

Arsenia suero

12/02/2021

Security Part 2

Debian.

1. **Take a snapshot of users every other hour (Use a cron job for this) to see if there is any suspicious adding/removing of users**

The first thing we must do is create the **script** to generate the snapshot
This is basically the command for the script.

```
#!/bin/bash
```

#From where the snapshots will be made

```
FROM=arseniasc@debian
```

```
SOURCE=/home/arseniasc
```

#Where the snapshots will be saved

```
DEST=/snap
```

```
LFPATH=/tmp
```

```
LF=$LFPATH/$(date +%Y%m%d_%T)_logfile.log
```

#Create a synchronization with all my sources

```
rsync --delete --log-file=$LF -avzq $SOURCE $DEST
```

-Now, install Snapd.

We will need snapd package this is a **requirement** to set up our cron job.

To install snapd type, **sudo apt install snapd** and **hit enter**. Wait until the download finish to install the package.

-Creating the cron job

After creating the script for generating the snapshots, please follow the next step to set up the snapshot to be run hourly.

-Start the daemon cron please run this command **sudo service cron start** and hit enter.

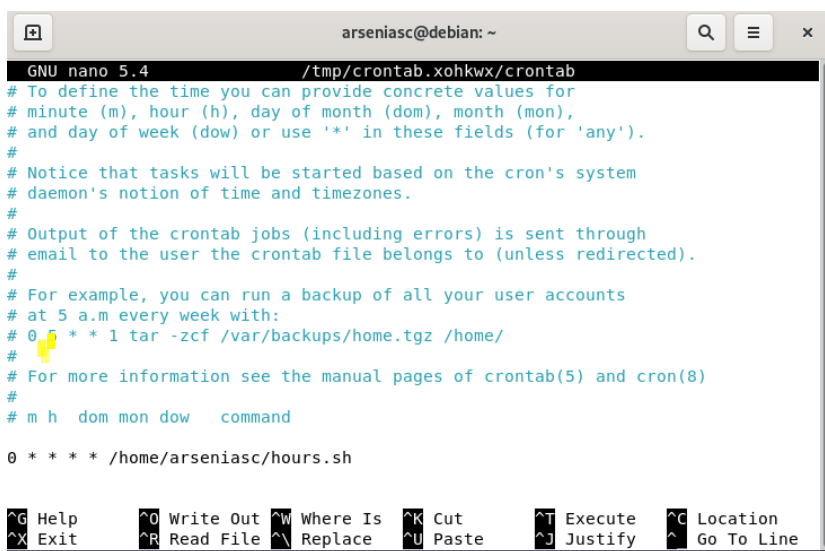
-Then type this command **crontab -e**

-Later you will be prompted to select a text editor, selected **nano** or any text editor you have available then press **enter**.

-On the text editor, look for this specific line below

#m h dom mon dow command

-To enter in the insert mode, hit the letter **I** on your keyboard, type the following below the line we saw above **0 * * * * /home/arseniasc/hour**. by adding this line will set up the cron job using the script hours.sh located on /home/arseniasc

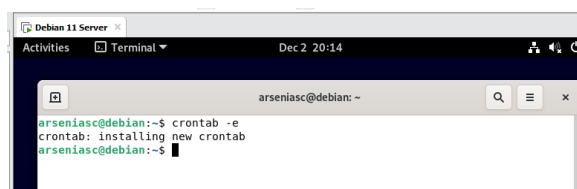


```
arseniasc@debian: ~
GNU nano 5.4 /tmp/crontab.xohkwx/crontab
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow  command
0 * * * * /home/arseniasc/hours.sh

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify  ^_ Go To Line
```

-Then save and exit editor, hit the **scope key** to exit the insert mode and type **:wq**

