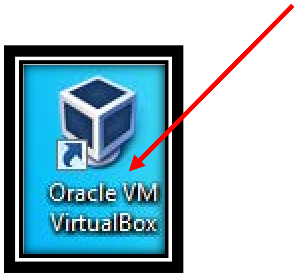
Practical Exercise 6-3: Managing Default and Special Permissions

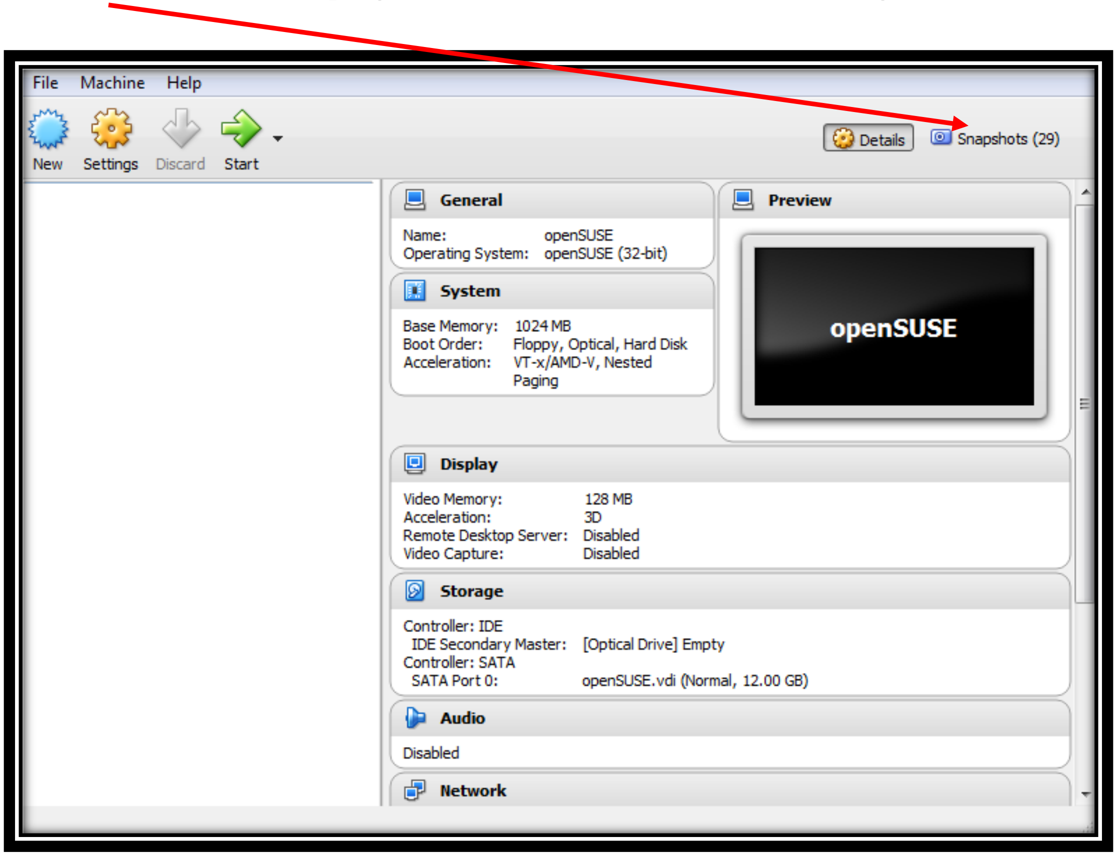
This Practical Exercise will have students modifying default permissions with unmask and adding special permissions to directories.

