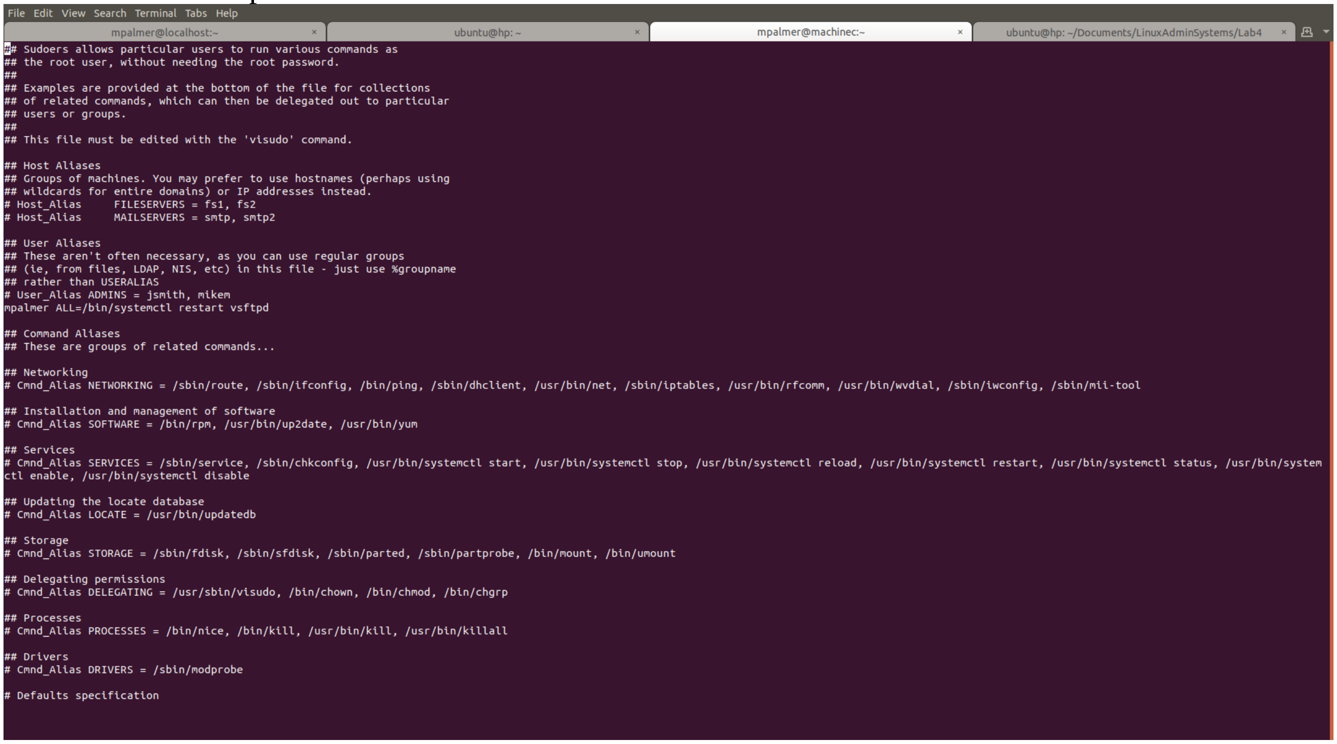
### Ehsan Karimi
### Lab4 Notes

1.
2. Added "mpalmer ALL=/bin/systemctl restart vsftpd" to visudo in machine c
Created a new group ftp_admin:
groupadd ftp_admin
Added users:
gpasswd -M mpalmer,ekarimi,mscott,jhalpert,dschrute ftp_admin
Changed group owner of /var/ftp:
chgrp ftp_admin /var/ftp
setguid for /var/ftp:
chmod 2770 /var/ftp


File Edit View Search Terminal Tabs Help
mpalmer@localhost:~
ubuntu@hp: ~
mpalmer@machinec:~
ubuntu@hp: ~/Documents/LinuxAdminSystems/Lab4

