CS 447/647

Filesystem(s)

Overview

- File Attributes
- Quotas
- Filesystems

File Attributes

- The permission bits
- setuid and setgid
- The sticky bit

The permissions bits

- AKA Portable Operating System Interface (POSIX)
- Made up of 9 bits in 3 groups
  - user (u) 000
  - group (g) 000
  - other (o) 000

000000000

u g o

001 = 1 Execute

010 = 2 Write

100 = 4 Read

755 = 111 101 101
User - read\write\execute
Group - read\execute
Other - read\execute

Octal	Binary	Perms	Octal	Binary	Perms
0	000	---	4	100	r--
1	001	--x	5	101	r-x
2	010	-w-	6	110	rw-
3	011	-wx	7	111	rwx

Spec	Meaning
u+w	Adds write permission for the owner of the file
ug=rw,o=r	Gives r/w permission to owner and group, and read permission to others
a-x	Removes execute permission for all categories (owner/group/other)
ug=srx,o=	Makes setuid/setgid and gives r/x permission to only owner and group
g=u	Makes the group permissions be the same as the owner permissions

setuid and setgid

- `setuid`
  - Octal 4000
  - Run as owner
  - Used by `passwd` command to change passwords
  - Disabled with `nosuid` mount option
    - `mount -o nosuid /dev/sdc1 /data`
- `setgid`
  - Octal 2000
  - Runs as group
  - When set on a directory all files created in the directory inherit the group

The sticky bit

- Octal 1000
- Historical used as a modifier for binaries
  - Introduced in 1974 to speed up execution of binaries
  - Now obsolete
- If set on a directory, it only allows deletion of files by
  - File Owner
  - Directory Owner
  - root

Permissions

- chmod - Change file mode bits
- chown - Change file owner and group
- chgrp - Change file group

```
chmod 700 1          #Owner RWX, Group ---, Other ---
chmod 755 1          #Owner RWX, Group R-X, Other R-X
chmod 2000 1         #setgid on the directory
chmod -R 700 1       #Recurisve chmod
#chown
chown root:root 1    #Change user and group to root
chown -R root:root   #Recursive chown
chown 1000:1000      #Chown with UID and GID
```

Permissions

- `chmod`, `chown`, `chgrp`
- Use `-R` sparingly
  - Clobbers permissions
- Better to use find with ch*

```
find /path -type f -exec chown 644 {} \;

find /path -type d -exec chown 755 {} \;
```

Permissions - umask

- 9 bits that represents what permissions to take away upon file creation
- Stored in /etc/login.defs and applied via PAM
- Unique per process
  - /proc/$PID/status

```
ps aux | grep $USER
grep umask /proc/$PID/status
```

Additional Flags - `lattr` and `chattr`

Flag	FS[a]	Meaning
A	XBE	Never update access time (`st_atime`; for performance)
a	XBE	Allow writing only in append mode[b]
C	B	Disable copy-on-write updates
c	B	Compress contents
D	BE	Force directory updates to be written synchronously
d	XBE	Do not back up; backup utilities should ignore this file
i	XBE	Make file immutable and undeletable[b]
j	E	Keep a journal for data changes as well as metadata
S	XBE	Force changes to be written synchronously (no buffering)
X	B	Avoid data compression if it is the default

a. X = XFS, B = Btrfs, E = ext3 and ext4
b. Can be set only by root

Access Control Lists

- Not a niche
- Very common on Windows
- Any complex environment will need them
  - NFS
  - SAMBA*
  - High-Performance Computing
  - GPFS, ZFS, etc.
- Two types
  - POSIX
  - NFSv4

