DUMPSQUEEN

RHCE (Redhat Certified Engineer)

RedHat RH302

Version Demo

Total Demo Questions: 15

Total Premium Questions: 330

Buy Premium PDF

https://dumpsqueen.com

support@dumpsqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Debug Section (38 Questions)	37
Topic 2, RHCT Section, Installation and Configuration Section (60 Questions)	60
Topic 3, RHCE Section, Installation and Configuration Section (75 Questions)	75
Topic 4, Practice – Debug (37 Questions)	37
Topic 5, Practice - RHCT, Installation and Configuration (51 Questions)	51
Topic 6, Practice, RHCE, Installation and Configuration (69 Questions)	70
Total	330

QUESTION NO: 1 - (SIMULATION)

SIMULATION

There are some part-time staff in your office. And you gave the username user9 and user10 to them. Their Office time is 12-2pm on Sunday, Monday and Friday. Configure to login only on their office time.

ANSWER: Dothefollowingstepsas:

Explanation:

1. vi /etc/security/time.conf

login;*;user9|user10;SuMoFri1200-1400

2. vi /etc/pam.d/login

account required pam_time.so

For Time based authentication, we should configured in /etc/security/time.conf

Syntax of /etc/security/time.conf

services;ttys;users;times

services

is a logic list of PAM service names that the rule applies to.

ttys

is a logic list of terminal names that this rule applies to.

users

is a logic list of users to whom this rule applies.

times

the format here is a logic list of day/time-range entries the days are specified by a sequence of two character entries, MoTuSa for example is Monday Tuesday and Saturday. Note that repeated days are unset MoMo = no day, and MoWk = all weekdays bar Monday. The two character combinations accepted are

Mo Tu We Th Fr Sa Su Wk Wd Al

the last two being week-end days and all 7 days of the week respectively. As a final example, AlFr means all days except Friday.

pam_time modules checks the file /etc/security/time.conf for authentication. So, we should call the pam_time modules in /etc/pam.d/login.

QUESTION NO: 2 - (SIMULATION)

SIMULATION

Backup of the Redhat Enterprise Linux 5 is on /var/ftp/pub, /var/www/html/pub on server named server1.example.com. You can install all required packages using yum by creating the repository file.

ANSWER: Dothefollowingstepsas:

Explanation:

1. Create the repository file

#vi /etc/yum.repos.d/server1.repo

[station?]

name=station?

baseurl=ftp://server1.example.com/pub/

enabled=1

gpgcheck=1

gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release

yum install

QUESTION NO: 3 - (SIMULATION)

SIMULATION

Create the directory /archive and group owner should be the sysuser group.

ANSWER: Dothefollowingstepsas:

Explanation:

1. chgrp sysuser /archive

2. Verify using ls -ld /archive command. You should get like

drwxr-x--- 2 root sysadmin 4096 Mar 16 17:59 /archive

chgrp command is used to change the group ownership of particular files or directory.

Another way you can use the chown command.

chown root:sysuser /archive

QUESTION NO: 4 - (SIMULATION)

SIMULATION

You are the Network Engineer of example.com domain. Configure to allow users user1, user2 and user3 to login only between 9am to 17pm on very day.

ANSWER: Dothefollowingstepsas:

Explanation:

1. vi /etc/security/time.conf

login;*;user1|user2|user3;Al0900-1700

2. vi /etc/pam.d/login

account required pam_time.so

For Time based authentication, we should configured in /etc/security/time.conf

Syntax of /etc/security/time.conf

services;ttys;users;times

services

is a logic list of PAM service names that the rule applies to.

ttys

is a logic list of terminal names that this rule applies to.

users

is a logic list of users to whom this rule applies.

times

the format here is a logic list of day/time-range entries the days are specified by a sequence of two character entries, MoTuSa for example is Monday Tuesday and Saturday. Note that repeated days are unset MoMo = no day, and MoWk = all weekdays bar Monday. The two character combinations accepted are

Mo Tu We Th Fr Sa Su Wk Wd Al

the last two being week-end days and all 7 days of the week respectively. As a final example, AlFr means all days except Friday.

pam_time modules checks the file /etc/security/time.conf for authentication. So, we should call the pam_time modules in /etc/pam.d/login.