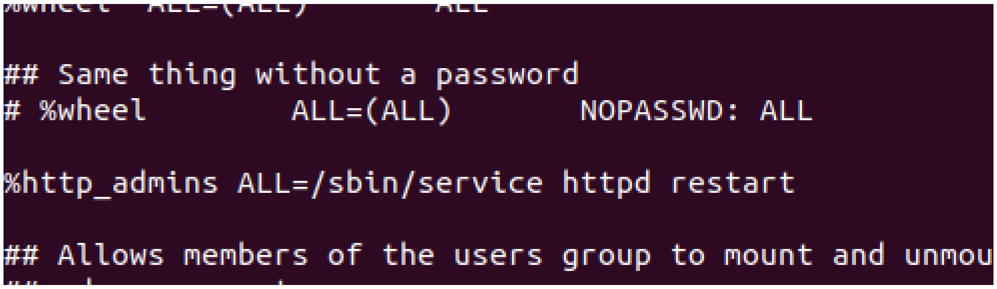
```
## Sudoers allows particular users to run various commands as
## the root user, without needing the root password.
##
## Examples are provided at the bottom of the file for collections
## of related commands, which can then be delegated out to particular
## users or groups.
##
## This file must be edited with the 'visudo' command.

## Host Aliases
## Groups of machines. You may prefer to use hostnames (perhaps using
## wildcards for entire domains) or IP addresses instead.
# Host_Alias     FILESERVERS = fs1, fs2
# Host_Alias     MAILSERVERS = smtp, smtp2

## User Aliases
## These aren't often necessary, as you can use regular groups
## (ie, from files, LDAP, NIS, etc) in this file - just use %groupname
## rather than USERALIAS
# User_Alias ADMINS = jsmith, mikem
mpalmer ALL=/bin/systemctl restart vsftpd

## Command Aliases
## These are groups of related commands...

## Networking
# Cmnd_Alias NETWORKING = /sbin/route, /sbin/ifconfig, /bin/ping, /sbin/dhclient, /usr/bin/net, /sbin/iptables, /usr/bin/rfcomm, /usr/bin/wvdial, /sbin/iwconfig, /sbin/mii-tool

## Installation and management of software
# Cmnd_Alias SOFTWARE = /bin/rpm, /usr/bin/up2date, /usr/bin/yum

## Services
# Cmnd_Alias SERVICES = /sbin/service, /sbin/chkconfig, /usr/bin/systemctl start, /usr/bin/systemctl stop, /usr/bin/systemctl reload, /usr/bin/systemctl restart, /usr/bin/systemctl status, /usr/bin/system
ctl enable, /usr/bin/systemctl disable

## Updating the locate database
# Cmnd_Alias LOCATE = /usr/bin/updatedb

## Storage
# Cmnd_Alias STORAGE = /sbin/fdisk, /sbin/sfdisk, /sbin/parted, /sbin/partprobe, /bin/mount, /bin/umount

## Delegating permissions
# Cmnd_Alias DELEGATING = /usr/sbin/visudo, /bin/chown, /bin/chmod, /bin/chgrp

## Processes
# Cmnd_Alias PROCESSES = /bin/nice, /bin/kill, /usr/bin/kill, /usr/bin/killall

## Drivers
# Cmnd_Alias DRIVERS = /sbin/modprobe

# Defaults specification
```

3. Created a new group http_admins:
groupadd http_admins
Added users:
gpasswd -M apache,ekarimi,pbeesly,kkapoor,abernard,mscott,jhalpert,dschrute http_admins

Changed group owner of /var/www/dundermifflin:
chgrp http_admins /var/www/dundermifflin

setguid for /var/www/dundermifflin:

