PassQueen
a.k.a dumpsqueen.com

Red Hat Certified Engineer – RHCE (v6+v7)

RedHat EX300

Version Demo

Total Demo Questions: 18

Total Premium Questions: 187

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, System configuration and management	51
Topic 2, Networking	18
Topic 3, Network services	97
Topic 4, Security	21
Total	187

QUESTION NO: 1 - (SIMULATION)

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 the Access to the Web Content

Create a directory private under the directory DocumentRoot in the web server on the system1, requirements are the following:

- Download a file copy to this directory from http://rhgls.domain11.example.com/materials/private.html and rename it as index.html.

- Don’t make any changes to this file content
- Any users from the system1 can browse the content of the private, but cannot access this directory content through other systems

ANSWER: See the explanation for the answer

Explanation:

On `system1.group3.example.com`, create the protected directory below Apache's DocumentRoot, download the required file as `index.html`, and restrict Apache access to requests originating on system1 only.

```
sudo mkdir -p /var/www/html/private
sudo curl -o /var/www/html/private/index.html \
  http://rhgls.domain11.example.com/materials/private.html
sudo chmod 755 /var/www/html/private
sudo chmod 644 /var/www/html/private/index.html
sudo restorecon -RFv /var/www/html/private
```

Create `/etc/httpd/conf.d/private.conf` with the following content:

```
<Directory "/var/www/html/private">
    AllowOverride None
    Require ip 172.24.3.5 127.0.0.1 ::1
</Directory>
```

This permits requests sent from system1's assigned address and local loopback addresses, while all requests from every other system are denied by default.

Enable and start Apache so the configuration survives reboot:

```
sudo systemctl enable --now httpd
sudo apachectl configtest
sudo systemctl reload httpd
```

Verify locally on system1:

```
curl http://system1.group3.example.com/private/
```

The page must be available locally, while a request from `system2` (or any other host) to `http://system1.group3.example.com/private/` must receive HTTP `403 Forbidden`.

QUESTION NO: 2 - (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:

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://systeml.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

ANSWER: See the explanation for the answer

Explanation:

Install and enable Apache with TLS support, download the supplied signed certificate, private key, and CA/signing certificate, then configure an HTTPS virtual host for `system1.domain11.example.com`. (The question's `systeml` is interpreted as `system1`.)

```
dnf -y install httpd mod_ssl
systemctl enable --now httpd

mkdir -p /etc/pki/tls/certs /etc/pki/tls/private
curl -o /etc/pki/tls/certs/system1.crt
http://host.domain11.example.com/materials/system1.crt
curl -o /etc/pki/tls/private/system1.key
http://host.domain11.example.com/materials/system1.key
curl -o /etc/pki/tls/certs/domain11.crt
http://host.domain11.example.com/materials/domain11.crt
chmod 600 /etc/pki/tls/private/system1.key
restorecon -Rv /etc/pki/tls
```

Create the encrypted site configuration. If `/encrypt` is intended by the question as the site content directory, use it as the document root:

```
mkdir -p /encrypt
restorecon -RFv /encrypt
```

```
cat > /etc/httpd/conf.d/system1-domain11-ssl.conf <<'EOF'
<VirtualHost *:443>
    ServerName system1.domain11.example.com
    DocumentRoot /encrypt

    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/system1.crt
    SSLCertificateKeyFile /etc/pki/tls/private/system1.key
    SSLCertificateChainFile /etc/pki/tls/certs/domain11.crt

    <Directory /encrypt>
        Require all granted
    </Directory>
</VirtualHost>
EOF

httpd -t
systemctl restart httpd
```

Allow HTTPS permanently through the firewall (or, if the exam permits it, the firewall may instead be disabled):

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

Verify that the service presents the supplied certificate:

```
curl -vk https://system1.domain11.example.com/
```

