

**Demonstration –P-02-01 – 5 minutes**

**Linux File ACLs**



Instructor Notes Begin

This Demonstration will show students some of the built in access controls in the default Linux file system, and how to manipulate them.

The screen captures shown here have been taken from a Red Hat LINUX Version 9.0 system using a command line interface.

Instructor Notes End

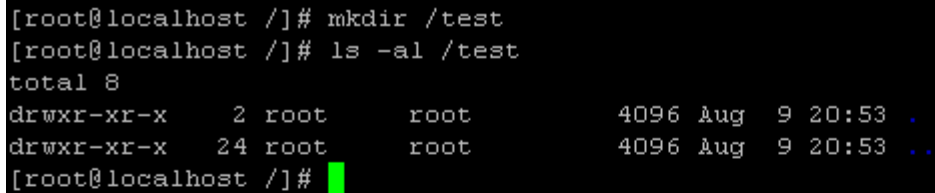


Here are the figures in this Demonstration:

Figure 1 - Making the <code>/test</code> directory .....	2
Figure 2 - Directory Listing.....	3
Figure 3 - Directory Listing after the Change .....	4
Figure 4 - Unsuccessful Directory Listing .....	5
Figure 5 - Successful Directory Listing.....	6

1. On any Red Hat or other Linux system, open a terminal window (command shell).
2. Login to the host as the `root` user.
3. Once logged in to the system as the `root` user, create a new directory calls `/test` with the following command (as shown in Figure 1):

```
mkdir /test
```

A terminal window with a black background and white text. The prompt is [root@localhost ~]#. The first command is mkdir /test. The second command is ls -al /test. The output shows the directory listing for /test, indicating it is a directory with permissions drwxr-xr-x, owned by root, and has a size of 4096 bytes. The prompt returns to [root@localhost ~]#.

```
[root@localhost ~]# mkdir /test
[root@localhost ~]# ls -al /test
total 8
drwxr-xr-x  2 root    root      4096 Aug  9 20:53 .
drwxr-xr-x 24 root    root      4096 Aug  9 20:53 ..
[root@localhost ~]#
```

I

**Figure 1 - Making the `/test` directory**

4. Once the directory has been created, list the contents of the / directory with the following command (the output will look similar to Figure 2)

```
ls -al /
```

```
drwxr-xr-x  2 root    root      4096 Jun 15 13:39 bin
drwxr-xr-x  4 root    root     2048 Jun 15 13:39 boot
drwxr-xr-x  6 root    root      4096 Jan 18  2005 dell
drwxr-xr-x 22 root    root    118784 Jun 30 11:24 dev
drwxr-xr-x 70 root    root      8192 Aug  3 12:45 etc
-rw-r--r--  1 root    root    23122 Feb  8 08:54 .fonts.cache-1
drwxr-xr-x  4 root    root      4096 Jul 13 10:40 home
drwxr-xr-x  2 root    root      4096 Jan 24  2003 initrd
drwxr-xr-x 11 root    root      4096 Jun 15 13:38 lib
drwxrwxrwx  5 root    root      4096 Feb 10 15:29 local_store
drwx----- 92 root    root    24576 Jan 18  2005 lost+found
drwxr-xr-x  2 root    root      4096 Nov 11  2004 misc
drwxr-xr-x  5 root    root      4096 Apr 28 13:37 mnt
drwxr-xr-x  2 root    root      4096 Jan 24  2003 opt
dr-xr-xr-x 99 root    root        0 Jun 30 07:23 proc
drwxr-x--- 21 root    root      4096 Aug  9 20:42 root
drwxr-xr-x  2 root    root      8192 Jun 15 13:39 sbin
drwxr-xr-x  2 root    root      4096 Aug  9 20:53 test
drwxrwxrwt 18 root    root      4096 Aug  9 11:56 tmp
drwxr-xr-x 15 root    root      4096 Apr 27  2004 usr
drwxr-xr-x 20 root    root      4096 Feb 14 09:33 var
drwxrwxrwx 10 root    root      4096 Jun 23 08:54 vmware
drwxr-xr-x  2 root    root      4096 Feb 14 11:44 windows
[root@localhost /]#
```

**Figure 2 - Directory Listing**

5. Notice the set of characters to the left of the listing of files and directories on the right – the ones which start `drwxr-xr-x`. These are the file attributes for the Linux file system.
- The first character identifies if the corresponding line is a directory (d) or not.
  - The next three characters describe the privileges of the owner of this file/directory. They are (from left to right) the ability to Read, Write, and Execute that file (or in the cases of a directory, the ability to read, write, or examine the contents of the directory).
  - The middle three characters describe the same privileges (read, write, execute) which are assigned to the group to which the owner of the file belongs. For example, if I am in the student group and the file permissions allow members of my group to write to a file which I have created, anyone in the student group will have write privileges on that particular file.
  - The last three characters describe the privileges of the rest of the users (commonly referred to as the ‘world’). Any authenticated user on the system will have whatever privileges show up in the ‘world’ group.
6. To change the permissions, we will use a command called `chmod` – which changes the ‘mode’ of the file. To change the mode of the file, enter the following command:

```
chmod 740 /test
```

7. Perform a listing of this directory, enter the following command (the output will be similar to that shown in Figure 3):  
`ls -al /test`
8. Notice that the privileges of the directory (shown in the directory in this listing) have changed to allow RWX to the owner, R to the group, and nothing to the world.

```
[root@localhost /]# ls -al /test
total 8
drwxr-----  2 root    root        4096 Aug  9 20:53 .
drwxr-xr-x   24 root    root        4096 Aug  9 20:53 ..
[root@localhost /]#
```


I

**Figure 3 - Directory Listing after the Change**

9. We can test out these ACLs by logging in as another user. If you do not have another account on this host, use the following two commands to create a user called student and to assign that user a password:  
`useradd student`  
`passwd student`
10. Change to the student account with the following command:  
`su student`

11. Attempt to change to the /test directory with the following command (you will be denied and the output should look like that in Figure 4).

```
cd /test
```

A terminal window with a black background and white text. The prompt is [student@localhost ~]. The user enters 'cd /test'. The output is 'bash: cd: /test: Permission denied'. The prompt returns to [student@localhost ~]. A green cursor is visible on the second line.

```
[student@localhost ~]$ cd /test
bash: cd: /test: Permission denied
[student@localhost ~]$
```

**Figure 4 - Unsuccessful Directory Listing**

12. To get back to the root user shell, type `exit`.
13. Change the permissions of the /test directory to allow world access with the following command:  

```
chmod 755 /test
```
14. Change to the student account again (`su student`).

15. List the contents of the `/test` directory with the following command (it will now be successful and look like the output shown in Look at the output from the **ethereal** capture, which should be similar to that in Figure 5:

```
ls -al /test
```

```
[student@localhost ~]$ cd /test
bash: cd: /test: Permission denied
[student@localhost ~]$ exit
exit
[root@localhost ~]# chmod 755 /test
[root@localhost ~]# su student
[student@localhost ~]$ ls -al /test
total 8
drwxr-xr-x  2 root    root      4096 Aug  9 20:53 .
drwxr-xr-x 24 root    root      4096 Aug  9 20:53 ..
[student@localhost ~]$
```

Figure 5 - Successful Directory Listing