Added "%http_admins ALL=/sbin/service httpd restart" to visudo in machine B



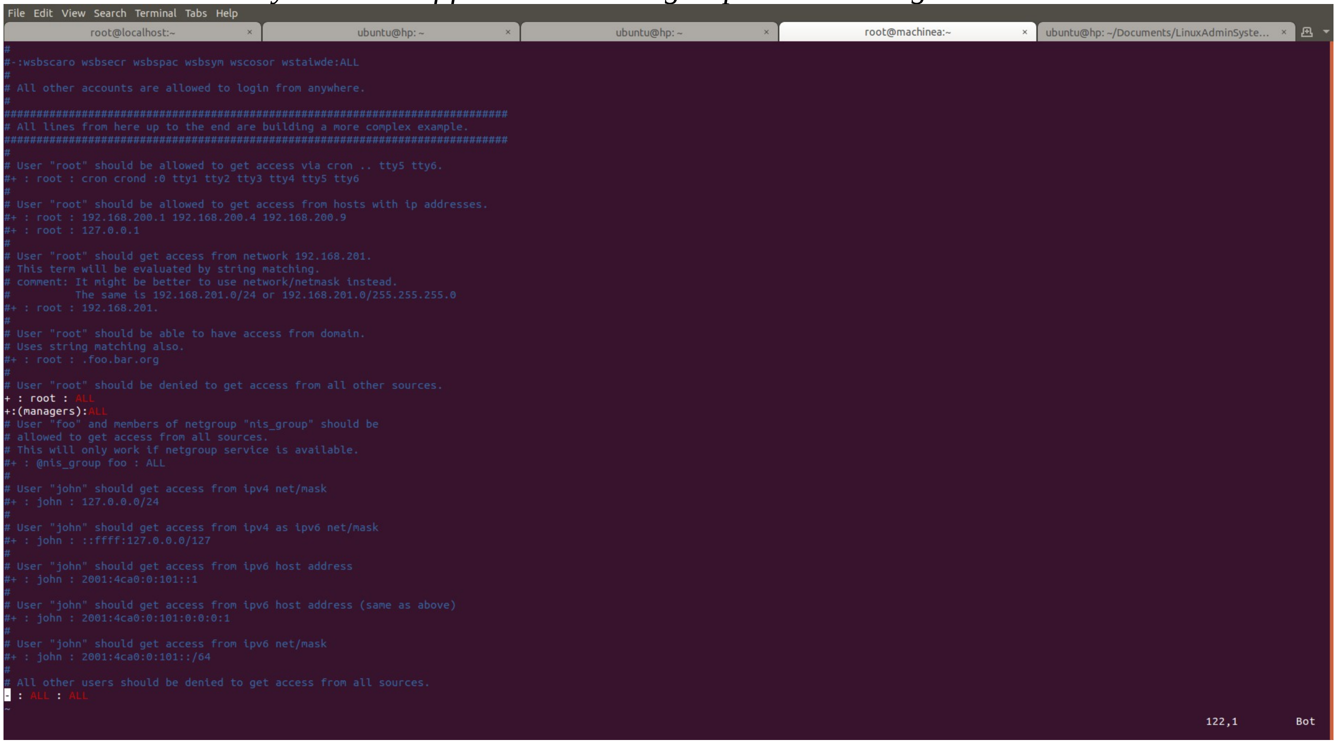
```
%wheel  ALL=(ALL)       ALL

## Same thing without a password
# %wheel        ALL=(ALL)       NOPASSWD: ALL

%http_admins ALL=/sbin/service httpd restart

## Allows members of the users group to mount and unmou
```

4. added the following line to /etc/profile (Source: https://stackoverflow.com/questions/12445527/set-different-umask-for-files-and-folders)