Open VirtualBox and start the openSUSE VM. Run snapshot 11-3 for the correctly configured environment. To run snapshot 11-3:

1. Open the Oracle VM VirtualBox manager by double clicking this icon on your desktop:



2. Click "Snapshots" in the top right of the Oracle VM Virtualbox Manager.



General
Name: openSUSE
Operating System: openSUSE (32-bit)

System
Base Memory: 1024 MB
Boot Order: Floppy, Optical, Hard Disk
Acceleration: VT-x/AMD-V, Nested Paging

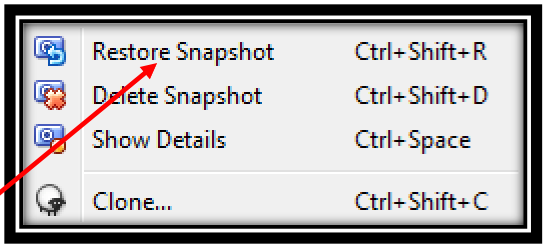
Display
Video Memory: 128 MB
Acceleration: 3D
Remote Desktop Server: Disabled
Video Capture: Disabled

Storage
Controller: IDE
IDE Secondary Master: [Optical Drive] Empty
Controller: SATA
SATA Port 0: openSUSE.vdi (Normal, 12.00 GB)

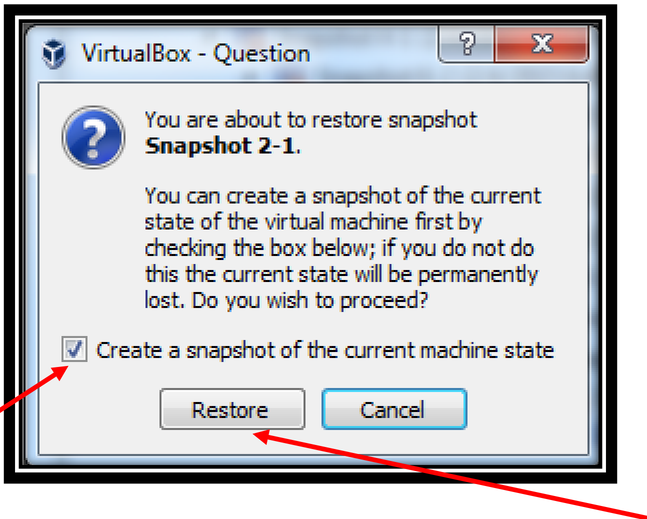
Audio
Disabled

Network

3. In the right side box populated with snapshots scroll up and find the one titled "Snapshot 11-3" and right click on it. The following box should appear:



4. Select "Restore Snapshot" and the following pop-up should appear:



VirtualBox - Question

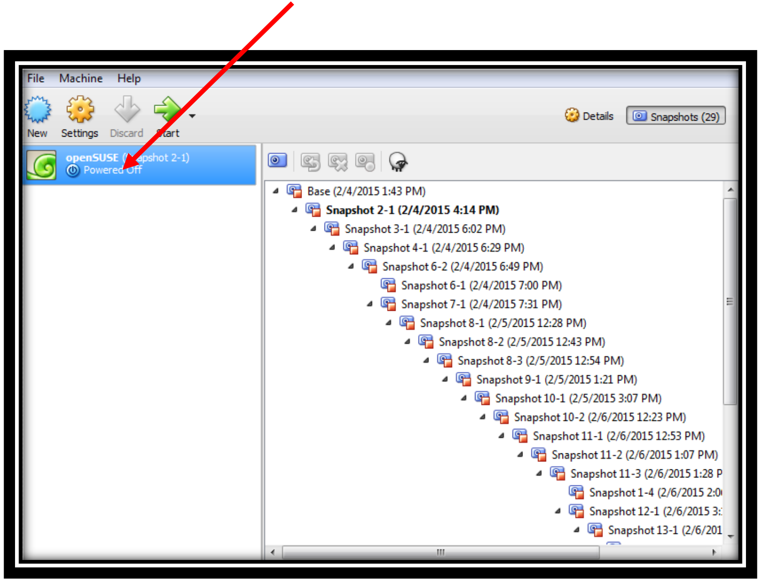
You are about to restore snapshot **Snapshot 2-1**.

You can create a snapshot of the current state of the virtual machine first by checking the box below; if you do not do this the current state will be permanently lost. Do you wish to proceed?