QUESTION NO: 5 - (SIMULATION)

SIMULATION

We are working on /data initially the size is 2GB. The /dev/test0/lvtestvolume is mount on /data. Now you required more space on /data but you already added all disks belong to physical volume. You saw that you have unallocated space around 5 GB on your harddisk. Increase the size of lvtestvolume by 5GB.

ANSWER: Dothefollowingstepsas:

Explanation:

1. Create a partition having size 5 GB and change the syste id ‘8e’.

2. use partprobe command

3. pvcreate /dev/hda9 Suppose your partition number is hda9.

4. vgextend test0 /dev/hda9 vgextend command add the physical disk on volume group.

5. lvextend –L+5120M /dev/test0/lvtestvolume

6. verify using lvdisplay /dev/test0/lvtestvolume.

QUESTION NO: 6 - (SIMULATION)

SIMULATION

Any mail coming for accountmanager should get by jeff user.

ANSWER: Dothefollowingstepsas:

Explanation:

1. vi /etc/mail/virtusertable

accountmanager@ jeff

2. service sendmail restart

QUESTION NO: 7 - (SIMULATION)

SIMULATION

Eric user should able to write on Document root directory.

ANSWER:
Documentdirectiveisusedinapacheconfigurationfiletospecifythedirectorywhereallwebsiterelateddocumentsare.Accordingtoquestionericusershouldabletowriteintothe Documentrootdirectory.

Explanation:

Better set the permission using ACL (Access Control List), to apply the permission using acl needs to mount the filesystem with acl options. Example in above answer documentroot is in /var and /var is mounting separate file system so needs to mount the /var file system with acl option.

1. vi /etc/fstab

LABEL=/var /var ext3 defaults 1 1

2. mount –o remount /var

3. setfacl –m u:eric:rwx /var/www/example

4. getfacl /var/www/example

getfacl and setfacl two commands used to maintain the permission through acl. setfacl is used to set the permission on file/directory, getfacl is used to display the permission of file/directory.

QUESTION NO: 8 - (SIMULATION)

SIMULATION

You are the administrator of example.com domain. Configure to deny local login to all normal users on your domain server. As well as allow to root login only on First Terminal.

ANSWER: Dothefollowingstepsas:

Explanation:

1. touch /etc/nologin

2. vi /etc/securetty

comment all available terminall then first.

If /etc/nologin file is created, then pam modules pan_nologin deny to all non-root users to login locally.

/etc/pam.d/login file calls the module.

#%PAM-1.0

auth required pam_securetty.so

auth required pam_stack.so service=system-auth

auth required pam_nologin.so

account required pam_stack.so service=system-auth

password required pam_stack.so service=system-auth

pam_selinux.so close should be the first session rule

session required pam_selinux.so close

session required pam_stack.so service=system-auth

session optional pam_console.so

pam_selinux.so open should be the last session rule

session required pam_selinux.so multiple open

pam_securetty modules checks the /etc/securetty file, which terminal are available to root. If terminal is not available in this file then pam_securetty module deny to login on unavailable terminal to root user.

QUESTION NO: 9 - (SIMULATION)

SIMULATION

Change the Group Owner of /data to training group.

ANSWER: chownorchgrpcommandisusedtochangetheownership.

Explanation:

Syntax of chown: chown [-R] username:groupname file/directory

Syntax of chgrp: chgrp [-R] groupname file/directory

Whenever user creates the file or directory, the owner of that file/directory automatically will be that user and that user's primary group name.

To change group owner ship

1. chgrp training /data Which set the Group Ownership to training

or

chown root.training /data Which set the user owner to root and group owner to training group.

Verify /data using: ls -ld /data

You will get: drwxr-xr-x 2 root training ……..

QUESTION NO: 10 - (SIMULATION)

SIMULATION

Your LAN is 192.168.0.0/24. Block the telnet connection from outside the LAN.

ANSWER: Dothefollowingstepsas:

Explanation:

1. vi /etc/hosts.deny

in.telnetd:ALL EXCEPT 192.168.0.

We can secure the services using tcp_wrappers. There are main two files, /etc/hosts.allow and /etc/hosts.deny.

There will be three stage access checking

-Is access explicitly permitted? Means permitted from /etc/hosts.allow?

- Otherwise, Is access explicitly denied? Means denied from /etc/hosts.deny?

- Otherwise, by default permit access if neither condition matched.