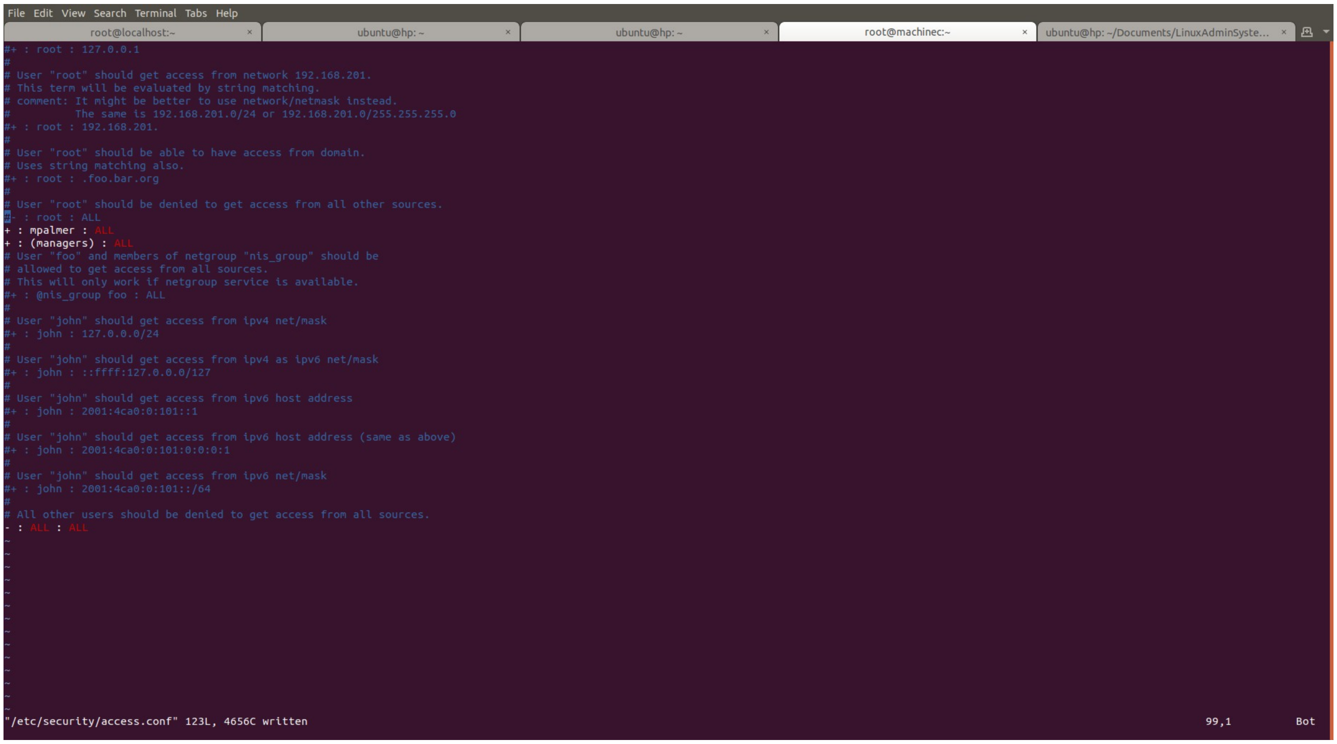
alias mkdir='mk:qdir -m 2770'

5.
uncomment “PermitRootLogin yes” in /etc/ssh/sshd_config
Added following to /etc/pam.d/login:
account   required   pam_access.so

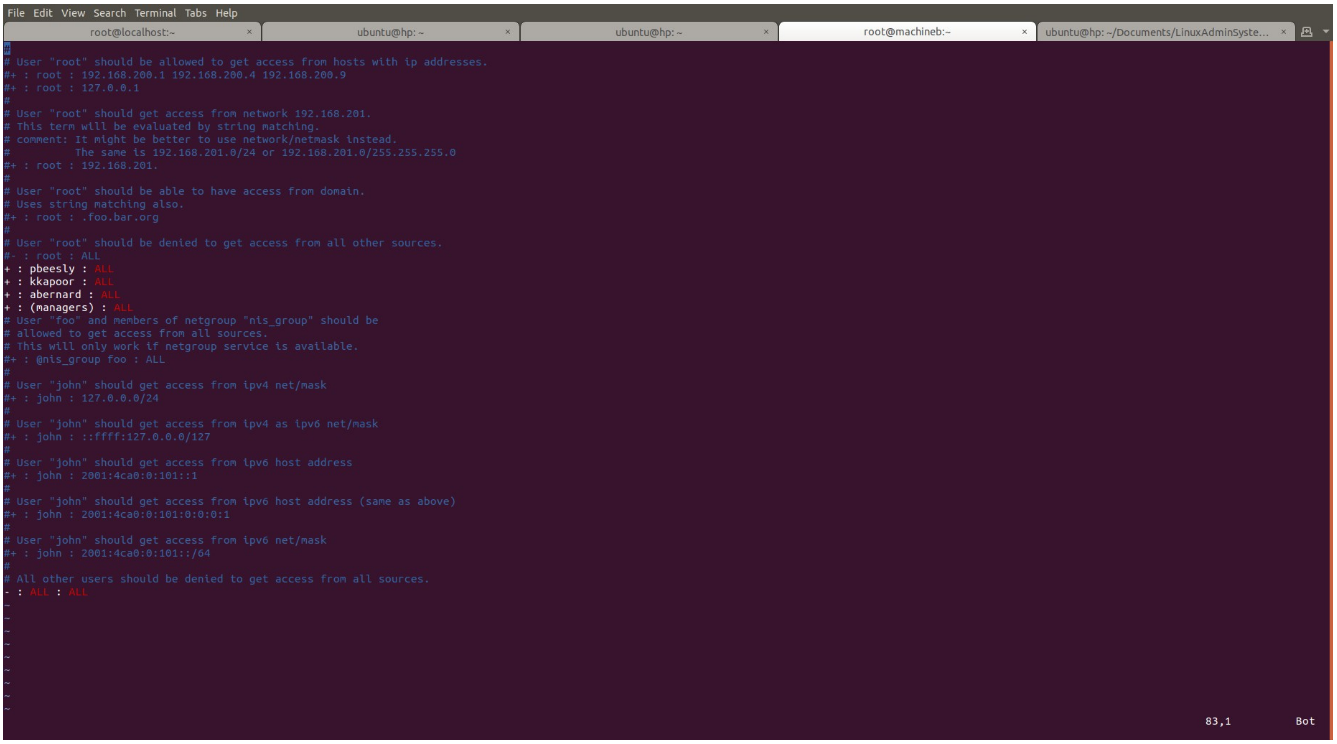
Modified /*etc/security/access.conf file to add users/groups that need login access*


