



EX300^{Q&As}

Red Hat Certified Engineer (RHCE)

Pass home 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 home
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



**QUESTION 1****SIMULATION**

In accordance with the following requirements, share /common directory through smb service. -- your sub service must be in the SAMBA working-set -- the shared name of common is common -- the common share just can be shared by the customers in the example.com domain -- the common must be available for browsing -- mary must be able to login to the SMB share and for read operation, "password" is the secret code if it need to be verified.

Correct Answer: Please see explanation

Explanation:

```
[root@server1 iscsi]# grep -v "^\\s*#" /etc/samba/smb.conf
| grep -v
"^\\s*;" | grep -v "^\\s*$"
[global]
workgroup = SAMBA
server string = Samba Server Version %v
hosts allow = 127. 192.168.0.
security = user passdb
backend = tdbsam
[common]
comment = Public
Stuff path = /common
public = no
browseable = yes
printable = no read
only = mary

Add SMB Mary users
smbpasswd -a mary
Modify the security context of /common directory
chcon -R -t samba_share_t /common
```

QUESTION 2



SIMULATION

There were two systems:

system1, main system on which most of the configuration take place

system2, some configuration here

Configure port forwarding.

Configure server X to forward traffic incoming on port 80/tcp from source network

172.25.X.0/255.255.255.0 to port on 5243/tcp.

Correct Answer: Please see explanation

Explanation:

```
firewall-cmd --add-rich-rule='rule family="ipv4" source
address="172.25.1.0/24" forward-port port="5423" protocol="tcp" to-
port="80" --permanent
firewall-cmd --reload
```

QUESTION 3

SIMULATION

Configure the nfs server, share the /common directory to domain30.example.com, and allow client to have the root user right when access as a root user.

Correct Answer: Please see explanation

Explanation:

```
# yum install -y nfs
# chkconfig nfs on
# chkconfig rpcbind on
# vim /etc/exports
    /common 172.24.30.0/255.255.255.0(rw,no_root_squash)
# showmount -e 172.16.30.5
# mount -t nfs 172.16.30.5:/common /mnt (Test)
```

QUESTION 4



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

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

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 NFS service



Configure the NFS service on the system1, as required:

1.

Share the directory /public in read only way, just can be accessed by systems in domain11.example.com at the same time.

2.

Share the directory /protected in read and write way, Kerberos security encryption required, you can use the key provided by the following URL: http://host.domain11.example.com/materials/nfs_server.keytab

3.

The directory /protected should contain the sub directory named project and the owner name is deepak;

4.

User deepak can access /protected/project in read and write ways

Correct Answer: Please see explanation

Explanation: system1:



```
vim /etc/exports
/protected 172.24.11.0/24(rw,sync,sec=krb5p)
/public 172.24.11.0/24(ro,sync)
wget -O /etc/krb5.keytab
http://host.domain11.example.com/materials/nfs_server.keytab
vim /etc/sysconfig/nfs
RPCNFSDARGS="-V 4.2 "
:wq
systemctl restart nfs
systemctl start nfs-secure-server
systemctl enable nfs-secure-server
exportfs -ra
showmount -e
firewall-cmd --add-service=nfs --permanent
firewall-cmd --add-service=rpc-bind --permanent
firewall-cmd --add-service=mountd --permanent
systemctl restart firewalld
mkdir -p /protected/project
chown deepak /protected/project/
ll /protected/
chcon -R -t public_content_t /protected/project/
```

QUESTION 5

SIMULATION

There were two systems:

system1, main system on which most of the configuration take place

system2, some configuration here

Configure repository.

Create a Repository for your virtual machines. The URL is <http://station.network.0.example.com/content/>

rhel7.0/x86_64/dvd

Correct Answer: Please see explanation



Explanation:

```
# vim /etc/yum.repos.d/local.repo
```

```
[localrepo]
name = Local Repo for RHCE Exam
baseurl = http://station.network0.example.com/content/rhel7.0/x86_64/dvd
gpgcheck = 0
enabled = 1
```

Save and Exit (:wq) Then run this:

```
# yum clean all
# yum repolist
```

QUESTION 6

SIMULATION

There were two systems:

system1, main system on which most of the configuration take place

system2, some configuration here

SMTP Configuration.

Configure the SMTP mail service on serverX and desktopX which relay the mail only from local system through station.network0.example.com, all outgoing mail have their sender domain as example.com. Ensure that mail should not store locally.

Verify the mail server is working by sending mail to a natasha user.

