, you can regard it as normal, or you can reset to Static IP in accordance

with the following requirements:

`system1.group3.example.com`: 172.24.3.5 `system2.group3.example.com`: 172.24.3.10

The subnet mask is 255.255.255.0

Your system is a member of DNS domain `group3.example.com`. All systems in DNS domain `group3.example.com` are all in subnet 172.24.3.0/255.255.255.0, the same all systems in this subnet are also in `group3.example.com`, unless specialized, all network services required to be configured can be accessed by systems of domain `group3`.

`host.group3.example.com` provides a centralized authentication service domain `GROUP3.EXAMPLE.COM`, both `system1` and `system2` have already been pre-configured to be the client

```
krishna (password: atenorth)
sergio (password: atenorth)
kaito (password: atenorth)
```

for this domain, this domain provides the following user account:

Firewall is enabled by default, you can turn it off when deemed appropriate, other settings about firewall may be in separate requirements.

Your system will be restarted before scoring, so please ensure that all modifications and service configurations you made still can be operated after the restart without manual intervention, virtual machine instances of all examinations must be able to enter the correct multi-user level after restart without manual assistance, it will be scored zero if the test using virtual machine system cannot be restarted or be properly restarted.



Corresponding distribution packages for the testing using operating system Red Hat Enterprise Linux version can be found in the following link: <http://server1.group3.example.com/rhel>

Part of the requirements include host security, ensure your host security limit does not prevent the request to allow the host and network, although you correctly configured the network service but would have to allow the host or network is blocked, this also does not score.

You will notice that some requirements which clearly do not allow services be accessed by service domain my133t.org, systems of this domain are in subnet 172.25.1.0/252.255.255.0, and systems of these subnets also belong to my 133t.org domain.

PS: Notice that some test questions may depend on other exam questions, for example, you might be asked to perform a series of restrictions on a user, but this user creation may be required in other questions. For convenient identification, each exam question has some radio buttons to help you identify which questions you have already completed or not completed. Certainly, you do not need to care these buttons if you don't need them.

Configure Security Web Service

Configure a TLS encryption for the site <http://system1.domain11.example.com>, encrypt/, get a signed certificate from <http://host.domain11.example.com/materials/system1.crt>. Get the certificate key from <http://host.domain11.example.com/materials/system1.key>. Get the signature authorization information of the certificate from <http://host.domain11.example.com/materials/domain11.crt>

Correct Answer: Please see explanation

Explanation:

QUESTION 4

SIMULATION

Create the directory /storage and group owner should be the sysusers group.

Correct Answer: Please see explanation

Explanation:

chgrp sysusers /storage

Verify using ls -ld /storage command.

You should get like drwxr-x--- 2 root sysusers 4096 Mar 16 17:59 /storage chgrp command is used to change the group ownership of particular files or directory.

Another way you can use the chown command.

chown root:sysusers /storage

QUESTION 5

SIMULATION Prevent Mary from performing user configuration tasks in your system.



Correct Answer: Please see explanation

Explanation:

```
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.

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

Configuration example:

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

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

Configuration example:

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 stopchkconfig 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
```

[Latest EX300 Dumps](#)

[EX300 PDF Dumps](#)

[EX300 Study Guide](#)