File Edit View Search Terminal Tabs Help
root@localhost:~
ubuntu@hp: ~
ubuntu@hp: ~
root@machinea:~
ubuntu@hp: ~/Documents/LinuxAdminSyste...

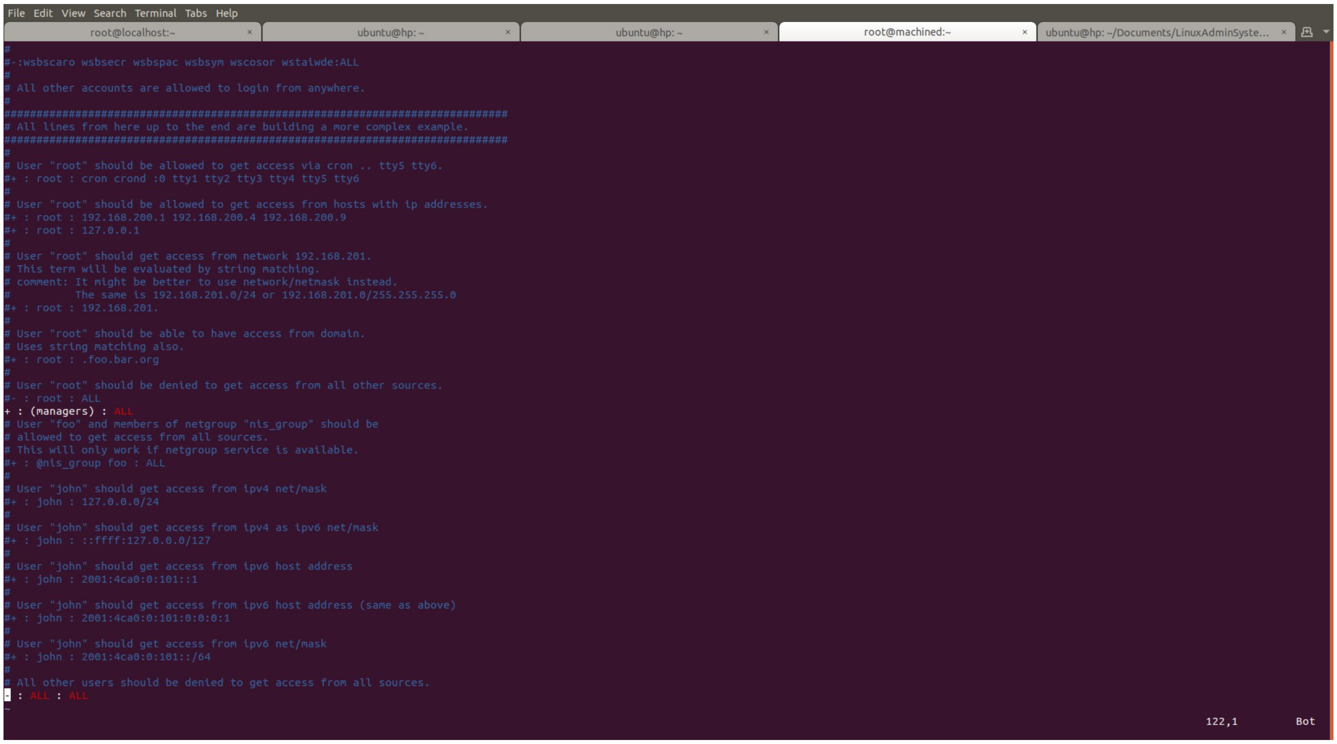
```
#
#-:wsbscaro wsbsecr wsbspac wsbsym wscosor wstaiwde:ALL
#
# All other accounts are allowed to login from anywhere.
#
###############################################################################
# All lines from here up to the end are building a more complex example.
###############################################################################
#
# User "root" should be allowed to get access via cron .. tty5 tty6.
#+ : root : cron crond :0 tty1 tty2 tty3 tty4 tty5 tty6
#
# User "root" should be allowed to get access from hosts with ip addresses.
#+ : root : 192.168.200.1 192.168.200.4 192.168.200.9
#+ : root : 127.0.0.1
#
# User "root" should get access from network 192.168.201.
# This term will be evaluated by string matching.
# comment: It might be better to use network/netmask instead.
#          The same is 192.168.201.0/24 or 192.168.201.0/255.255.255.0
#+ : root : 192.168.201.
#
# User "root" should be able to have access from domain.
# Uses string matching also.
#+ : root : .foo.bar.org
#
# User "root" should be denied to get access from all other sources.
+ : root : ALL
+:(managers):ALL
# User "foo" and members of netgroup "nis_group" should be
# allowed to get access from all sources.
# This will only work if netgroup service is available.
#+ : @nis_group foo : ALL
#
# User "john" should get access from ipv4 net/mask
#+ : john : 127.0.0.0/24
#
# User "john" should get access from ipv4 as ipv6 net/mask
#+ : john : ::ffff:127.0.0.0/127
#
# User "john" should get access from ipv6 host address
#+ : john : 2001:4ca0:0:101::1
#
# User "john" should get access from ipv6 host address (same as above)
#+ : john : 2001:4ca0:0:101:0:0:0:1
#
# User "john" should get access from ipv6 net/mask
#+ : john : 2001:4ca0:0:101::/64
#
# All other users should be denied to get access from all sources.
- : ALL : ALL
~
                                                                  122,1         Bot
```