To deny the services we can configure /etc/hosts.deny file using ALL and EXCEPT operation. Pattern of /etc/hosts.allow and /etc/hosts.deny file is:

Demon_list:client_list:options

In Client list can be either domain name or IP address. Here in.telnetd is the telnet server program name.

QUESTION NO: 11 - (SIMULATION)

SIMULATION

Create the group named training

ANSWER: Dothefollowingstepsas:

Explanation:

1. groupadd training

To create a group we use the groupadd command.

Verify from: cat /etc/group whether group added or not?

QUESTION NO: 12 - (SIMULATION)

SIMULATION

Configure to allow the pop3 and imap connection from your domain example.com

and my133t.org domain.

ANSWER: Dothefollowingstepsas:

Explanation:

1. vi /etc/hosts.deny

dovecot:ALL EXCEPT .example.com, .my133t.org

We can secure the services using tcp_wrappers. There are main two files, /etc/hosts.allow and /etc/hosts.deny.

There will be three stage access checking

- Is access explicitly permitted? Means permitted from /etc/hosts.allow?

- Otherwise, Is access explicitly denied? Means denied from /etc/hosts.deny?

- Otherwise, by default permit access if neither condition matched.

To deny the services we can configure /etc/hosts.deny file using ALL and EXCEPT operation. Pattern of /etc/hosts.allow and /etc/hosts.deny file is:

Demon_list:client_list:options

In Client list can be either domain name or IP address.

QUESTION NO: 13 - (SIMULATION)

SIMULATION

Deny the ALL services to the member of cracker.org but allow to trusted.cracker.org.

ANSWER: Dothefollowingstepsas:

Explanation:

1. vi /etc/hosts.deny

ALL:.cracker.org EXCEPT trusted.cracker.org

We can secure the services using tcp_wrappers. There are main two files, /etc/hosts.allow and /etc/hosts.deny.

There will be three stage access checking

-Is access explicitly permitted? Means permitted from /etc/hosts.allow?

- Otherwise, Is access explicitly denied? Means denied from /etc/hosts.deny?

- Otherwise, by default permit access if neither condition matched.

To deny the services we can configure /etc/hosts.deny file using ALL and EXCEPT operation. Pattern of /etc/hosts.allow and /etc/hosts.deny file is:

Demon_list:client_list:options

In Client list can be either domain name or IP address.

QUESTION NO: 14 - (SIMULATION)

SIMULATION

One User named peter working with you as your assistance. His main responsibility is to manager users. Give the privilege to run useradd, passwd, groupadd, userdel, groupdel, usermod command using sudo.

ANSWER: Dothefollowingstepsas:

Explanation:

1. visudo

User alias Specification

User_alias LIMITEDTRUST=peter

Cmnd alias Specification

Cmnd_alias MINIMUM=/usr/sbin/useradd, /usr/bin/passwd, /usr/sbin/groupadd, /usr/sbin/userdel, /usr/sbin/groupdel, /usr/sbin/usermod

User Privilege Specification

LIMITEDTRUST ALL=MINIMUM

2. Login as peter user and run sudo useradd username

Using Sudo we can give root level privilege on commands. Visudo is the sudo editor. In user alias Specification we create the user alias and in Cmnd alias Specification, we create the command alias. In User Privilege Specification section, list the users, groups allowed to use the sudo.

QUESTION NO: 15 - (SIMULATION)

SIMULATION

You are giving RHCE exam. You should boot the system in Run level 3. When you start the system after while it is going on runlevel 6 : like

INIT: Entering Run level 6

Sending TERM Single

Fix the problem and boot the system.

ANSWER: Itisduetoeitherdefaultrunlevelorrunlevelspecificscripts.

Explanation:

1. id:?:initdefault: □Where default runlevel is specified. It shouldn't be 6.

2. l3:3:wait:/etc/rc.d/rc 6 □ It reads the scripts of runlevel 6 while booting system on rulevel 3.

It should be like:

si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0

l1:1:wait:/etc/rc.d/rc 1

l2:2:wait:/etc/rc.d/rc 2

l3:3:wait:/etc/rc.d/rc 3 Should be like this

l4:4:wait:/etc/rc.d/rc 4

l5:5:wait:/etc/rc.d/rc 5

l6:6:wait:/etc/rc.d/rc 6