**Modifying File and Directory Permissions**

**Scenario**

You're concerned about how to protect files and directories on a Linux server. You will interpret the existing permissions of a few files, and then configure permissions for the file owner, the group, and all others for files and directories.

**Objectives**

Completing this activity will help you to use content examples from the following syllabus objectives:

* 3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership

**Configuring permissions**

1. Log in as student01 with Pa22w0rd as the password.
2. Enter ls -l to see the permissions string for files and directories in the **student01** home directory.

Review the permissions assigned, identifying which bits are configured for the owner, the group, and all others.

1. Enter ls -l /etc/ssh/sshd\_config to view the permissions for this configuration file.
2. Write down the permissions for the owner, group, and others.

Owner:  


Group:  


Other:  


1. Enter ls -l /var/log/cron to view the permissions for this log file.
2. Write down the permissions for the owner, group, and others.

Owner:  


Group:  


Other:  


**Create a test directory and file you can configure the permissions for**

1. Enter mkdir permissions-demo to create a directory in the **student01** home directory.
2. Enter cd permissions-demo to change to that directory.
3. Enter mkdir DirA to create a permissions demonstration directory named **DirA**.
4. Enter touch file1 to create a permissions demonstration file named **file1**.
5. Enter ls -l to display the current permissions on both objects.

**Configure permissions for the test directory and file using absolute mode.**

1. Enter chmod 755 DirA to set permissions on **DirA**.
2. Enter ls -l to see how the permissions have changed on the directory.
3. Enter chmod 660 file1 to set permissions on **file1**.
4. Enter ls -l to see how the permissions have changed on **file1**.
5. Enter chmod 750 DirA to set different permissions on **DirA**.
6. Enter ls -l to see how the permissions have changed on **DirA**.
7. Enter chmod 744 file1 to configure permissions on **file1**.
8. Enter ls -l and note the permissions changes.

**Configure permissions for the test directory and file using symbolic mode.**

1. Enter chmod o+r DirA to set permissions on **DirA**.
2. Enter ls -l to see how the permissions have changed on **DirA**.
3. Enter chmod go+rw file1 to set different permissions on **file1**.
4. Enter ls -l to see how the permissions have changed on **file1**.
5. Enter chmod go-rwx DirA to set permissions on **DirA**.
6. Enter ls -l and note the permissions changes on **DirA**.
7. Enter chmod go-w file1 to set permissions on **file1**.
8. Enter ls -l and note the permissions changes on **file1**.

The final permissions state of the directory should be: drwx------

The final permissions state of the file should be: -rwxr--r--

**Modifying Default Permissions**

**Scenario**

One of the Develetech employees, Chris Mason, wants to create files and directories with nondefault permissions so he can share them more easily with a co-worker. Since the requested change does not violate the Develetech security policy, it has been approved. You will implement the change for Chris.

**Objectives**

Completing this activity will help you to use content examples from the following syllabus objectives:

* 3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership

**Display the current default permissions settings for users that create new files and directories.**

1. Enter umask to display the default **umask** value that defines default permissions for newly-created files and directories.

Verify that the default mask is **0002**

For standard users, no advanced permissions are set by default (the first 0), owner and group permissions aren't masked, and other user permissions are masked by 2

**Configure Chris Mason's .bashrc file with a non-standard umask value.**

1. Enter sudo vim /home/cmason/.bashrc to open the file in a text editor.
2. Press **Page Down** to move the cursor to the bottom of the file.
3. Press **i** to enter Insert mode.
4. Add the following text on a new line:

umask 022

1. Press **Esc** to exit Insert mode.
2. Enter **:wq** to save and close the file.

**Test the new default permissions.**

1. Enter su - cmason to switch credentials.
2. Enter Pa22w0rd when prompted.
3. Enter umask to view the current permissions default.

You should see the 0022 value that was configured in the steps above.

1. Enter touch test-file to create a new file named **test-file**.
2. Enter ls -l and verify that the permissions for **test-file** match the newly configured umask value.

The permissions should be: -rw-r--r--

1. Enter exit to return to your student account.

**Modifying File and Directory Ownership**

**Scenario**

You will create a Graphics department directory where department members can store content. You will investigate default ownership and group associations, and then create the /Graphics directory. You will configure ownership and group associations of the directory and files.