File Edit View Search Terminal Tabs Help
root@localhost:~
ubuntu@hp: ~
ubuntu@hp: ~
root@machinec:~
ubuntu@hp: ~/Documents/LinuxAdminSyste...

```
#+ : root : 127.0.0.1
#
# User "root" should get access from network 192.168.201.
# This term will be evaluated by string matching.
# comment: It might be better to use network/netmask instead.
#          The same is 192.168.201.0/24 or 192.168.201.0/255.255.255.0
#+ : root : 192.168.201.
#
# User "root" should be able to have access from domain.
# Uses string matching also.
#+ : root : .foo.bar.org
#
# User "root" should be denied to get access from all other sources.
#- : root : ALL
+ : mpalmer : ALL
+ : (managers) : ALL
# User "foo" and members of netgroup "nis_group" should be
# allowed to get access from all sources.
# This will only work if netgroup service is available.
#+ : @nis_group foo : ALL
#
# User "john" should get access from ipv4 net/mask
#+ : john : 127.0.0.0/24
#
# User "john" should get access from ipv4 as ipv6 net/mask
#+ : john : ::ffff:127.0.0.0/127
#
# User "john" should get access from ipv6 host address
#+ : john : 2001:4ca0:0:101::1
#
# User "john" should get access from ipv6 host address (same as above)
#+ : john : 2001:4ca0:0:101:0:0:0:1
#
# User "john" should get access from ipv6 net/mask
#+ : john : 2001:4ca0:0:101::/64
#
# All other users should be denied to get access from all sources.
- : ALL : ALL
~
~
~
~
~
~
~
~
~
~
~
~
~
~
"/etc/security/access.conf" 123L, 4656C written                                                              99,1          Bot
```