POSIX ACLs

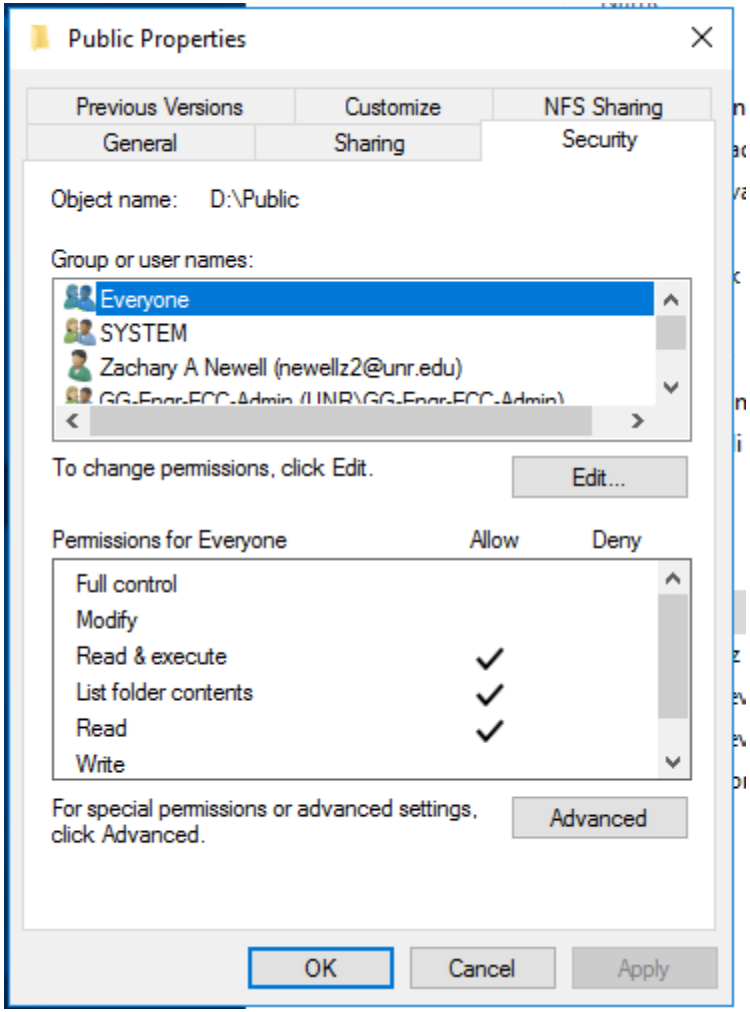
`setfacl` - set ACL

`getfacl` - read ACL

```
apt install -y acl
setfacl -m "u:newellz2:rw" file
setfacl -m "g:cs447:rx" file
setfacl -R -m "u:newellz2:rw" folder
setfacl -d -m "u:newellz2:rw" folder #Files inherit this ACL
```

Windows Permissions

- All permissions are ACLs
- Graphical
  - VB
  - PowerShell
- Inheritance
- System Accounts\Roles
  - Authenticated User
  - Domain Computer
  - System
  - Everyone
  - Guest
  - Anonymous


Public Properties
Previous Versions
Customize
NFS Sharing
General
Sharing
Security
Object name: D:\Public
Group or user names:
Everyone
SYSTEM
Zachary A Newell (newellz2@unr.edu)
To change permissions, click Edit.
Edit...
Permissions for Everyone
Allow
Deny
Full control
Modify
Read & execute
List folder contents
Read
Write
For special permissions or advanced settings, click Advanced.
Advanced
OK
Cancel
Apply

Advanced Security Settings for Public

Name: D:\Public

Owner: Zachary A Newell (newellz2@unr.edu) Change

Permissions | Share | Auditing | Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Allow	Domain Computers (RD\Dom...	Read & execute	None	This folder, subfolders and files
Allow	Everyone	Read & execute	None	This folder, subfolders and files
Allow	SYSTEM	Full control	None	This folder, subfolders and files
Allow	Zachary A Newell (newellz2@...	Full control	None	This folder, subfolders and files
Allow	GG-Engr-ECC-Admin (UNR\G...	Full control	None	This folder, subfolders and files
Allow	Guest (ECC\Guest)	Read & execute	None	This folder, subfolders and files
Allow	ANONYMOUS LOGON	Read & execute	None	This folder, subfolders and files

Add | Remove | View

Enable inheritance

☐ Replace all child object permission entries with inheritable permission entries from this object