If Apache reports that `SSLCertificateChainFile` is unsupported on the particular supplied Apache release, append the CA certificate to the server certificate instead and remove that directive:

```
cat /etc/pki/tls/certs/domain11.crt >> /etc/pki/tls/certs/system1.crt
# Remove SSLCertificateChainFile from the virtual-host configuration.
systemctl restart httpd
```

QUESTION NO: 3 - (SIMULATION)

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

ANSWER: See the explanation for the answer

Explanation:

On `system1`, configure Apache HTTP Server with TLS for `https://serverX.example.com`. Replace `X` with the network number assigned in the question if it is not literally `X`.

```
dnf install -y httpd mod_ssl
systemctl enable --now httpd

curl -o /etc/pki/tls/certs/system1.networkX.crt \
  http://classroom.example.com/pub/rhce/tls/certs/system1.networkX.crt
```

```
curl -o /etc/pki/tls/private/system1.networkX.key \
  http://classroom.example.com/pub/rhce/tls/private/system1.networkX.key
curl -o /etc/pki/tls/certs/example-ca.crt \
  http://classroom.example.com/pub/example-ca.crt

chmod 600 /etc/pki/tls/private/system1.networkX.key
restorecon -Rv /etc/pki/tls
```

Create a dedicated TLS virtual-host configuration, for example `/etc/httpd/conf.d/serverX-ssl.conf`:

```
<VirtualHost *:443>
    ServerName serverX.example.com
    DocumentRoot /var/www/html

    SSLEngine on
    SSLCertificateFile /etc/pki/tls/certs/system1.networkX.crt
    SSLCertificateKeyFile /etc/pki/tls/private/system1.networkX.key
    SSLCACertificateFile /etc/pki/tls/certs/example-ca.crt

    ErrorLog logs/serverX-ssl-error_log
    CustomLog logs/serverX-ssl-access_log combined
</VirtualHost>
```

Validate the configuration, start/reload Apache, and allow HTTPS through the firewall:

```
apachectl configtest
systemctl reload httpd
firewall-cmd --permanent --add-service=https
firewall-cmd --reload
```

Verify from `system2` (or any client that can resolve `serverX.example.com`):

```
curl --cacert http://classroom.example.com/pub/example-ca.crt \
  https://serverX.example.com/
```

The required TLS directives are `SSLCertificateFile` pointing to `system1.networkX.crt`, `SSLCertificateKeyFile` pointing to `system1.networkX.key`, and `SSLCACertificateFile` pointing to `example-ca.crt`.

QUESTION NO: 4 - (SIMULATION)

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.

Share directories via SMB.

Configure the SMB service on the system1.

Your SMB server must be a member of the STAFF Working Group.

Share the folder /common and the name must be common.

Only clients of domain11.example.com can access the common share.

Common must be able to browse.

User Andy must be able to read the content of the share, if necessary, verification code is redhat.

ANSWER: See the explanation for the answer

Explanation:

Perform the SMB configuration on `system1.group3.example.com`. Install Samba, configure the server workgroup as `STAFF`, and restrict the share by the client DNS domain.

```
yum -y install samba samba-client policycoreutils-python
mkdir -p /common
chmod 0755 /common
```

Ensure the Samba account exists for the local UNIX account `andy` (use the exact account spelling present on the system). Set its Samba password to `redhat` if prompted by the task:

```
id andy || useradd andy
smbpasswd -a andy
# Enter redhat twice
```

Configure `/etc/samba/smb.conf` with the following relevant settings (existing unrelated global settings may remain):

```
[global]
        workgroup = STAFF
        security = user

[common]
        path = /common
        browseable = yes
        read only = yes
        valid users = andy
        hosts allow = .domain11.example.com
        hosts deny = ALL
```

`hosts allow = .domain11.example.com` permits clients whose verified host names are in that DNS domain; `hosts deny = ALL` ensures clients outside that domain cannot access the share. The `valid users` entry makes Andy an authenticated reader; `read only = yes` prevents writes.