Check the mail on both serverX and desktopX with the below URL

<http://station.network0.example.com/system1> <http://station.network0.example.com/system2>

Correct Answer: Please see explanation

Explanation:



```
vim /etc/postfix/main.cf
inet_interfaces = loopback-only

mydestination =
muorigin=example.com
mynetworks = 127.0.0.0/8, [::1]/128
relayhost = [station.network0.example.com]
local_transport = error: local delivery dosabled
```

QUESTION 7

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

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

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 Link Aggregation

Configure a link between system1.group3.example.com and system2. group3.example.com as required: This link uses interfaces eth1 and eth2 This link still can work when one interface fails This link uses the following address 172.16.3.20/255.255.255.0 on system1 This link uses the following address 172.16.3.25/255.255.255.0 on system2 This link remains normal after the system is restarted

Correct Answer: Please see explanation

Explanation:

If you forget how to write the name, you can search examples in /var/share/doc/team-1.9/ example_configs/

```
nmcli connection add con-name team0 type team ifname team0 config
 '{"runner":{"name":"activebackup"}}'
nmcli con modify team0 ipv4.addresses '172.16.11.25/24'
nmcli connection modify team0 ipv4.method manual
nmcli connection add type team-slave con-name team0-p1 ifname eth1
master team0
nmcli connection add type team-slave con-name team0-p2 ifname eth2
master team0
nmcli connection up team0

nmcli con up team0-p1
nmcli con up team0
```

QUESTION 8

SIMULATION

According to the following requirements, deploy your ftp login rule:



Users in example.com domain must be able to login to your ftp server as an anonymous user.

But users outside the example.com domain are unable to login to your server

Correct Answer: Please see explanation

Explanation:

```
[root@server1 ~]# grep vsftpd /etc/hosts.deny
vsftpd: .example.com

[root@server1 ~]# grep vsftpd /etc/hosts.deny
vsftpd:ALL

/etc/vsftpd/vsftpd.conf:
anonymous_enable=YES
```

QUESTION 9

SIMULATION

There were two systems:

system1, main system on which most of the configuration take place

system2, some configuration here

Script2.

Create a script on serverX called /root/createusers

When this script is called with the argument, it should add all the users from the file

Download the file from <http://station.network0.example.com/pub/testfile>

All users should have the login shell as /bin/false, password not required

When this script is called with any other argument, it should print the message as "Input File Not Found"

When this script is run without any argument, it should display "Usage:/root/createusers"

NOTE: if the users are added no need to delete

Correct Answer: Please see explanation

Explanation:



```
cd /root
wget [url="http://station.network0.example.com/pub/testfile"]http://station.network0.example.com/pub/testfile[/url]

vim /root/createusers

#!/bin/bash
a=""
case $@ in
testfile)

    for user in $(cat $1);do
    echo "Adding this user:" $user
    useradd -s /bin/false $user
    done
    ;;
$a)
    echo "Usage: /root/createusers"
    ;;
*)
    echo "Input File Not Found"
    ;;
esac

chmod +x /root/createusers
```

QUESTION 10

SIMULATION Configure ssh to allow user harry to access, reject the domain t3gg.com (172.25.0.0/16) to access.

Correct Answer: Please see explanation

Explanation:



```
# yum install -y sshd
# chkconfig sshd on
# vim /etc/hosts.deny
    sshd: 172.25.0.0/16
# service sshd restart
```

Use iptables:

```
# chkconfig iptables on
# iptables -F
# iptables -X
# iptables -Z
# iptables -nvL
# iptables -A INPUT -s 172.25.0.0/16 -p tcp --dport 22 -j REJECT
# services iptables save
# iptables -nvL
# cat /etc/services (check port)
```

QUESTION 11**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 12



SIMULATION Connect to the email server and send email to admin, and it can be received by harry.

Correct Answer: Please see explanation

Explanation:

```
# vim /etc/aliases
admin: harry
# newaliases
```

QUESTION 13

SIMULATION

There were two systems:

system1, main system on which most of the configuration take place

system2, some configuration here

Secured webserver.

Configure the website <https://serverX.example.com> with TLS

SSLCertificate file <http://classroom.example.com/pub/rhce/tls/certs/system1.networkX.crt>

SSLCertificatekeyfile <http://classroom.example.com/pub/rhce/tls/private/system1.networkX.key>

SSL CA certificate file <http://classroom.example.com/pub/example-ca.crt>

Correct Answer: Please see explanation

Explanation:



```
yum install -u mod_ssl

wget http://classroom.example.com/pub/rhce/tls/certs/system1.network1.crt

wget http://classroom.example.com/pub/rhce/tls/private/system1.network1.key

wget http://classroom.example.com/pub/example-ca.crt

mv system1.network1.crt /etc/pki/tls/certs/
mv system1.network1.key /etc/pki/tls/private/
mv example-ca.crt /etc/pki/tls/certs/

# Very Important, Fix the Permission on Key File
chmod 0600 /etc/pki/tls/private/system1.network1.key

vim /etc/httpd/conf.d/server1.conf

(Add the following)

<VirtualHost *:443>

ServerName server1.example.com
DocumentRoot /var/www/html

SSLEngine on
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
#SSLCertificateChainFile /etc/pki/tls/certs/server-chain.crt

</VirtualHost>

firewall-cmd --permanent --add-service=https
firewall-cmd --reload
```

QUESTION 14

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
```

QUESTION 15

SIMULATION

Configure the ftp to allow anonymously download the directory /var/ftp/pub, and reject the domain t3gg.com to access.

Correct Answer: Please see explanation

Explanation:



```
# yum install -y vsftpd
# chkconfig vsftpd on
# services vsftpd start

# vim /etc/hosts.deny
vsftpd: 172.25.0.0/16
```

OR

```
# iptables -A INPUT -s 172.25.0.0/16 -p tcp -dport 20:21 -j REJECT
# services iptables save
```

[Latest EX300 Dumps](#)

[EX300 Exam Questions](#)

[EX300 Braindumps](#)