DUMPSARENA

RHCE (Redhat Certified Engineer)

RedHat RH302

Version Demo

Total Demo Questions: 15

Total Premium Questions: 330

Buy Premium PDF

https://dumpsarena.co

sales@dumpsarena.co

sales@dumpsarena.co
dumpsarena.co

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

Now a days you are observing that your system being very slow. You observe the processes that one user named user1 running more than 50 processes. Configure to limit the number of processes that user1 couldn't run more than 7 process.

ANSWER: Dothefollowingstepsas:

Explanation:

1. vi /etc/security/limits.conf

user1 hard nproc 7

2. vi /etc/pam.d/system-auth

session required /lib/security/pam_limits.so

To limit the number of process or number of logins, we should configure on /etc/security/limits.conf. First Columns contains the username separated by comma or @group name. Second column either hard or soft limits. Third columns called the item, maxloigns or nproc etc.

To identify the session of users we should call the pam_limits module in /etc/pam.d/system-auth.

QUESTION NO: 2 - (SIMULATION)

SIMULATION

You have a domain in your LAN example.com. Configure to allow login to jack only from station10.example.com.

ANSWER: Dothefollowingstepsas:

Explanation:

1. vi /etc/security/access.conf

-:jack:ALL EXCEPT station10.example.com

2. vi /etc/pam.d/system-auth

account required /lib/security/pam_access.so

/etc/security/access.conf file helps to allow or deny login to users on the basis of origin.

Syntax of /etc/security/access.conf

permission : users : origins

The first field should be a "+" (access granted) or "-" (access denied) character.

The second field should be a list of one or more login names, group names, or ALL (always matches). A pattern of the form user@host is matched when the login name matches the "user" part, and when the "host" part matches the local machine name.

The third field should be a list of one or more tty names (for non-networked logins), host names, domain names (begin with "."), host addresses, internet network numbers (end with "."), ALL (always matches) or LOCAL (matches any string that does not contain a "." character).

The EXCEPT operator makes it possible to write very compact rules

QUESTION NO: 3 - (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: 4 - (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: 5 - (SIMULATION)

.

SIMULATION

You have a dedicated internet line in your LAN and IP from your ISP is 202.2.2.2. Your LAN is in 192.168.0.0/24. Configure the SNAT that allows all system in your LAN can access the Internet.

ANSWER: Dothefollowingstepsas:

Explanation:

1. iptables -t nat -A POSTROUTING -s 192.168.0.0/24 -p tcp -j SNAT –to-source 202.2.2.2.

POSTROUTING This filter point handles packets immediately prior leaving the system.

When Packets leave the system all's source address change to 202.2.2.2 and can access the internet.

iptables is the build-in firewall tools, used to filter the packets and for nat. By identifying Source Address, Destination Address, type of protocol, source and destination port we can filter the packets.

-s Source Address

-d Destination Address

-p Layer 3 Protocol

-dDestination Address

--sport Source Prot

--dportDestination Port

-i Incoming Interface

-o Outgoing Interface

-t □ Table either filter or nat or mangle

-A□ Chain can be either INPUT, OUTPUT, FORWARD, PREROUTING, POSTROUTING.

QUESTION NO: 6 - (SIMULATION)

SIMULATION

Create the group named sysadmin.

ANSWER: Dothefollowingstepsas:

Explanation:

1. groupadd sysadmin

groupadd command is used to create the group and all group information is stored in /etc/group file.

QUESTION NO: 7 - (SIMULATION)

SIMULATION

Make Secondary belongs the jackie and curtin users on sysuser group. But david user should not belongs to sysuser group.

ANSWER: Dothefollowingstepsas:

Explanation:

1. usermod -G sysuser jackie

2. usermod –G sysuser curtin

3. Verify by reading /etc/group file

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 belongs 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 NO: 8 - (SIMULATION)

SIMULATION

Make Secondary belongs the both users on sysadmin group.

ANSWER: Dothefollowingstepsas:

Explanation:

1. usermod -G sysadmin john

2. usermod –G sysadmin jane

3. Verify by reading /etc/group file

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 belongs 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 NO: 9 - (SIMULATION)

SIMULATION

Create the user named eric but eric should not belong to the sysadmin group.

ANSWER: Dothefollowingstepsas:

Explanation:

1. useradd eric

Very tricky question given to you that this user should not belongs to sysadmin group.

QUESTION NO: 10 - (SIMULATION)

SIMULATION

You have ftp site named ftp.example.com. You want to deny login as an anonymous on your ftp site. Configure to deny the anonymous.