Apply the SELinux label and enable the service permanently:

```
semanage fcontext -a -t samba_share_t '/common(/.*)?'
restorecon -RFv /common
systemctl enable --now smb nmb
firewall-cmd --permanent --add-service=samba
firewall-cmd --reload
```

Optionally validate the configuration before finishing:

```
testparm
pdbedit -L | grep '^andy:'
smbclient -L localhost -U andy
```

The `common` share is browseable, is read-only for Andy, and is accessible only from hosts in `domain11.example.com`.

QUESTION NO: 5 - (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.

ANSWER: See the explanation for the answer

Explanation:

Configure Samba with the `SAMBA` workgroup, restrict the share to hosts whose names are in `example.com`, and make `mary` the only permitted Samba user.

```
# mkdir -p /common
# chmod 0755 /common

# useradd -s /sbin/nologin mary
# printf 'password\npassword\n' | smbpasswd -s -a mary

# semanage fcontext -a -t samba_share_t '/common(/.*)?'
# restorecon -RFv /common
```

Ensure the following settings exist in `/etc/samba/smb.conf`:

```
[global]
        workgroup = SAMBA

[common]
        path = /common
        browseable = yes
        read only = yes
        valid users = mary
        hosts allow = .example.com
```

The `hosts allow = .example.com` setting permits only clients in the `example.com` DNS domain. `browseable = yes` makes the share visible while browsing, and `read only = yes` gives Mary read-only access.

```
# testparm
# systemctl enable --now smb nmb
# firewall-cmd --permanent --add-service=samba
# firewall-cmd --reload
```

If the system does not provide the `nmb` unit, enabling `smb` is sufficient for the file service; `nmb` is useful for legacy NetBIOS browsing.

QUESTION NO: 6 - (SIMULATION)

SIMULATION

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

ANSWER: See the explanation for the answer

Explanation:

Prevent user `tom` from using `crontab` by adding the user to the cron deny file:

```
echo tom >> /etc/cron.deny
chmod 600 /etc/cron.deny
chown root:root /etc/cron.deny
```

If `/etc/cron.deny` does not already exist, the command creates it. Do not create `/etc/cron.allow` unless specifically required, because when that file exists it becomes the allow-list for all cron users.

Verify as the user:

```
su - tom -c 'crontab -l'
```

The command should be denied because `tom` is listed in `/etc/cron.deny`.

QUESTION NO: 7 - (SIMULATION)

SIMULATION

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

Configure smb access.

- Share the /sambadir directory via SMB on serverX
- Your SMB server must be a member of the TESTGROUP workgroup
- The share name must be data

- The data share must be available to example.com domain clients only
- The data share must be browseable
- susan must have read access to the share, authenticating with the same password “password”, if necessary
- Configure the serverX to share /opstack with SMB share name must be cluster
- The user frankenstein has readable, writeable, accessable to the /opstack SMB share - Both users should have the SMB passwd “SaniTago”

ANSWER: See the explanation for the answer

Explanation:

Perform the configuration on `serverX`. Install and enable Samba, create the directories/users, label the directories for SELinux, and open the Samba service:

```
yum -y install samba samba-client policycoreutils-python
useradd susan
useradd frankenstein
mkdir -p /sambadir /opstack
chown root:root /sambadir
chmod 0755 /sambadir
chown frankenstein:frankenstein /opstack
chmod 0700 /opstack
semanage fcontext -a -t samba_share_t '/sambadir(/.*)?'
semanage fcontext -a -t samba_share_t '/opstack(/.*)?'
restorecon -RFv /sambadir /opstack
firewall-cmd --permanent --add-service=samba
firewall-cmd --reload
```

Create the Samba accounts. The last sentence of the question explicitly says that *both users* have the SMB password `SaniTago`, so use that password for the Samba database:

```
printf 'SaniTago\nSaniTago\n' | smbpasswd -s -a susan
printf 'SaniTago\nSaniTago\n' | smbpasswd -s -a frankenstein
```

Configure `/etc/samba/smb.conf` as follows (retain any required existing global defaults):

```
[global]
        workgroup = TESTGROUP
        security = user

[data]
        path = /sambadir
        browseable = yes
        read only = yes
        valid users = susan
        hosts allow = .example.com

[cluster]
        path = /opstack
        browseable = yes
        read only = no
        writable = yes
        valid users = frankenstein
```

The `hosts allow = .example.com` entry applies only to `data`, restricting that share to clients whose source host names resolve under the `example.com` domain. Ensure forward/reverse DNS works for those clients; Samba uses name/address matching for this restriction.