OK | Cancel | Apply

Permission Entry for Public

Principal: Zachary A Newell (newellz2@unr.edu) Select a principal

Type: Allow

Applies to: This folder, subfolders and files

Advanced permissions: Show basic permissions

- [x] Full control
- [x] Traverse folder / execute file
- [x] List folder / read data
- [x] Read attributes
- [x] Read extended attributes
- [x] Create files / write data
- [x] Create folders / append data
- [x] Write attributes
- [x] Write extended attributes
- [x] Delete subfolders and files
- [x] Delete
- [x] Read permissions
- [x] Change permissions
- [x] Take ownership

- [ ] Only apply these permissions to objects and/or containers within this container

Clear all

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

User | Group | Member of each | Value | Click Add items | Add items | Remove

Add a condition

OK Cancel

Windows Permissions

```
PS D:\> Get-ACL -Verbose .\Public |  Format-List


Path   : Microsoft.PowerShell.Core\FileSystem::D:\Public
Owner  : UNR\newellz2
Group  : UNR\Domain Users
Access : Everyone Allow  ReadAndExecute, Synchronize
         NT AUTHORITY\ANONYMOUS LOGON Allow  ReadAndExecute, Synchronize
         NT AUTHORITY\SYSTEM Allow  FullControl
         UNR\newellz2 Allow  FullControl
         UNR\GG-Engr-ECC-Admin Allow  FullControl
         RD\Domain Computers Allow  ReadAndExecute, Synchronize
         ECC\Guest Allow  ReadAndExecute, Synchronize
Audit  :
Sddl   : O:S-1-5-21-1275210071-1123561945-682003330-119339G:S-1-5-21-127521
         0a9;;;WD)(A;OICI;0x1200a9;;;AN)(A;OICI;FA;;;SY)(A;OICI;FA;;;S-1-5-
         CI;FA;;;S-1-5-21-1275210071-1123561945-682003330-202991)(A;OICI;0x
```

ACLs Exercise

1. Open a root terminal.
2. Use **`setfacl -m g:account:rx /data/sales`** to give the group account read permissions on the **`/data/sales`** directory, and use **`setfacl -m g:sales:rx /data/account`** to give the group sales read permissions on the **`/data/account`** directory.
3. Use **`getfacl /data/`** to verify that the permissions have been set the way you intended to.
4. Use **`setfacl -m d:g:account:rx,g:sales:rwx /data/sales`** to set the default ACL for the directory sales.
5. Add the default ACL for the directory /**`data/account`** by using **`setfacl -m d:g:sales:rx,g:account:rwx /data/account`**.
6. Verify that the ACL settings are effective by adding a new file in **`/data/sales`**. Use **`touch /data/sales/newfile`** and use **`getfacl /data/sales/newfile`** to check the current permission assignments.

Quotas

xfs

- Created in 1993 by Silicon Graphics Inc. (SGI)
- A 64-bit journaled filesystem
- Suited for large files and filesystems
  - 8 exbibytes max file size
  - 2^64 (1.8446744e+19) max number of files
- Supports
  - Quotas
  - Snapshots
  - Live resizing (growing)
- Standard FS in SUSE and RedHat

Exercise

```
mkdir -p /var/tmp/quotas && cd /var/tmp/quotas

truncate -s 1G xfs_disk.img #Create a sparse file

losetup --find --show xfs_disk.img #Mount the file as a loop
dev

mkfs.xfs /dev/loop0 #man mkfs.xfs

mkfs.xfs -f -L data  /dev/loop0 #man mkfs.xfs

mount -o defaults,uquota,gquota /dev/loop0 /mnt
```

Exercise

```
adduser --disabled-password --gecos "" robert

mkdir /mnt/robert && chown robert /mnt/robert

xfs_quota -x -c 'limit bsoft=75m bhard=100m robert' /mnt

xfs_quota -x -c 'limit isoft=3 ihard=4 robert' /mnt #inode limit

dd if=/dev/zero of=/mnt/robert/file.bin bs=1M count=80
chown robert /mnt/robert/file.bin

xfs_quota -x -c 'state'
```