File Edit View Search Terminal Tabs Help
root@localhost:~
ubuntu@hp: ~
ubuntu@hp: ~
root@machineb:~
ubuntu@hp: ~/Documents/LinuxAdminSyste...

```
#
# User "root" should be allowed to get access from hosts with ip addresses.
#+ : root : 192.168.200.1 192.168.200.4 192.168.200.9
#+ : root : 127.0.0.1
#
# User "root" should get access from network 192.168.201.
# This term will be evaluated by string matching.
# comment: It might be better to use network/netmask instead.
#          The same is 192.168.201.0/24 or 192.168.201.0/255.255.255.0
#+ : root : 192.168.201.
#
# User "root" should be able to have access from domain.
# Uses string matching also.
#+ : root : .foo.bar.org
#
# User "root" should be denied to get access from all other sources.
#- : root : ALL
+ : pbeesly : ALL
+ : kkapoor : ALL
+ : abernard : ALL
+ : (managers) : ALL
# User "foo" and members of netgroup "nis_group" should be
# allowed to get access from all sources.
# This will only work if netgroup service is available.
#+ : @nis_group foo : ALL
#
# User "john" should get access from ipv4 net/mask
#+ : john : 127.0.0.0/24
#
# User "john" should get access from ipv4 as ipv6 net/mask
#+ : john : ::ffff:127.0.0.0/127
#
# User "john" should get access from ipv6 host address
#+ : john : 2001:4ca0:0:101::1
#
# User "john" should get access from ipv6 host address (same as above)
#+ : john : 2001:4ca0:0:101:0:0:0:1
#
# User "john" should get access from ipv6 net/mask
#+ : john : 2001:4ca0:0:101::/64
#
# All other users should be denied to get access from all sources.
- : ALL : ALL
~
~
~
~
~
~
~
~
~
                                                                                                             83,1          Bot
```



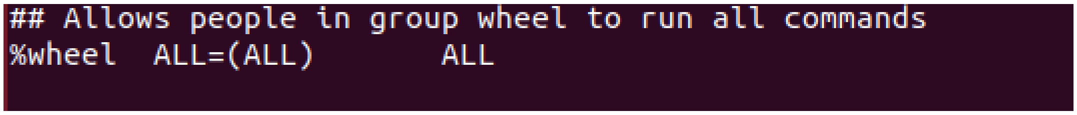
File Edit View Search Terminal Tabs Help
root@localhost:~
ubuntu@hp: ~
ubuntu@hp: ~
root@machined:~
ubuntu@hp: ~/Documents/LinuxAdminSyste...

```
#
#-:wsbscaro wsbsecr wsbspac wsbsym wscosor wstaiwde:ALL
#
# All other accounts are allowed to login from anywhere.
#
###############################################################################
# All lines from here up to the end are building a more complex example.
###############################################################################
#
# User "root" should be allowed to get access via cron .. tty5 tty6.
#+ : root : cron crond :0 tty1 tty2 tty3 tty4 tty5 tty6
#
# User "root" should be allowed to get access from hosts with ip addresses.
#+ : root : 192.168.200.1 192.168.200.4 192.168.200.9
#+ : root : 127.0.0.1
#
# User "root" should get access from network 192.168.201.
# This term will be evaluated by string matching.
# comment: It might be better to use network/netmask instead.
#          The same is 192.168.201.0/24 or 192.168.201.0/255.255.255.0
#+ : root : 192.168.201.
#
# User "root" should be able to have access from domain.
# Uses string matching also.
#+ : root : .foo.bar.org
#
# User "root" should be denied to get access from all other sources.
#- : root : ALL
+ : (managers) : ALL
# User "foo" and members of netgroup "nis_group" should be
# allowed to get access from all sources.
# This will only work if netgroup service is available.
#+ : @nis_group foo : ALL
#
# User "john" should get access from ipv4 net/mask
#+ : john : 127.0.0.0/24
#
# User "john" should get access from ipv4 as ipv6 net/mask
#+ : john : ::ffff:127.0.0.0/127
#
# User "john" should get access from ipv6 host address
#+ : john : 2001:4ca0:0:101::1
#
# User "john" should get access from ipv6 host address (same as above)
#+ : john : 2001:4ca0:0:101:0:0:0:1
#
# User "john" should get access from ipv6 net/mask
#+ : john : 2001:4ca0:0:101::/64
#
# All other users should be denied to get access from all sources.
- : ALL : ALL
~
                                                                  122,1         Bot
```

6. ran the following commands to grant admin privileges to Dwight Schrute and myself:

```
usermod -a -G wheel dschrute
usermod -a -G wheel ekarimi
```

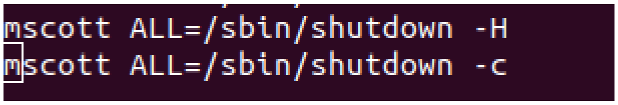
uncommented wheel entry in visudo



```
## Allows people in group wheel to run all commands
%wheel  ALL=(ALL)       ALL
```