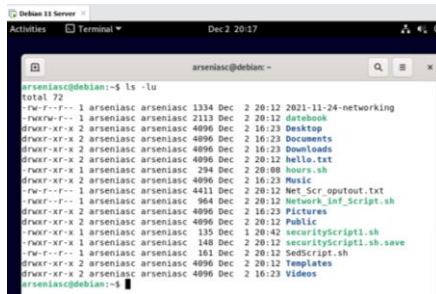
-Later, you will see a message on the command line saying **crontab: installing new crontab**. This confirms your crontab was created successfully.



```
Debian 11 Server
Activities Terminal Dec 2 20:14
arseniasc@debian: ~
arseniasc@debian:~$ crontab -e
crontab: installing new crontab
arseniasc@debian:~$
```

-Please type the following command to list your current cron job **crontab -l**

Finally, Type **ls -lu** to see the timestamps associated with the creation of each snapshot



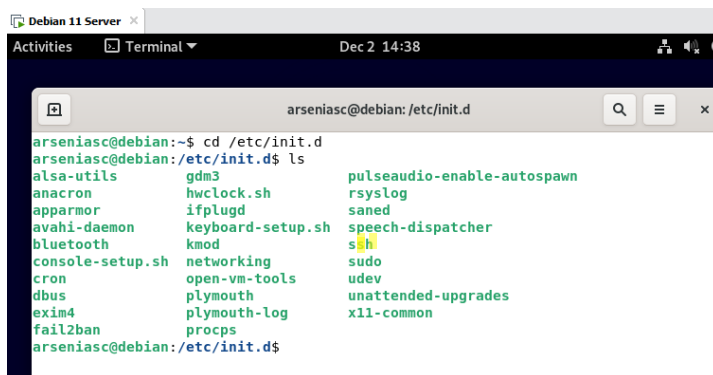
```
arseniasc@debian:~$ ls -lu
total 72
-rw-r--r-- 1 arseniasc arseniasc 1334 Dec 2 20:12 2021-11-24-networking
-rw-r--r-- 1 arseniasc arseniasc 2113 Dec 2 20:12 datebook
drwxr-xr-x 2 arseniasc arseniasc 4096 Dec 2 16:23 Desktop
drwxr-xr-x 2 arseniasc arseniasc 4096 Dec 2 16:23 Documents
drwxr-xr-x 2 arseniasc arseniasc 4096 Dec 2 16:23 Downloads
drwxr-xr-x 2 arseniasc arseniasc 4096 Dec 2 20:12 hello.txt
-rw-r--r-- 1 arseniasc arseniasc 294 Dec 2 20:08 hours.sh
drwxr-xr-x 2 arseniasc arseniasc 4096 Dec 2 16:23 Music
-rw-r--r-- 1 arseniasc arseniasc 4411 Dec 2 20:12 Net_Scr_output.txt
-rw-r--r-- 1 arseniasc arseniasc 964 Dec 2 20:12 Network_inf_script.sh
drwxr-xr-x 2 arseniasc arseniasc 4096 Dec 2 16:23 Pictures
drwxr-xr-x 2 arseniasc arseniasc 4096 Dec 2 20:12 Public
-rw-r--r-- 1 arseniasc arseniasc 135 Dec 1 20:42 securityScript1.sh
-rw-r--r-- 1 arseniasc arseniasc 148 Dec 2 20:12 securityScript1.sh.save
-rw-r--r-- 1 arseniasc arseniasc 161 Dec 2 20:12 SetScript.sh
drwxr-xr-x 2 arseniasc arseniasc 4096 Dec 2 20:12 Templates
drwxr-xr-x 2 arseniasc arseniasc 4096 Dec 2 16:23 Videos
arseniasc@debian:~$
```

2. Write a document that will show how to control what daemons run on boot and how to change that. assume your audience is technically inclined, but not an expert.

How to control what daemons run on boot?

