Cloud Platform Development

Moaaz Sobhy Mahmoud Ismail Briek

WhatsApp | Email | LinkedIn | GitHub

1. How do you edit the current user's crontab?

```
root@DESKTOP-0E8M98L: ~
root@DESKTOP-0E8M98L:~# crontab -e
no crontab for root - using an empty one

Select an editor.  To change later, run 'select-editor'.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.basic
  3. /usr/bin/vim.tiny
  4. /bin/ed

Choose 1-4 [1]: 1
No modification made
root@DESKTOP-0E8M98L:~#
```

2. How do you list scheduled cron jobs for the current user?

```
root@DESKTOP-0E8M98L: ~
root@DESKTOP-0E8M98L:~# crontab -l
no crontab for root
root@DESKTOP-0E8M98L:~#
root@DESKTOP-0E8M98L:~#
```

3. How do you delete all cron jobs for the current user?

```
root@DESKTOP-0E8M98L: ~
root@DESKTOP-0E8M98L:~# crontab -r
no crontab for root
root@DESKTOP-0E8M98L:~#
root@DESKTOP-0E8M98L:~#
root@DESKTOP-0E8M98L:~#
```

4. Cron Syntax Questions

a. Schedule a job to run every day at 3:30 AM

30 3 * * * command

b. Run a script every Monday at 5:15 PM

15 17 * * 1 script

c. Execute a command every 10 minutes

*/10 * * * * command

d. Schedule a task to run every weekday (Mon-Fri) at 6:30 PM

30 18 * * 1-5 task

e. Run a job on the 1st and 15th of each month at 8:00 AM

0 8 1,15 job

5. How do you restrict users from using cron?

```
root@DESKTOP-0E8M98L:~# echo moaaz >> /etc/cron.deny
root@DESKTOP-0E8M98L:~# cat /etc/cron
cron.d/        cron.daily/   cron.deny      cron.hourly/  cron.monthly/ cron.weekly/   crontab
root@DESKTOP-0E8M98L:~# cat /etc/cron.d
cron.d/        cron.daily/ cron.deny
root@DESKTOP-0E8M98L:~# cat /etc/cron.deny
username
moaaz
root@DESKTOP-0E8M98L:~#
```

6. Set USerID

a. Create File and Set Execution and setuid permission

b. Check if setuid is enabled on File

```
root@DESKTOP-0E8M98L: ~
root@DESKTOP-0E8M98L:~# touch myfile
root@DESKTOP-0E8M98L:~# chmod u+xs myfile
root@DESKTOP-0E8M98L:~# ls -l myfile
-rwsr--r-- 1 root root 0 Apr  1 15:30 myfile
root@DESKTOP-0E8M98L:~#
```

7. SetGroupID

a. Create directory testdir and set setgid

b. Check if setgid is enabled on directory

c. Logout and login as root

d. Create testfile in testdir and verify ownership

```
moaaz@DESKTOP-0E8M98L:~$ ls
moaaz@DESKTOP-0E8M98L:~$ mkdir testdir
moaaz@DESKTOP-0E8M98L:~$ chmod g+s testdir
moaaz@DESKTOP-0E8M98L:~$ ls -ld testdir
drwxrwsr-x 2 moaaz moaaz 4096 Apr  1 15:32 testdir
moaaz@DESKTOP-0E8M98L:~$ su -
Password:
root@DESKTOP-0E8M98L:~# touch testdir/testfile
touch: cannot touch 'testdir/testfile': No such file or directory
root@DESKTOP-0E8M98L:~# ls
myfile   scheduler.sh
root@DESKTOP-0E8M98L:~# su - moaaz
moaaz@DESKTOP-0E8M98L:~$ ls
testdir
moaaz@DESKTOP-0E8M98L:~$ pwd
/home/moaaz
moaaz@DESKTOP-0E8M98L:~$ su -
Password:
root@DESKTOP-0E8M98L:~# cd /home/moaaz/
root@DESKTOP-0E8M98L:/home/moaaz# touch testdir/testfile
root@DESKTOP-0E8M98L:/home/moaaz# ls -l testdir/testfile
-rw-r--r-- 1 root moaaz 0 Apr  1 15:33 testdir/testfile
root@DESKTOP-0E8M98L:/home/moaaz#
```

8. Stick bit

a. Create public directory dir1 with sticky bit

b. Check if sticky bit is enabled on directory

c. Logout and login as user1

d. Create userfile1 in dir1

e. Login as user2 and attempt to remove userfile1

```
moaaz@DESKTOP-0E8M98L: ~
root@DESKTOP-0E8M98L:~# sudo groupadd sharedgroup
root@DESKTOP-0E8M98L:~# sudo usermod -aG sharedgroup amen
root@DESKTOP-0E8M98L:~# sudo usermod -aG sharedgroup moaaz
root@DESKTOP-0E8M98L:~# mkdir /opt/shared
root@DESKTOP-0E8M98L:~# sudo chgrp sharedgroup /opt/shared
root@DESKTOP-0E8M98L:~# chmod +t /opt/shared/
root@DESKTOP-0E8M98L:~# ls -ld /opt/shared/
drwxr-xr-t 2 root sharedgroup 4096 Apr  1 23:07 /opt/shared/
root@DESKTOP-0E8M98L:~# su - amen
amen@DESKTOP-0E8M98L:~$ touch /opt/shared/amenfile
touch: cannot touch '/opt/shared/amenfile': Permission denied
amen@DESKTOP-0E8M98L:~$ su -
Password:
root@DESKTOP-0E8M98L:~# chmod g+w /opt/shared
root@DESKTOP-0E8M98L:~# su - amen
amen@DESKTOP-0E8M98L:~$ touch /opt/shared/amenfile
amen@DESKTOP-0E8M98L:~$ ls -l /opt/shared/amenfile
-rw-rw-r-- 1 amen amen 0 Apr  1 23:14 /opt/shared/amenfile
amen@DESKTOP-0E8M98L:~$ ls -ld /opt/shared
drwxrwxr-t 2 root sharedgroup 4096 Apr  1 23:14 /opt/shared
amen@DESKTOP-0E8M98L:~$ su - moaaz
Password:
moaaz@DESKTOP-0E8M98L:~$ rm /opt/shared/amenfile
rm: remove write-protected regular empty file '/opt/shared/amenfile'? y
rm: cannot remove '/opt/shared/amenfile': Operation not permitted
moaaz@DESKTOP-0E8M98L:~$
```

