Practice Exam Questions

PE124

Red Hat Preliminary Exam in System Administration I

EXAMAIDES

PASS YOUR EXAM AT FIRST TRY

Volume: 8 Chapter Labs + One Final Lab (include 5 task Labs)

Lab1: Using SCP to Transfer Files Between Systems
Lab2: Configuring User Accounts and Permissions on a Development Server
Lab3: Creating a Backup Structure and Archiving Files
Lab4: Create a Collaborative Directory
Lab5: Managing and Troubleshooting System Services and Processes
Lab6: Reviewing System Logs and Updating the journald Configuration
Lab7: Viewing, Installing and Removing Packages Using YUM and RPM
Lab8: Validating Network Configuration and Configuring Network Services
Final Lab: 5 task labs

Lab1: Using SCP to Transfer Files Between Systems

Introduction

In this hands-on lab, we will connect to a primary development system using SSH, and, once connected, will review the proper syntax for the scp command using either man or info. With the proper syntax in mind, we will use scp to copy a file from the primary development server to a new secondary development system. The last step of the lab will be to copy an audit file from the remote development system to a directory on the primary system.

Solution

Log in to the lab server using the credentials provided:
ssh cloud_user@<PUBLIC_IP_ADDRESS>

Connect to the Primary Development System

Connect to the primary system:
ssh cloud_user@<PUBLIC_IP_ADDRESS>

Use man or info to Review the scp Command Options

1. View the man page for scp:
man scp

2. Exit man page:
q

3. View info page for scp:
info scp

4. Exit info page for scp:
q

Use scp to Copy the Local .bashrc to the New Development System

Copy local .bashrc file to new development system:
scp .bashrc cloud_user@<DEVELOPMENT_SYSTEM_PUBLIC_IP_ADDRESS>:/home/cloud_user

Use scp to Copy a Remote File to the Local System

1. Transfer remote file to the local system:
scp cloud_user@<DEVELOPMENT_SYSTEM_PUBLIC_IP_ADDRESS>:/home/cloud_user/build/devsys12-account-audit.log /home/cloud_user/audit

2. Verify file was successful copied:
ls -l audit/
cat audit/devsys12-account-audit.log

Lab2: Configuring User Accounts and Permissions on a Development Server

Introduction

In this hands-on lab, you will connect to a Red Hat 8 system using SSH. Once connected, you will use the useradd command to add several users, set passwords using the passwd command, use the groupadd command to add a couple of groups, and use either the usermod or gpasswd commands to add users to groups. Once the groups are in place, you will grant elevated privileges to a set of users using the new groups and test the permissions by using the su - command to switch to a user and attempt to run the commands.

Solution

Log in to the lab server using the credentials provided:
ssh cloud_user@<PUBLIC_IP_ADDRESS>

Note: When copying and pasting code into Vim from the lab guide, first enter :set paste (and then i to enter insert mode) to avoid adding unnecessary spaces and hashes. To save and quit the file, press Escape followed by :wq. To exit the file without saving, press Escape followed by :q!.

Add 5 Users to the System

1. Create the new users:
sudo useradd -c "Peter Gibbons" pgibbons
sudo useradd -c "Michael Bolton" mbolton
sudo useradd -c "Samir Nagheenanajar" snagheenanajar

```
sudo useradd -c "Milton Waddams" mwaddams
sudo useradd -c "Tom Smykowski" tsmykowski
```

2. Set the default password of initech123 for all users:

```
sudo passwd pgibbons
sudo passwd mbolton
sudo passwd snagheenanajar
sudo passwd mwaddams
sudo passwd tsmykowski
```

Add 2 Groups to the System

Create the new groups:

```
sudo groupadd devops
sudo groupadd helpdesk
```

Add Users to the New Groups

Add users to the group:

```
sudo gpasswd -M pgibbons,mbolton,snagheenanajar devops
sudo gpasswd -M mwaddams,tsmykowski helpdesk
```

Grant Superuser Privileges Using the New Groups

1. Configure Superuser access:

```
sudo visudo -f /etc/sudoers.d/20-groups
```

2. Add the following access configurations to the file:

```
%devops         ALL=(root)       ALL
%helpdesk     ALL=(root)       /usr/bin/ls,/usr/bin/cat
```

3. Write out the file and close it:

```
:wq
```

Validate Superuser Access for Two of the Accounts, One from Each Group

1. Switch to Peter's account:

```
su - pgibbons
```

2. Run some commands as Peter, list /root directory:

```
ls -al /root
```

3. Elevate permissions and list /root directory:

```
sudo ls -al /root
```

4. Use the two different commands to view /etc/sudoers file:
sudo cat /etc/sudoers
sudo less /etc/sudoers

5. Switch out of Peter's account:
exit

6. Switch to Tom's account:
su - tsmykowski

7. Run some commands as Tom, list /root directory:
ls -al /root

8. Elevate permissions and list /root directory:
sudo ls -al /root

9. Use the two different commands to view /etc/sudoers file:
sudo cat /etc/sudoers
sudo less /etc/sudoers

Lab3: Creating a Backup Structure and Archiving Files

Introduction

In this hands-on lab, you will connect to a Red Hat 8 system using SSH. Once connected, you will install the star archive utility using yum. This directory will be used to collect files for a backup archive. Once the files are connected you will create an archive using the star utility, add a file to the archive once it has been created and then compress the archive using bzip2 compression. The last step will be to view the contents of the archive using the star utility.

Solution

Log in to the lab server using the credentials provided:
ssh cloud_user@<PUBLIC_IP_ADDRESS>

Install the star Utility

Install the star package:
sudo yum install star

Create a Backup Directory and Populate It with Data to be Archived