RHCSA.GURU

Solutions : Mock Test 1

Task 1 - Create a cron job that appends the word Hello_World to the /var/log/messages log file. Ensure that this job runs at 12 PM (noon) only on weekdays.

Solution - 1- Open the crontab editor: crontab -e to edit the user's cron jobs.

```
bash-5.1# crontab -e
```

RHCSA.GURU

2- Add the cron job:

- 0 12: Run the job at 12:00 PM (noon).
- * *: Run on any day of the month and any month.
- 1-5: Restrict execution to weekdays (Monday to Friday).
- echo "Hello_World" >> /var/log/messages: Append the text Hello_World to /var/log/messages.

```
0 12 * * 1-5 echo "Hello_World" >> /var/log/messages

~
```

RHCSA.GURU

Task 2 - Find the user 'root' in the /etc/passwd file. Output this information to a file named users_entry in the /home directory. Afterwards, edit the file /home/users_entry to replace the user's shell from /bin/bash to /bin/sh.

Solution - 1- Find and output 'root' user entry:

- Searches for lines starting with root: in /etc/passwd.
- Redirects the output to the file /home/users_entry.

```
bash-5.1# grep '^root:' /etc/passwd > /home/users_entry
bash-5.1#
```

RHCSA.GURU

2- Edit the shell from /bin/bash to /bin/sh:

- -i: Edits the file in place.
- s|/bin/bash|/bin/sh|: Substitutes /bin/bash with /bin/sh.

```
bash-5.1# sed -i 's|/bin/bash|/bin/sh|' /home/users_entry
bash-5.1# cat /home/users_entry
root:x:0:0:root:/root:/bin/sh
bash-5.1#
```

RHCSA.GURU

Task 3 - Configure the system to limit the number of SSH login attempts to only 3. Also set that the password for all new users should expire after 20 days.

Solution -

1. Limit SSH login attempts to 3:
   - Edit the SSH configuration file and modify the MaxAuthTries using vi editor

```
bash-5.1# vi /etc/ssh/sshd_config
```

```
#StrictModes yes
MaxAuthTries 3
#MaxSessions 10

#PubkeyAuthentication yes
:wq!
```

   - Restart the SSH service to apply changes

```
bash-5.1# systemctl restart sshd
bash-5.1#
```

RHCSA.GURU

2. Set password expiration to 20 days for new users:

- Edit the default user settings in /etc/login.defs and update PASS_MAX_DAYS to 20 using vi editor

```
bash-5.1# vi /etc/login.defs
```

```
#
PASS_MAX_DAYS   20
PASS_MIN_DAYS   0
PASS_WARN_AGE   7

# Currently PASS_MIN_LEN is not supporte
```

RHCSA.GURU

Task 4 - Search for the Redis container image on the RHEL system and pull the image from the Docker registry.

Solution -

1. Install Podman:

```
bash-5.1# dnf install podman -y
Updating Subscription Management repositories.
Unable to read consumer identity
```

2. Pull the Redis container Image from docker.io

```
bash-5.1# podman pull redis
? Please select an image:
   registry.access.redhat.com/redis:latest
   registry.redhat.io/redis:latest
 ▸ docker.io/library/redis:latest
```

3. Confirm the Redis image has been pulled:

RHCSA.GURU

Task 5 - Configure the SELinux boolean value 'container_manage_cgroup' to be enabled (set to 'on') and ensure that this setting is persistent across reboots.

Solution -

1. Enable the SELinux Boolean:
   - Use the setsebool command to enable the container_manage_cgroup boolean:

```
bash-5.1# setsebool container_manage_cgroup on
bash-5.1#
```

RHCSA.GURU

2. Make the Boolean Persistent:
   - Use the -P option with setsebool to ensure the setting persists across reboots:

```
bash-5.1# setsebool -P container_manage_cgroup on
bash-5.1#
```

RHCSA.GURU

Task 6 - Add a new user 'expert' to the system with a UID of 1500. Set the user's home directory to /home/expertDir and the user's shell to /bin/sh. Also set the user's password to any string of your choice.

