

14741/18631 HW3 Writeup

Hao Zhang

TOTAL POINTS

60 / 60

QUESTION 1

1 Access Control 60 / 60

- **10 pts** No Explanation of Design

+ **60** Point adjustment

Question 1

1. Set up container:

- a. Creating shared folder: `mkdir shared_folder`
- b. Run docker: `docker run --name hw3 -d -t \`
`-v "$(pwd)"/shared_folder:/shared_folder \`
Ubuntu:18.04 (following commands refer to hw3 guide)

2. Create Users and groups (20001 is gid(group id) and 10002 is uid(user id)):

- a. Create groups: `groupadd -g 20001 instructors`
- b. Create users based on its group: `useradd -g 20001 -u 10002 hh`

3. Create ACL policy:

- a. Create all directories for handouts, submissions, etc with `mkdir`
- b. Set policy -m: For example, in terms of handouts, instructors would have read, write access. Using `setfacl -m "g:instructors:rwX" handouts`. This command set the group instructor with read, write, and execute access to handouts directory. (Note: execute is needed to open a directory)
- c. Set policy -dm: for the same handouts example, if a TA write a new handout, our instructor should still be able to view and write it. Therefore, we need default access: `setfacl -dm "g:instructors:rwX" handouts`. Default access is used when a new file is created, it will follow the acl policy of its parent folder(directory)
- d. Verify policy: using `getfacl handouts`, we can view the ACL policy we created (ls -l servers similar purpose). Note: the effective acl is the actual access for a user, which is a combination of masking and ACL policy(extended rule)

4. Testing

- a. Switch user: `su hh`
- b. Create file in handouts folder: `touch new.txt`
- c. Read file: `cat new.txt`

With proper ACL policy, I will be able to complete the testing without being noticed for permission denied

5. Wrapping up

- a. Tar the file: `tar --acls -cpf HW3.tar assignments`
- b. Copy to shared folder for submission: `cp HW3.tar shared_folder/`

Take away:

1. With ACL, we can implement a role-based access control model.
2. Group access permission helps organize access. For example, a fired TA, who is removed from TA group, will lose access immediately
3. It is hard to imagine an admin that will do this ACL policy for an entire company. There should be better way to visualize and organize access chart

1 Access Control 60 / 60

- 10 pts No Explanation of Design

+ 60 Point adjustment