Finally validate and start the service:

```
testparm
systemctl enable --now smb nmb
```

`susan` can read the browseable `data` share only, while `frankenstein` has read/write access to `cluster`.

Password wording note: the question contains a contradiction: it first says Susan authenticates with `password`, then says both users' SMB password is `SaniTago`. A Samba account cannot simultaneously have both passwords. If the Susan-specific `password` instruction is the intended grading requirement instead, replace only Susan's password command with:

```
printf 'password\npassword\n' | smbpasswd -s -a susan
```

QUESTION NO: 8 - (SIMULATION)

There were two systems:

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

system2, some configuration here

Configure selinux.

Configure your systems that should be running in Enforcing.

ANSWER: See the explanation for the answer

Explanation:

On **both system1 and system2**, configure SELinux to run in enforcing mode now and after every reboot.

```
# setenforce 1
# sed -i 's/^SELINUX=.*/SELINUX=enforcing/' /etc/selinux/config
```

Verify the running mode and persistent configuration:

```
# getenforce
Enforcing

# grep '^SELINUX=' /etc/selinux/config
SELINUX=enforcing
```

If the machine was previously configured with SELinux disabled, reboot it after changing the configuration, then verify again:

```
# reboot
# getenforce
Enforcing
```

`setenforce 1` changes the current runtime state; setting `SELINUX=enforcing` in `/etc/selinux/config` makes the setting persistent.

QUESTION NO: 9 - (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

ANSWER: See the explanation for the answer

Explanation:

Configure both `serverX` and `desktopX` as Postfix null clients: they accept mail only from the local host, rewrite locally generated sender addresses to `example.com`, and relay every message to `station.network0.example.com`. They must not consider themselves a final destination for mail.

On **each system**, install and configure Postfix:

```
dnf -y install postfix mailx
postconf -e 'myhostname = '"$(hostname -f)"
postconf -e 'myorigin = example.com'
postconf -e 'relayhost = [station.network0.example.com]'
postconf -e 'inet_interfaces = loopback-only'
postconf -e 'mynetworks = 127.0.0.0/8, [::1]/128'
postconf -e 'mydestination ='
systemctl enable --now postfix
systemctl restart postfix
```

`myorigin = example.com` makes locally submitted mail use sender addresses such as `root@example.com`.
`relayhost` sends all nonlocal mail to the specified station. Square brackets make Postfix connect directly to that host rather than looking up its MX record.
`inet_interfaces = loopback-only` and `mynetworks` ensure only the local system can submit mail.
An empty `mydestination` prevents either machine from accepting mail for local delivery/storage; messages are relayed instead.

Verify from both systems by sending a message to Natasha through the relay:

```
echo 'SMTP relay test from '"$(hostname)" | mail -s 'SMTP relay test' natasha@example.com
mailq
```

`mailq` should be empty after successful delivery (or only briefly show a message while it is being relayed). Confirm receipt using the supplied URLs:

`http://station.network0.example.com/system1` for serverX/system1
`http://station.network0.example.com/system2` for desktopX/system2

QUESTION NO: 10 - (SIMULATION)

One Logical Volume is created named as myvol under vo volume group and is mounted. The Initial Size of that Logical Volume is 400MB. Make successfully that the size of Logical Volume 200MB without losing any data. The size of logical volume 200MB to 210MB will be acceptable.

ANSWER: See the explanation for the answer

Explanation:

Reduce the mounted filesystem first, then reduce the logical volume. Do **not** run `lvreduce` before shrinking the filesystem, because that can destroy data.

