1. Meredith Palmer must be able to run systemctl restart vsftpd (not start/stop, just restart) on Machine C. She must be able to read and modify all files and folders under /var/ftp/.

To do this, [ systemctl restart vsftpd ]

SSH to Machine C.

Open sudoers by

sudo visudo

**( this is now opening in vi editor)**

then goto the end of the document.

append following code. (Press I to insert)

mpalmer ALL=/usr/sbin/service vsftpd restart, /bin/systemctl restart vsftpd

save and exit. ( press **esc ,** type **:wq** , hit **Enter** )

now log in as mpalmer.

todo that.

su – mpalmer

enter password: “password”

To Do this [read and modify all files and folders under /var/ftp/.]

issue following command on machine C.

First change the ownership of the file to mpalmer

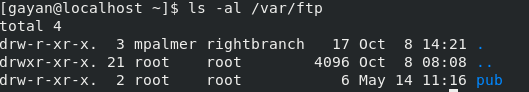
sudo chown mpalmer: /var/ftp

now set the user permission to read and modify only ( no executable access)

sudo chmod -R u=rw- /var/ftp

check the file permissions at the directory by issuing

ls -al /var/ftp



Should look like above.

Alternative method.

install acl if not already installed.

sudo yum install acl

now

setfacl -m u:mpalmer:-rw- /var/ftp

1. Pam Beesly, Kelly Kapoor, and Andy Bernard must be allowed to restart the http daemon (not start/stop, just restart) on machine B through sudo, and modify all files under /var/www/dundermifflin/ without affecting the user apache’s ability to read them.

all three of them belong to the “sales” subgroup in all machines.

for this case ssh to machine B.

there open sudoers by

sudo visudo

append following line at the end.

%sales ALL=/usr/sbin/service httpd restart, /bin/systemctl restart httpd

save and exit.

You **can su – pbeesly** and check restarting the httpd service by,

sudo systemctl restart httpd

Todo this [modify all files under /var/www/dundermifflin/]

since they already belong to the group sales we can change ownership to the sales group.

sudo chgrp sales /var/www/dundermifflin/

then set permissions

sudo setfacl -m g:sales:-w- /var/www/dundermufflin/



1. The default umask must be adjusted on machines A, C, D, and E so that when new directories are created the owner can read, write, and execute, the group can read, write and execute, and others have no access. You need to do either the reading from the prior homework or some independent research to identify how to do this.

**SSh to A,B,C,D**

**then do all the steps in each machine.**

open /etc/bashrc or /etc/profile

and append the umask line. Changes will take effect from the next login.

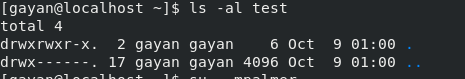
for the requested scenario umask should be,

umask 007

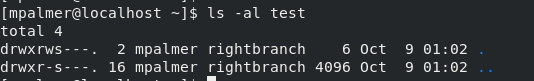
which is calculated by, umask user,group,others

* **Octal value** : Permission
* **0** : read, write and execute
* **1** : read and write
* **2** : read and execute
* **3** : read only
* **4** : write and execute
* **5** : write only
* **6** : execute only
* **7** : no permissions

before



after the umask change ( and logged in as another user. logout same user and logging back in also works)



1. Access on each server should be restricted such that only users who need to are allowed to log in. The one exception is all users should be allowed to log in on machine E. Access restriction should be imposed using pam\_access so that the /etc/passwd and /etc/shadow files stay consistent across all machines. IMPORTANT: You must explicitly allow root access via SSH. While it is certainly more secure to disallow direct access to root remotely, access to root must be maintained so we can grade your machines.

For this task not clear which users are allowed to log in, and which are not allowed to log in.

So, following configurations are based on the assumption.

* 1. Setting control on machine A.

only kleung, mscott, dschrute has access. (kleung myself is the sys admin)

ssh to machine A.

open

sudo nano /etc/security/**access**.conf

Append following lines to the end.

