Access Control

File Permissions

- Files that are not scripts do not have x
- Directories have x because users can cd into them

d	r	w	x	r	w	x	r	w	x
file type	user read	user write	user execute	group read	group write	group execute	others read	others write	others execute

Numerical Permissions

- 7 = rwx
- 6 = rw
- 5 = rx
- 4 = r
- 2 = w
- 1 = x
- 0 = -

Owner of parent directory can still delete a file or subdirectory

chmod u+rw filename	user owner add rw
chomd g-w filename	group owner remove w
chmod o+r filename	others owner add r
chmod a-r filename	all owners remove r
chmod 755 filename	set to rwxr-xr-x
chmod 644 filename	set to rw-r--r--
chmod 777 filename	set to rwxrwxrwx
chown root filename	change user owner to root
chgrp root filename	change group owner to root

Access Control Lists (ACLs)

ACLs are used to grant rwx to a specific user, separate from the file owners

- As you assign ACL to a file/directory it adds + to the permissions
- w permission does not include delete (owner only)

getfacl	get file acl
setfacl -m u:user:rwx filename	add permissions for user
setfacl -m g:group:rw filename	add permissions for group
setfacl -rm u:user:rwx dirname	add permissions for directory -r recursive

setfacl -x u:user filename	remove entry for user
setfacl -b filename	remove all entries

Revision #1
Created 2026-07-05 06:13:50 UTC by Admin
Updated 2026-07-05 06:13:54 UTC by Admin