Identify the mount point and confirm the filesystem type:

```
findmnt -S /dev/vo/myvol
# or
findmnt | grep myvol
```

Assuming the filesystem is ext2/ext3/ext4, replace `/mountpoint` below with the mount point returned by `findmnt`:

```
umount /mountpoint
```

```
e2fsck -f /dev/vo/myvol
resize2fs /dev/vo/myvol 210M
lvreduce -L 210M /dev/vo/myvol
mount /mountpoint

df -hT /mountpoint
lvs vo
```

The resulting LV size is `210M`, which is within the required 200--210 MB range. The existing `/etc/fstab` entry does not need to change because the LV path and mount point remain the same.

If `findmnt` shows an XFS filesystem, it cannot be shrunk in place. In that case, back up/copy its data to temporary storage, recreate a 200--210 MB ext4 filesystem/LV as appropriate, restore the data, and remount it.

QUESTION NO: 11 - (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:

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:

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 the Access to the Web Content

Create a directory private under the directory DocumentRoot in the web server on the system1, requirements are the following:

Download a file copy to this directory from http://rhgls.domain11.example.com/materials/private.html and rename it as index.html.
Don't make any changes to this file content
Any users from the system1 can browse the content of the private, but cannot access this directory content through other systems

ANSWER: See the explanation for the answer

Explanation:

On `system1`, create the private content directory under Apache's default `DocumentRoot`, download the required file as `index.html`, and restrict Apache access to requests originating from system1 itself.

```
mkdir -p /var/www/html/private
curl -o /var/www/html/private/index.html \
  http://rhgls.domain11.example.com/materials/private.html
chmod 755 /var/www/html/private
chmod 644 /var/www/html/private/index.html
restorecon -Rv /var/www/html/private
```

Create an Apache configuration file:

```
cat > /etc/httpd/conf.d/private.conf <<'EOF'
<Directory "/var/www/html/private">
    Require ip 127.0.0.1 ::1 172.24.3.5
</Directory>
EOF
```

This permits requests from the local loopback interface and from system1's own address, while denying requests sent from all other systems.

```
apachectl configtest
systemctl enable --now httpd
systemctl reload httpd
```

Verify locally on system1:

```
curl http://localhost/private/
curl http://172.24.3.5/private/
```

A request from system2 to `http://system1.group3.example.com/private/` must be denied (normally HTTP 403).

QUESTION NO: 12 - (SIMULATION)

Given the kernel of a permanent kernel parameters: sysctl=1.

It can be shown on cmdline after restarting the system.

Kernel of /boot/grub/grub.conf should be a34dded finally, as:

ANSWER: See the explanation for the answer

Explanation:

Add `sysctl=1` to the end of the active `kernel` line in `/boot/grub/grub.conf`. For example:

```
kernel /vmlinuz-$(uname -r) ro root=/dev/mapper/vg_root-lv_root sysctl=1
```

On systems using a fixed kernel path, preserve the existing options and append only the requested parameter:

```
kernel /vmlinuz-... ro root=... sysctl=1
```

Reboot the host. After it starts, verify that the parameter was passed by GRUB:

```
cat /proc/cmdline
```

The output must include `sysctl=1`.

QUESTION NO: 13 - (SIMULATION)

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.

Implement/configure a Web Service.

Configure a site http://systeml. domain11.example.com/ on the system1, then execute the following steps:

(1) Download file from http://rhgls.domain11.example.com/materials/station.html and rename this files index.html, don't modify the file contents;

(2) Copy the file index.html to your web server's DocumentRoot directory

(3) Clients from domain group3.example.com can access to this web service

(4) Clients from domain my133t.org deny access to this web service

ANSWER: See the explanation for the answer

Explanation:

On `system1`, install and enable Apache, download the file without changing it, and restrict Apache authorization by source network. The requested name appears as `systeml.domain11.example.com` (lowercase letter `l`); configure that name exactly, and an alias for the likely intended `system1` spelling is harmless.

```
# dnf -y install httpd
# systemctl enable --now httpd

# curl -o /var/www/html/index.html \
  http://rhgls.domain11.example.com/materials/station.html
# restorecon -Rv /var/www/html
```

Replace the stock Apache authorization for `/var/www`. Do **not** leave `Require all granted`, since that would also permit the my133t.org clients.

```
# vi /etc/httpd/conf/httpd.conf
```

Change the standard section to the following (the relevant result is shown):

```
<Directory "/var/www">
    AllowOverride None
    Require ip 172.24.3.0/24
</Directory>
```

Create a named virtual host:

```
# cat > /etc/httpd/conf.d/systeml.conf <<'EOF'
<VirtualHost *:80>
    ServerName systeml.domain11.example.com
    ServerAlias system1.domain11.example.com
    DocumentRoot /var/www/html
</VirtualHost>
EOF

# apachectl configtest
# systemctl restart httpd
```

Permit HTTP through the enabled firewall permanently:

```
# firewall-cmd --permanent --add-service=http
# firewall-cmd --reload
```

`Require ip 172.24.3.0/24` permits every client in `group3.example.com`, whose stated subnet is 172.24.3.0/24. It denies 172.25.1.0/24 (the `my133t.org` subnet) and all other non-group3 sources with HTTP 403. The `httpd` service is enabled, so this remains functional after reboot.

QUESTION NO: 14 - (SIMULATION)

There were two systems:

system1, main system on which most of the configuration take place
system2, some configuration here

Configure NFS mount.

Mount /nfsshare directory on desktopX under /public directory persistently at system boot time.
Mount /nfssecure/protected with krb5p secured share on desktopX beneath /secure/protected provided with keytab station.network0.example.com/pub/keytabs/desktopX.keytab">http://station.network0.example.com/pub/keytabs/desktopX.keytab
The user harry is able to write files on /secure directory

ANSWER: See the explanation for the answer

Explanation:

On the NFS server (use the system that owns `/nfsshare` and `/nfssecure/protected`), export the shares. The secure export must explicitly permit only Kerberos privacy (`krb5p`):

```
cat >> /etc/exports <<'EOF'
/nfsshare              *(rw,sync)
/nfssecure/protected    *(rw,sync,sec=krb5p)
EOF
exportfs -rav
systemctl enable --now nfs-server
```

On `desktopX`, install the supplied host keytab, create the mount points, and make the parent `/secure` directory writable by `harry`:

```
curl -o /etc/krb5.keytab \
  http://station.network0.example.com/pub/keytabs/desktopX.keytab
chmod 600 /etc/krb5.keytab
restorecon -v /etc/krb5.keytab

mkdir -p /public /secure/protected
chown harry:harry /secure
chmod 0755 /secure

systemctl enable --now nfs-client.target
```

Add the persistent mounts to `/etc/fstab`. Replace `<nfs-server>` below with the hostname or address of the NFS server from the simulation (for example, `system1` if that is the export server):

```
<nfs-server>:/nfsshare              /public            nfs  defaults,_netdev          0 0
<nfs-server>:/nfssecure/protected    /secure/protected  nfs  sec=krb5p,_netdev         0 0
```

Mount and verify:

```
mount -a
findmnt /public
findmnt /secure/protected
su - harry -c 'touch /secure/harry-write-test'
```

The first mount is a normal persistent NFS mount. The second uses `sec=krb5p`, which supplies Kerberos authentication, integrity, and encryption/privacy. Giving `harry` ownership of `/secure` allows that user to create files directly beneath that directory while retaining the protected NFS mount at `/secure/protected`.

QUESTION NO: 15 - (SIMULATION)

There were two systems:

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

system2, some configuration here

Webserver.