+: kleung:ALL

+: mscott:ALL

+: dschrute:ALL

-:ALL:ALL

save and exit.

* 1. Setting control on machine B

sysadmin, managers, rightbranch, sales has access

open the

sudo nano /etc/security/**access**.conf

+: kleung:ALL

+: (managers):ALL

+: (rightbranch)::ALL

+: (sales)::ALL

-:ALL:ALL

save and exit.

* 1. Configuring machine C

Only mpalmer,sysadmin and managers has access.

**open the /etc/security/access.conf** and append following.

+: kleung:ALL

+: (managers):ALL

+: mpalmer::ALL

-:ALL:ALL

* 1. Configure machine D

Only sysadmin(kleung), and mscott, dshrute are allowed.

**open the /etc/security/access.conf** and append following.

+: kleung:ALL

+: mscott:ALL

+: dschrute:ALL

-:ALL:ALL

* 1. Configure machine E

All the users are allowed to log in. So no access configuration needed.

1. Sudo access to all commands, on all machines, should be granted to responsible users who have specifically requested it. This includes your own personal account.

Already coverd in above.

1. Michael Scott should be allowed to shut all servers down with no less than 2 hours notice to other users (see man shutdown). He should be limited to shutting them down, not restarting. He should also be allowed to cancel a pending shutdown.

To [all servers down with no less than 2 hours notice ]

log in to all the servers and perform following on each.

open sudoers in each server.

sudo visudo

append the following line.

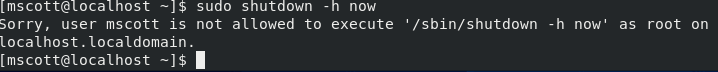
mscott ALL=/sbin/shutdown -P +120, /sbin/shutdown -c

save and exit.

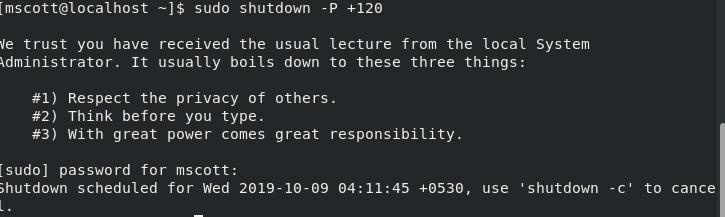
su – mscott ( password is password)

Now try scheduling a shutdown by,

sudo shutdown -h now

**fails.** 

sudo shutdown -P +120

**success. (now don’t forget to cancel the shutdown, otherwise servers will be down and your grade will decrease)** 

sudo shutdown -c

**login to the next server and do the same.**

1. Password changes must be enforced on all servers such that pam ensures that new passwords are at least 10 characters long, and contain at least 2 digits, 2 uppercase, and 1 non alphanumeric character.

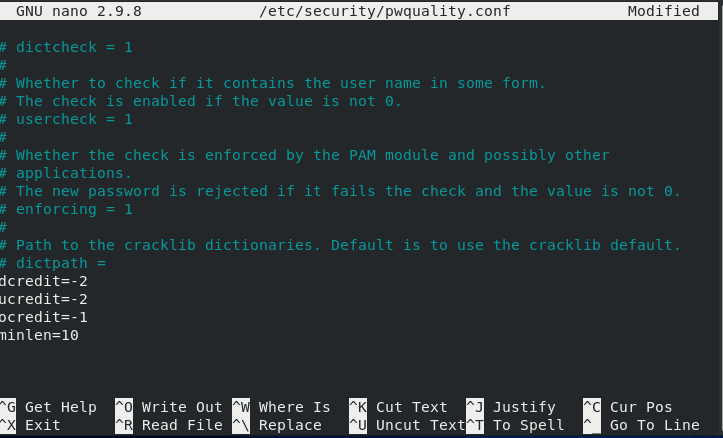
**you have to do this in all servers. log in to each server and**

**dcredit=-2**

**ucredit=-2**

**ocredit=-1**

**minlen=10**



now you can try changing the password by . [ make sure you remember the password ]

passwd

