Linux File Permissions Task - CentOS

**1. Change File Permissions using chmod (Two Methods)**

To set the following permissions:  
- Owner: read (r) and write (w) permissions  
- Group: write (w) and execute (x) permissions  
- Others: execute (x) permission  
  
First Method (Symbolic):  
```bash  
chmod u=rw,g=wx,o=x file.txt  
```  
Second Method (Numeric):  
```bash  
chmod 731 file2.txt  
```  


**2. Change Default Permissions to 027**

To set the default file permissions to 027 (umask), run the following command:  
```bash  
umask 027  
```  
This sets the following default permissions for newly created files and directories:  
- Owner: read and write  
- Group: read only  
- Others: no permissions



**3. Maximum Default Permissions for Files and Directories**

The maximum permission a file can have by default when created depends on the 'umask' setting. If the 'umask' is 000, the maximum default permissions would be:  
- File: 666 (read and write for owner, group, and others)  
- Directory: 777 (read, write, and execute for owner, group, and others)  
However, files are typically created with 666 and directories with 777 permissions, modified by the 'umask'.



**4. Change Default Permissions for Owner, Group, and Others**

To change the default file permissions so that the owner gets read and execute permissions, the group gets full permissions, and others have no permissions, use the following command:  
```bash  
umask 037  
```  
This results in the following default permissions:  
- Owner: read and execute  
- Group: read, write, and execute  
- Others: no permissions

**5. Create a File and Directory, and Note Permissions**

To create a file and a directory, use the following commands:  
```bash  
touch testfile  
mkdir testdir  
```  
After creation, check the permissions using 'ls -l':  
```bash  
ls -l testfile testdir  
```  
This will display the default permissions based on the current 'umask' settings.



**6. Copy /etc/passwd to Home Directory and Compare Permissions**

To copy the '/etc/passwd' file to your home directory, use the following command:  
```bash  
cp /etc/passwd ~/passwd\_copy  
```  
Before copying, the '/etc/passwd' file has the following permissions:  
```bash  
ls -l /etc/passwd  
```  
After copying, the new file will have permissions determined by your 'umask' settings. Use 'ls -l ~/passwd\_copy' to view the permissions. The difference occurs because when copying, the file inherits the permissions based on the 'umask' value instead of preserving the original.

**7. Create a File with 444 Permissions and Try Editing/Removing**

To create a file with read-only permissions for all users, use the following command:  
```bash  
touch readonlyfile  
chmod 444 readonlyfile  
```  
Attempt to edit the file:  
```bash  
nano readonlyfile  
```  
You will not be able to save changes. Similarly, if you try to remove the file with 'rm readonlyfile', you will likely encounter a permission error, unless you are the owner and force the deletion.

**8. Difference Between "x" Permission for Files and Directories**

The 'x' (execute) permission behaves differently for files and directories:  
- For files: The 'x' permission allows the file to be executed as a program or script.  
- For directories: The 'x' permission allows users to enter (cd) the directory and access its contents.  
Without 'x' permission on a directory, users can list the contents (if read permission is granted) but cannot access or execute anything within the directory.