**Objectives**

Completing this activity will help you to use content examples from the following syllabus objectives:

* 3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership

**Display the current ownership and group associations for files and directories**

1. Enter ls -l /var/log/cron to view ownership and group details about the **cron** log file.

The root user is the owner, and the root group is the group.

1. Enter ls -l /etc/ssh/sshd\_config to view ownership and group details about th **sshd** configuration file.

The root user is the owner, and the root group is the group.

1. Enter sudo ls -l /home/cmason to view ownership and group details about the contents of **cmason**'s home directory.

The cmason user is the owner, and the cmason group is the group.

**Create a directory and populate the directory with files, then manage the ownership values.**

1. Enter sudo mkdir /Graphics to create a directory named **Graphics** at the root of the file system.
2. Enter sudo touch /Graphics/file1 to create a file named **file1** in the **Graphics** directory.
3. Repeat this command with **file2** and **file3** to create two additional empty files inside the directory.
4. Enter ls -l /Graphics to display the ownership information.

The owner is the creator; in this case that is the root account, due to the use of the sudo command.

1. Enter sudo chmod -R 774 /Graphics to set permissions on the **/Graphics** directory and its contents.
2. Enter sudo ls -l /Graphics to view the new permissions.

A picture containing text

Description automatically generated

**Change the owner and group values of the /Graphics directory and its contents**

1. Enter sudo chown -R :GraphicsDept /Graphics to set the group association as the **GraphicsDept** group.
2. Enter sudo ls -ld /Graphics to display the changes.
3. Enter sudo chown rstanley /Graphics/file2 to change the ownership of **file2** to **Rose Stanley**.
4. Enter sudo ls -l /Graphics to confirm **rstanley** is now the owner of **file2**.

# Configuring SGID Permissions and Sticky Bits

## Scenario

Some users have noted that the group associations for /Graphics are not applied to files created in the directory. One user also complained that another user accidentally deleted one of her files. You are asked to correct these concerns.

## Objectives

Completing this activity will help you to use content examples from the following syllabus objectives:

* 3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership

## Use SGID to automatically set group associations for newly created files in the /Graphics directory

1. Enter ls -ld /Graphics to see the default permissions on the **/Graphics** directory.
2. Enter sudo chmod g+s /Graphics to set the SGID on **/Graphics** so that newly created files will get the group association.
3. Enter ls -ld /Graphics to display the new permissions.
4. Enter su - rstanley and enter Pa22w0rd to switch to Rose Stanley's credentials.
5. Enter cd /Graphics and then touch file4 to create a file named **file4**.
6. Enter ls -l and confirm **rstanley** is the owner and the group is **GraphicsDept** for **file4**.
7. Enter exit to return to the **student01** login.

### Use the sticky bit to better protect files from deletion by anyone but their owner

1. Enter sudo chmod +t /Graphics to configure the sticky bit on the **/Graphics** directory.
2. Enter su - jrobinson and enter Pa22w0rd to switch to Jerry Robinson's credentials.
3. Enter cd /Graphics to move to the **/Graphics** directory.
4. Enter rm file4 to attempt to delete **file4**, which is owned by **rstanley**.

Note that you receive an "Operation not permitted" response. If this were a permissions issue, you would receive an "access denied" response instead. Even though jrobinson is a member of the GraphicsDept group, and that group has the permissions to delete a file in this directory, the sticky bit is preventing file deletion from a non-owner.

1. Enter exit to return to the **student01** login.

**Configuring ACLs**

**Scenario**

The Graphics department has requested that the Marketing department be given read-only access to the /Graphics directory. With standard permissions, only one group association can exist. You will use access control lists (ACLs) to ensure that both the Graphics and Marketing departments have access.

**Objectives**

Completing this activity will help you to use content examples from the following syllabus objectives:

* 3.1 Given a scenario, apply or acquire the appropriate user and/or group permissions and ownership

**Set an ACL for the Marketing department.**

1. Enter sudo getfacl /Graphics to view the current ACL on the **Graphics** directory.
2. Enter sudo setfacl -R -m g:MarketingDept:r /Graphics to grant read-only permissions to the **MarketingDept** to the **/Graphics** directory and its contents.

You can ignore the "Operation not permitted" warning about the README file; the ACL settings will still apply to all other objects.

1. Enter sudo getfacl /Graphics to view the new level of access for the **MarketingDept**.

Text

Description automatically generated