7. Added these two lines visudo:

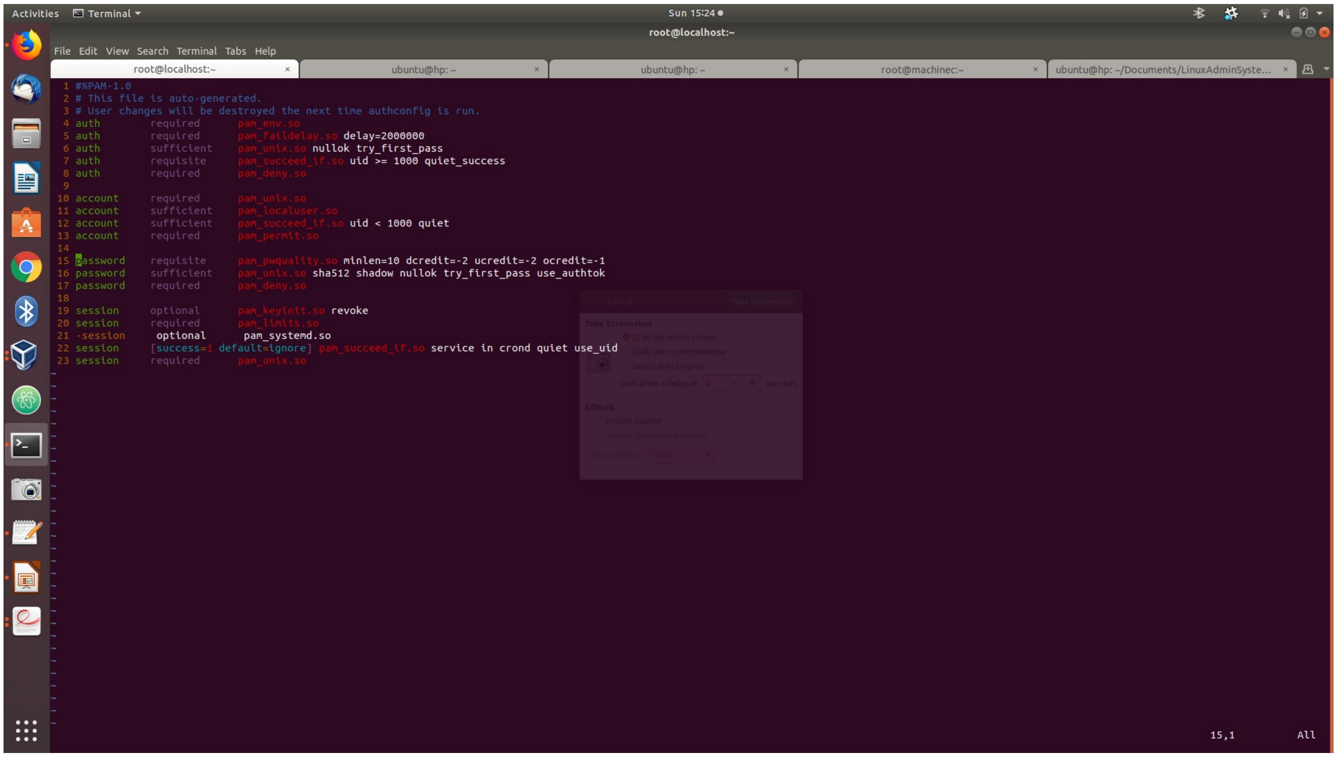
```
mscott ALL=/sbin/shutdown -H
mscott ALL=/sbin/shutdown -c
```



```
mscott ALL=/sbin/shutdown -H
mscott ALL=/sbin/shutdown -c
```

8.
Added following line to /etc/pam.d/system-auth

```
password    requisite     pam_pwquality.so minlen=10 dcredit=-2 ucredit=-2 ocredit=-1
```



```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_faildelay.so delay=2000000
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so minlen=10 dcredit=-2 ucredit=-2 ocredit=-1
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
                                                                              15,1          All
```

ran the following bash script to force password change on next login:

```
#!/bin/bash
getent passwd | while IFS=: read -r name password uid gid gecos home shell;
do
    passwd --expire $name
done
```

Source: https://unix.stackexchange.com/questions/199220/how-to-loop-over-users