Solution -

1. **Add the user 'expert' with a UID of 1500:**
   - Create the user with the specified UID, home directory, and shell:
   - useradd Options:
     - -u 1500: Sets the user's UID to 1500.
     - -d /home/expertDir: Specifies the user's home directory.
     - -s /bin/sh: Sets the user's default shell to /bin/sh.

```
bash-5.1# useradd -u 1500 -d /home/expertDir -s /bin
/sh expert
bash-5.1#
```

2. Setting Password:

- The passwd command assigns a password to the user. Enter the password when prompted

```
bash-5.1# passwd expert
Changing password for user expert.
New password:
BAD PASSWORD: The password is shorter than 8 chara
ers
Retype new password:
passwd: all authentication tokens updated successf
ly.
bash-5.1#
```

RHCSA.GURU

Task 7 - Create a new group called panel , new user named 'dev' and add the new user dev to panel group as a secondary group. After this, set the default permissions for the user dev such that:

- All newly created files by dev should have the permissions -r-------- (read-only for the owner).
- All newly created directories by dev should have the permissions dr-x------ (read-only for the owner).

Solution - **1. Create the new group 'panel' and a new user 'dev'**

```
bash-5.1# groupadd panel
bash-5.1# useradd dev
bash-5.1#
```

RHCSA.GURU

2. **Add user ‘dev’ to the 'panel' group:**

- usermod -aG command adds dev as a member of the panel group without removing them from other groups. The -a flag ensures the user is appended to the group list.

```
bash-5.1# usermod -aG panel dev
bash-5.1#
```

3. **Set the default permissions for user 'dev'**:

- Add the umask command to /home/dev/.bashrc to ensure that all newly created files have -r-------- (read-only for the owner) and directories have dr-x------ (read-only for the owner):

```
bash-5.1# echo 'umask 0277' >> /home/dev/.bashrc
bash-5.1#
```

2. Apply the changes and verify:

- To apply the changes immediately, source the .bashrc file:

```
bash-5.1# source /home/dev/.bashrc
bash-5.1#
```

- Switch to user dev and create a directory (testDir) and a file (file) with umask 0277 applied, resulting in read-only permissions for the owner (-r-------- for the file and dr-x------ for the directory)

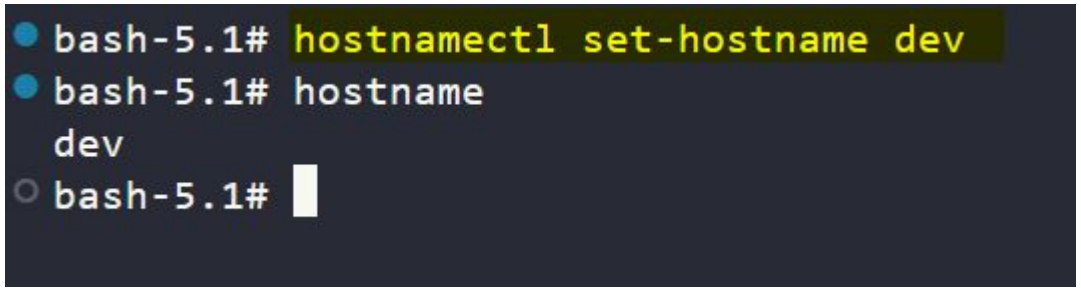
```
bash-5.1# su - dev
Last login: Tue Jan 14 11:55:27 UTC 2025 on pts/0
[dev@ip-172-31-46-91 ~]$ mkdir testDir && touch file
[dev@ip-172-31-46-91 ~]$ ls -l
total 0
-r--------. 1 dev dev 0 Jan 14 11:56 file
dr-x------. 2 dev dev 6 Jan 14 11:56 testDir
[dev@ip-172-31-46-91 ~]$
```

RHCSA.GURU

Task 8 - Modify the system's hostname to 'dev'

Solution -

- The hostnamectl set-hostname dev command changes the system's hostname to dev, taking effect immediately and persisting across reboots . Verify it using hostname command.