☑ Create a snapshot of the current machine state

5. Uncheck the "Create a Snapshot of the current machine state" box and then click the "Restore" button.

6. You should now see in the left box the openSUSE (Snapshot 11-3) with a status of "Powered Off." Power it on by double clicking it.



openSUSE (Snapshot 2-1)
Powered Off

```
Base (2/4/2015 1:43 PM)
  Snapshot 2-1 (2/4/2015 4:14 PM)
    Snapshot 3-1 (2/4/2015 6:02 PM)
      Snapshot 4-1 (2/4/2015 6:29 PM)
        Snapshot 6-2 (2/4/2015 6:49 PM)
          Snapshot 6-1 (2/4/2015 7:00 PM)
          Snapshot 7-1 (2/4/2015 7:31 PM)
            Snapshot 8-1 (2/5/2015 12:28 PM)
              Snapshot 8-2 (2/5/2015 12:43 PM)
                Snapshot 8-3 (2/5/2015 12:54 PM)
                  Snapshot 9-1 (2/5/2015 1:21 PM)
                    Snapshot 10-1 (2/5/2015 3:07 PM)
                      Snapshot 10-2 (2/6/2015 12:23 PM)
                        Snapshot 11-1 (2/6/2015 12:53 PM)
                          Snapshot 11-2 (2/6/2015 1:07 PM)
                            Snapshot 11-3 (2/6/2015 1:28 P
                              Snapshot 1-4 (2/6/2015 2:0
                              Snapshot 12-1 (2/6/2015 3:
                                Snapshot 13-1 (2/6/201
```

7. A separate window should open and you should see the openSUSE Linux OS booting.

8. Press **CTRL+ALT+F1** to move to the command line shell.

9. At your login prompt, authenticate to the system as the user: **root** and password: **student**.

10. Change to the /RandD directory by entering **cd /RandD** at the shell prompt.

11. You need to create several Research and Development documents in the RandD directory. However, you need to make sure these documents are secure from prying eyes. Recall from the previous exercise that Others is automatically granted read access to files when you create them. You don't want this to happen. You need Others to have no access at all to any documents created. Do the following:

a. Change the default permissions by entering **umask 027** at the shell prompt.

b. Verify the value of umask by entering **umask** at the shell prompt. It should display 0027.

c. Create a new file named schedule.odt by entering **touch schedule.odt** at the shell prompt.

d. Enter **ls –l** at the shell prompt. Verify that Owner has rw–, Group has r--, and Others has – – – permissions.

12. In a previous exercise, we granted Owner and Group rwx permissions to the RandD directory. However, having the write permission to the directory allows anyone in the research group to delete any file in the directory. We want to configure the directory so that users in the research group can only delete files they actually own. Do the following:

a. At the shell prompt, enter **cd /**.

b. At the shell prompt, add the Sticky Bit permission to the RandD directory by entering **chmod 1770 RandD**.

c. At the shell prompt, enter **ls –l**. Notice that a T has been added to the last digit of the Others portion of the mode of the RandD directory. This indicates that the sticky bit has been set:

```
openSUSE:/ # ls –l
total 105
drwxrwx--T 2 tux research 4096 Mar 18 11:25 RandD
...
```

13. Experiment with the new permissions you just added by logging in as different users in the system and testing what the permissions will and won’t allow you to do.

14. In an earlier exercise, we created a user named dtracy. However, because we didn’t use the –m option when we created him, he doesn’t have a home directory. Using what you’ve learned, do the following:

a. su to the dtracy account (**su dtracy**).

b. Move to the RandD folder if not there already by entering **cd /home/RandD**.

c. Attempt to delete any of the files located in the RandD folder with the rm utility (**rm design_doc.odt or rm schedule.odt**).

d. Can you delete the files? You should not be able to. The Sticky Bit on the RandD directory will only permit the owner of the file, in this case root and student, to delete those files. Without the Sticky Bit applied users with certain permissions to the RandD directory could delete the files within the directory regardless of their permissions to the file.

e. Switch back to the root user (**su -**). Remove the Sticky Bit by entering **chmod 0770 /RandD**. Switch back to the dtracy user (**su dtracy**) and try to delete either of the files (**rm design_doc.odt or rm schedule.odt**) located in the RandD directory as the dtracy user. The dtracy user should be able to now delete the files. The user student and root might not be too happy about that.

--End of Practical Exercise--