Implement a webserver for the site http://server X.example.com

Download the webpage from http://station.network0.example.com/pub/rhce/rhce.html

Rename the downloaded file in to index.html

Copy the file into the document root

Do not make any modification with the content of the index.html

Clients within my22ilt.org should NOT access the webserver on your systems

ANSWER: See the explanation for the answer

Explanation:

Perform the following on **each web server system** (using its appropriate name, for example `server1.example.com` and/or `server2.example.com`). The supplied page must be used unchanged.

```
dnf -y install httpd
curl -o /var/www/html/index.html http://station.network0.example.com/pub/rhce/rhce.html
restorecon -Rv /var/www/html
systemctl enable --now httpd
firewall-cmd --permanent --add-service=http
firewall-cmd --reload
```

Create an Apache configuration file such as `/etc/httpd/conf.d/site-access.conf` with the following content. This permits normal access to the document root but rejects clients whose host name is in `my22ilt.org`.

```
<Directory "/var/www/html">
    <RequireAll>
        Require all granted
        Require not host my22ilt.org
    </RequireAll>
</Directory>
```

Then validate and reload Apache:

```
apachectl configtest
systemctl reload httpd
```

If the task requires an explicit name-based virtual host for the local server name, add the following as well (replace `serverX.example.com` with the hostname assigned to that system):

```
<VirtualHost *:80>
    ServerName serverX.example.com
    DocumentRoot /var/www/html
</VirtualHost>
```

The page is served as `http://serverX.example.com/`, with `index.html` unchanged. `Require not host my22ilt.org` relies on reverse and forward DNS hostname verification, which is appropriate when the requested restriction is by DNS domain.

QUESTION NO: 16 - (SIMULATION)

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 iSCSI Clients

Configure the system2 to make it can link to iqn.2014-09.com.example.domain11:system1 provided by the system, meet the following requirements at the same time:

1. iSCSI device automatically loads during the system start-up.

Block device iSCSI contains a 2100MIB partition, and is formatted as ext4.

This partition mount to the /mnt/data and mount automatically during the system start-up.

ANSWER: See the explanation for the answer

Explanation:

Perform the iSCSI initiator configuration on `system2.group3.example.com`. The target portal is `system1.group3.example.com` (or `172.24.3.5`) and the required target IQN is `iqn.2014-09.com.example.domain11:system1`.

```
# Install the initiator utilities if they are not already installed
yum -y install iscsi-initiator-utils

# Discover the target and log in to its specified IQN
iscsiadm -m discovery -t sendtargets -p 172.24.3.5
iscsiadm -m node -T iqn.2014-09.com.example.domain11:system1 -p 172.24.3.5 --login

# Make the saved target session reconnect automatically at boot
iscsiadm -m node -T iqn.2014-09.com.example.domain11:system1 -p 172.24.3.5 \
  --op update -n node.startup -v automatic
systemctl enable iscsid iscsi
```

Identify the new iSCSI disk. It will normally appear as a new `/dev/sdX` device after login. Confirm carefully before partitioning:

```
lsblk
iscsiadm -m session -P 3
```

Assuming the newly attached iSCSI disk is `/dev/sdb`, create one partition exactly 2100 MiB in size, format it as ext4, and mount it persistently:

```
parted -s /dev/sdb mklabel gpt
parted -s /dev/sdb mkpart primary ext4 1MiB 2101MiB
partprobe /dev/sdb
mkfs.ext4 -F /dev/sdb1

mkdir -p /mnt/data
UUID=$(blkid -s UUID -o value /dev/sdb1)
echo "UUID=$UUID /mnt/data ext4 defaults,_netdev 0 0" >> /etc/fstab
mount -a
findmnt /mnt/data
```

The `_netdev` option ensures the mount is treated as network-backed and is mounted only after the iSCSI device becomes available. Verify persistence with:

```
iscsiadm -m node
cat /etc/fstab
```

QUESTION NO: 17 - (SIMULATION)

SIMULATION

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

NFS server.