9. Give user john read and write permissions on myfile.txt

10. How to view the ACL of a file named myfile.txt?

```
root@DESKTOP-0E8M98L: ~
root@DESKTOP-0E8M98L:~# ls
myfile
root@DESKTOP-0E8M98L:~# setfacl -m u:amen:rw myfile
root@DESKTOP-0E8M98L:~# ls -l
total 0
-rw-rw-r--+ 1 root root 0 Apr  1 23:20 myfile
root@DESKTOP-0E8M98L:~# getfacl myfile
# file: myfile
# owner: root
# group: root
user::rw-
user:amen:rw-
group::r--
mask::rw-
other::r--

root@DESKTOP-0E8M98L:~#
```

11.How do you give the group developers execute permissions on the directory

/home/user/documents


```
root@DESKTOP-0E8M98L: ~                                                          —  □  ✕

root@DESKTOP-0E8M98L:~# groupadd developers
root@DESKTOP-0E8M98L:~# mkdir devdir
root@DESKTOP-0E8M98L:~# setfacl -m g:developers:--x devdir/
root@DESKTOP-0E8M98L:~# get
getcap        getconf     getent      getfacl      getkeycodes  getopt      getopts      getpcaps      ge
root@DESKTOP-0E8M98L:~# getfacl devdir/
# file: devdir/
# owner: root
# group: root
user::rwx
group::r-x
group:developers:--x
mask::r-x
other::r-x

root@DESKTOP-0E8M98L:~#
```

12.How to remove the ACL entry for the user john on the file file1.txt?

```
root@DESKTOP-0E8M98L:~# setfacl -x u:amen myfile
root@DESKTOP-0E8M98L:~# getfacl myfile
# file: myfile
# owner: root
# group: root
user::rw-
group::r--
mask::r--
other::r--

root@DESKTOP-0E8M98L:~#
```

13.How do you set a default ACL for a directory so that all new files and directories
created inside it inherit the same permissions?

```
root@DESKTOP-0E8M98L: ~
root@DESKTOP-0E8M98L:~# setfacl -d -m u::rwx,g::r-x,o::r-- devdir/
root@DESKTOP-0E8M98L:~# getfacl devdir/
# file: devdir/
# owner: root
# group: root
user::rwx
group::r-x
group:developers:--x
mask::r-x
other::r-x
default:user::rwx
default:group::r-x
default:other::r--

root@DESKTOP-0E8M98L:~#
```

14.Allow group developers to read all files in ~/Music recursively

```
root@DESKTOP-0E8M98L:~# setfacl -R -m g:developers:r-- ~/Music
setfacl: /root/Music: No such file or directory
root@DESKTOP-0E8M98L:~# mkdir ~/Music
root@DESKTOP-0E8M98L:~# setfacl -R -m g:developers:r-- ~/Music
root@DESKTOP-0E8M98L:~# getfacl ~/Music/
getfacl: Removing leading '/' from absolute path names
# file: root/Music/
# owner: root
# group: root
user::rwx
group::r-x
group:developers:r--
mask::r-x
other::r-x

root@DESKTOP-0E8M98L:~#
```

15.How to remove all ACLs from the file file1.txt and revert to the standard Unix permissions?

```
root@DESKTOP-0E8M98L:~# setfacl -b myfile
root@DESKTOP-0E8M98L:~# getfacl myfile
# file: myfile
# owner: root
# group: root
user::rw-
group::r--
other::r--

root@DESKTOP-0E8M98L:~#
```

16.Set a mask on myfile.txt to limit all non-owners to r--.

```
root@DESKTOP-0E8M98L:~# setfacl -m mask:r-- myfile
root@DESKTOP-0E8M98L:~# getfacl myfile
# file: myfile
# owner: root
# group: root
user::rw-
group::r--
mask::r--
other::r--

root@DESKTOP-0E8M98L:~#
```

17.How would you allow user 'alice' to run only the 'yum' command as root?

```
root@DESKTOP-0E8M98L: ~                                                    —  ☐  ✕
root@DESKTOP-0E8M98L:~# echo "alice ALL=(root) /usr/bin/yum" >> /etc/sudoers
root@DESKTOP-0E8M98L:~# cat echo "alice ALL=(root) /usr/bin/yum" >> /etc/sudoers
cat: echo: No such file or directory
cat: 'alice ALL=(root) /usr/bin/yum': No such file or directory
root@DESKTOP-0E8M98L:~# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
alice ALL=(root) /usr/bin/yum
```

18.How would you allow a group 'developers' to run any command as root without a password?

```
root@DESKTOP-0E8M98L: ~                                                    —  □  ✕
root@DESKTOP-0E8M98L:~# echo "%developers ALL=(ALL) NOPASSWD: ALL" >> /etc/sudoers
root@DESKTOP-0E8M98L:~# cat /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
alice ALL=(root) /usr/bin/yum
%developers ALL=(ALL) NOPASSWD: ALL
root@DESKTOP-0E8M98L:~#
```