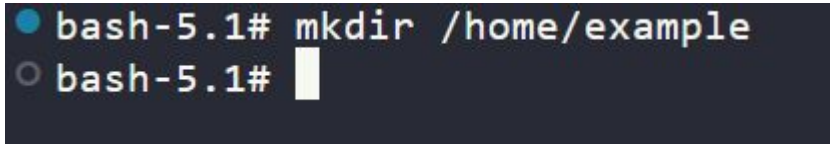


RHCSA.GURU

Task 9 - Create a directory named 'example' in the /home directory. Change the ownership of the directory to the 'expert' user.

Solution -

1. **Create the directory 'example':**
    - mkdir command creates a new directory named example in the /home directory.



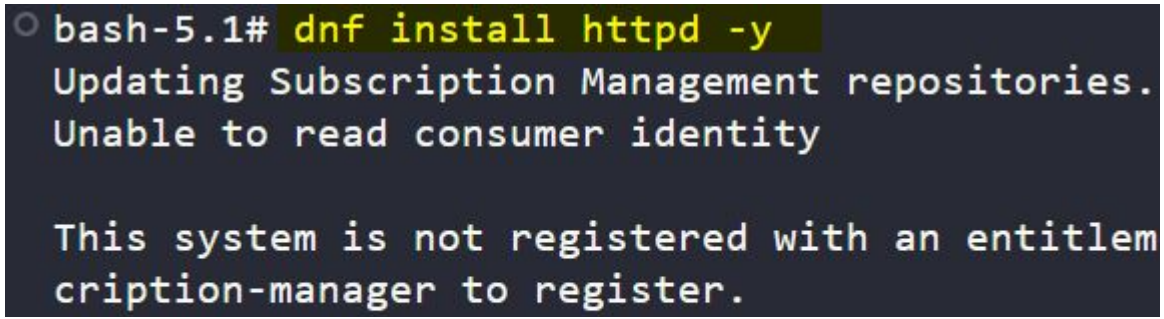
2. **Change ownership to the 'expert' user:**
   - chown command changes the ownership of the /home/example directory to the expert user.

RHCSA.GURU

Task 10 - Configure the Apache HTTP Server to host a simple website displaying the message 'Hello World!'. Ensure that the service is running on port 82

Solution -

1. **Install Apache HTTP Server:**



RHCSA.GURU

2. **Create the HTML file:**
   - Creates a simple index.html file with the 'Hello World!' message in the /var/www/html/ directory.

```
bash-5.1# vi /var/www/html/index.html
bash-5.1#
```

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-width, ini
    <title>Hello World</title>
</head>
<body>
    <h1>Hello, World!</h1>
</body>
</html>
```

3. Configure Apache

- Edit the Apache configuration file by changing Listen 80 to Listen 82

```
bash-5.1#  vi /etc/httpd/conf/httpd.conf
bash-5.1#
```

```
#Listen 12.34.56.78:80
Listen 82

#
# Dynamic Shared Object (DSO) Support
#
:wq!
```

RHCSA.GURU

4. **Adjust SELinux to allow Apache on port 82:**

- semanage command is used to update SELinux policies, allowing Apache to listen on port 82.

```
bash-5.1# semanage port -a -t http_port_t -p tcp 82
bash-5.1#
```

- **port:** Specifies the SELinux policy type for network ports.
- **-a:** Adds a new rule.
- **-t http_port_t:** Associates the port with the HTTP service context.
- **-p tcp:** Specifies the TCP protocol.
- **82:** Defines port 82 for HTTP services.

4. Start the httpd service and verify by using curl command:

```
bash-5.1# systemctl start httpd
bash-5.1# curl http://localhost:82
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta name="viewport" content="width=device-widt
h, initial-scale=1.0">
    <title>Hello World</title>
</head>
<body>
    <h1>Hello, World!</h1>
</body>
</html>
```

RHCSA.GURU