- Configure serverX with the following requirements
- Share the /nfsshare directory within the example.com domain clients only, share must be writable
- Share the /nfssecure, enable krb5p security to secure access to the NFS share from URL http://station.network0.example.com/pub/keytabs/serverX.keytab ▪ Create a directory named as protected under /nfssecure
- The exported directory should have read/write access from all subdomains of the example.com domain
- Ensure the directory /nfssecure/protected should be owned by the user harry with read/write permission

ANSWER: See the explanation for the answer

Explanation:

Perform the following on `serverX`. The wildcard `*.example.com` permits hosts in subdomains of `example.com` and does not permit arbitrary external hosts.

```
# Install the NFS and Kerberos client utilities if needed
yum -y install nfs-utils krb5-workstation

# Create the exported directories
mkdir -p /nfsshare /nfssecure/protected
chown harry:harry /nfssecure/protected
chmod 700 /nfssecure/protected

# Install the NFS service Kerberos keytab
curl -o /etc/krb5.keytab \
  http://station.network0.example.com/pub/keytabs/serverX.keytab
chown root:root /etc/krb5.keytab
chmod 600 /etc/krb5.keytab
restorecon -v /etc/krb5.keytab
```

Create the NFS export configuration, for example in `/etc/exports.d/serverX.exports`:

```
/nfsshare  *.example.com(rw)
/nfssecure *.example.com(rw,sec=krb5p)
```

Configure SELinux appropriately for nonstandard writable NFS export paths and activate the exports:

```
semanage fcontext -a -t nfs_t '/nfsshare(/.*)?'
semanage fcontext -a -t nfs_t '/nfssecure(/.*)?'
restorecon -RFv /nfsshare /nfssecure
setsebool -P nfs_export_all_rw on

exportfs -rav
```

Start and enable the regular and Kerberos-secured NFS services. On RHEL 7, `nfs-secure-server` starts the server-side GSS daemon needed for `sec=krb5p`.

```
systemctl enable --now nfs-server nfs-secure-server
```

If `firewalld` is enabled, allow NFS access:

```
firewall-cmd --permanent --add-service=nfs
firewall-cmd --permanent --add-service=mountd
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --reload
```

The important secure export option is `sec=krb5p`; it supplies Kerberos authentication plus integrity and privacy (encryption). The `/nfssecure/protected` directory is owned by `harry` and mode `700`, giving that owner read, write, and directory traversal access while denying access to other local users.

QUESTION NO: 18 - (SIMULATION)

You are giving RHCE exam. Examiner gave you the Boot related problem and told to you that make successfully boot the System. When you started the system, System automatically asking the root password for maintenance. How will you fix that problem?

ANSWER: See the explanation for the answer

Explanation:

The maintenance/emergency shell is normally reached because systemd cannot mount an entry required by `/etc/fstab` (for example, a nonexistent device, an incorrect UUID, or a filesystem needing repair). Log in with the root password and correct the failing mount.

```
# mount -o remount,rw /
# systemctl --failed
# journalctl -xb
# cat /etc/fstab
# lsblk -f
# blkid
```

Compare the device/UUID and filesystem type in `/etc/fstab` with the output of `lsblk -f` or `blkid`. Edit `/etc/fstab` and either correct the bad entry or comment it out if that filesystem should not be mounted:

```
# vi /etc/fstab
```

For example, replace an invalid UUID with the correct UUID, or temporarily comment out the failed line:

```
#UUID=wrong-uuid  /data  xfs  defaults  0 0
```

Validate the corrected file before rebooting:

```
# systemctl daemon-reload
# mount -a
```

`mount -a` must complete without errors. If the device exists but its filesystem is damaged, repair it while it is not mounted (for example, `fsck -y /dev/sdXN` for ext filesystems; use the appropriate XFS recovery procedure for XFS), then run `mount -a` again.

Finally, continue the boot or reboot:

```
# systemctl reboot
# or: exit
```

The important fix is to make every mandatory `/etc/fstab` entry valid and mountable. For a nonessential disk, adding `nofail` to its mount options also prevents its absence from stopping boot.