ANSWER: Dothefollowingstepsas:

Explanation:

1. vi /etc/vsftpd/vsftpd.conf

anonymous_enable=no

2. service vsftpd restart

/etc/vsftpd/vsftpd.conf file is used to allow or deny to anonymous or real user. To allow anonymous anonymous_enable=yes should be there. Sample configuration is like.

Allow anonymous FTP? (Beware - allowed by default if you comment this out).

anonymous_enable=YES

```
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
# obviously need to create a directory writable by the FTP user.
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
```

```
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/vsftpd.log
#
# If you want, you can have your log file in standard ftpd xferlog format
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
```

```
# mangling on files when in ASCII mode.
# Beware that turning on ascii_download_enable enables malicious remote parties
# to consume your I/O resources, by issuing the command "SIZE /big/file" in
# ASCII mode.
# These ASCII options are split into upload and download because you may wish
# to enable ASCII uploads (to prevent uploaded scripts etc. from breaking),
# without the DoS risk of SIZE and ASCII downloads. ASCII mangling should be
# on the client anyway..
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd.banned_emails
#
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd.chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
```

the presence of the "-R" option, so there is a strong case for enabling it.

#ls_recurse_enable=YES

pam_service_name=vsftpd

userlist_enable=YES

#enable for standalone mode

listen=YES

tcp_wrappers=YES

QUESTION NO: 11 - (SIMULATION)

SIMULATION

There are mixed lots of System running on Linux and Windows OS. Some users are working on Windows Operating System. You want to make available /data directory to samba users only from 192.168.0.0/24 network. Configure the samba server.

ANSWER: Dothefollowingstepsas:

Explanation:

1. vi /etc/samba/smb.conf

[global]

netbios name=station?

workgroup = mygroup

server string=Share from Linux Server

security=user

smb passwd file=/etc/samba/smbpasswd

encrypt passwords=yes

hosts allow=192.168.0.

[data]

path=/data

writable=yes

public=no

browsable=yes

2. service smb start| restart

3. chkconfig smb on

Samba servers helps to share the data between linux and windows. Configuration file is /etc/samba/smb.conf. There are some pre-defined section, i. global use to define the global options, ii. Printers use to share the printers, iii. homes use to share the user's home directory.

Security=user validation by samba username and password. May be there are other users also. To allow certain share to certain user we should use valid users option.

smbpasswd Helps to change user's smb password. –a option specifies that the username following should be added to the local smbpasswd file.

If any valid users option is not specified, then all samba users can access the shared data. By Default shared permission is on writable=no means read only sharing. Write list option is used to allow write access on shared directory to certain users or group members.

To allow access the shared directory only from certain network or hosts, there is a option hosts allow= host or network. If this option is applied on global option, then it will apply to all shared directory.

QUESTION NO: 12 - (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: 13 - (SIMULATION)

SIMULATION

Raw printer named printerx where x is your station number is installed and shared on server1.example.com. Install the shared printer on your PC to connect shared printer using IPP Protocols. Your server is 192.168.0.254.

ANSWER: Dothefollowingstepsas:

Explanation:

1. Open the Browser either firefox or links

2. Type : http://localhost:631

3. Click on Manage Printer

4. Click on Add Printer

5. Type Queue name like stationx and click on continue

6. Type Device type or printing Protocol: i.e Internet printing Protocol

7. Click on Continue

8. Type Device URL: ipp://server1.example.com/printers/printerx

9. Click on Continue

10. Select RAW Model printer

11. Click on Continue

12. Test by sending the printing job

QUESTION NO: 14 - (SIMULATION)

SIMULATION

Port 8080

Configure the squid server to allow the Local Domain and deny to my133t.org domain.

ANSWER:
AtexamLabexample.comdomainresideson172.24.0.0/16Networkandmy133t.orgresideson172.25.0.0/16Network.

Explanation:

1. vi /etc/squid/squid.conf

#detault:

http_port 8080

#Recommended minimum configuration:

Near the src acl src section

acl allownet src 172.24.0.0/255.255.0.0

acl denynet src 172.25.0.0/255.255.0.0

#Default:

http_access deny all

#Under Here

http_access allow allownet

http_access deny denynet

2. service squid start

3. chkconfig squid on

squid is a proxy caching server, using squid we can share the internet, block the internet, to certain network. First we should define the port for squid, the standard port for squid is 3128. We can run squid on different port by specifying http_port portnumber.

QUESTION NO: 15 - (SIMULATION)

SIMULATION

One Package named zsh is dump on ftp://server1.example.com under pub directory. Install the package from ftp server.

ANSWER: Dothefollowingstepsas:

Explanation:

1. rpm –ivh ftp://server1.example.com/pub/zsh-*

2. Package will install

rpm command is used to install, update and remove the package, -i means install, -v means verbose and -h means display the hash mark.