-The first thing we must know is that we can use the man pages to see information about daemons. Also, we know that daemons are programs that are executed as a background process. To control this process that is running in the background we must:

-Navigate to the **/etc/init.d** directory on your terminal for the list of available daemons on your Linux system. Type **cd /etc/init.d** to go to this directory. Later type **ls** to see the available daemons.



```
arseniasc@debian:~$ cd /etc/init.d
arseniasc@debian:/etc/init.d$ ls
alsa-utils      gdm3             pulseaudio-enable-autospawn
anacron         hwclock.sh       rsyslog
apparmor        ifplugd          saned
avahi-daemon    keyboard-setup.sh speech-dispatcher
bluetooth       knod             ssh
console-setup.sh networking        sudo
cron            open-vm-tools    udev
dbus            plymouth         unattended-upgrades
exim4           plymouth-log     x11-common
fail2ban        procps
```

-To **start** a daemon in this case I selected **ssh** as an example, you can type the following command **sudo service ssh start**

-If you want to **stop** the ssh daemon type the following **sudo service ssh stop**

-and also, if you want to **restart** the daemon you can type the following command **sudo service ssh restart**

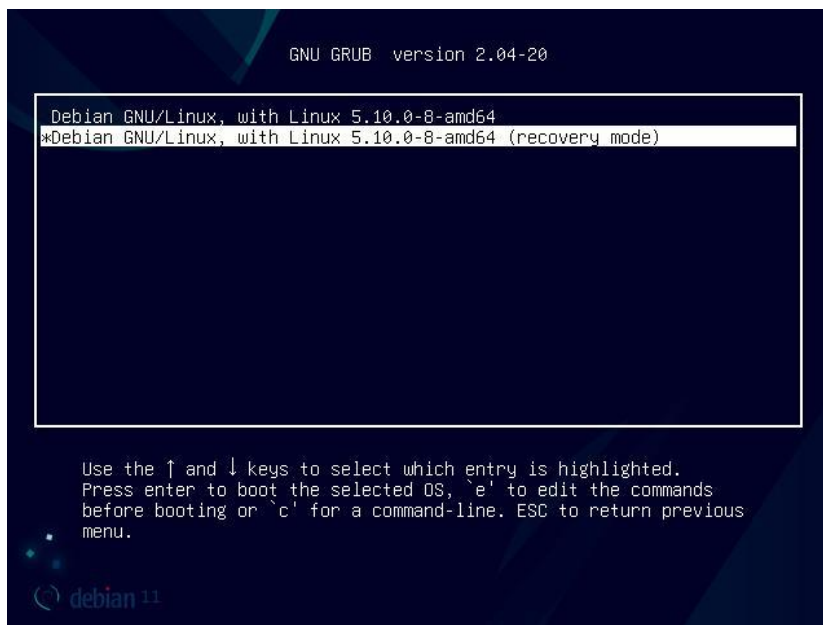
3. Find out how to boot into emergency mode for both your servers. Write a one-page (or less) document on how to do that. Include 1 paragraph executive summary on why you might want to.

You need the root password to get into recovery/emergency mode in most Linux, including Debian, Fedora, CentOS, etc.

The emergency mode in Linux provides the most minimal environment possible and allows you to repair your system even if the system is unable to enter rescue mode

-Debian recovery mode is present in the boot menu. **Start or restart** your computer and press Esc.

-Then choose **Advanced options** from the menu and boot the kernel entry with recovery mode.



Later it will boot into the text console and ask you to type root user password to get a pass. if the root is not enabled it will say **root account is locked**. Type the password and hit Enter, then it will take you right to the emergency mode.

There are different situations why you might enter the emergency mode for example when a filesystem is corrupted on your system or there are broke drivers or forgot user password, then

you may find yourself stuck and you will have to run **the emergency mode** to solve these kind of issue.

CentOS.

Take a snapshot of users every other hour (Use a cron job for this) to see if there is any suspicious adding/removing of users

The first thing you must do is create the **script** to generate the snapshot
This is basically the command for the script.

Script

```
#!/bin/bash
```

#from where the snapshots will be made

```
FROM=asuero@localhost
```

```
SOURCE=/home/asuero
```

#Where the snapshots will be saved

```
DEST=/snap
```

```
LFPATH=/tmp
```

```
LF=$LFPATH/$(date +%Y%m%d_%T)_logfile.log
```

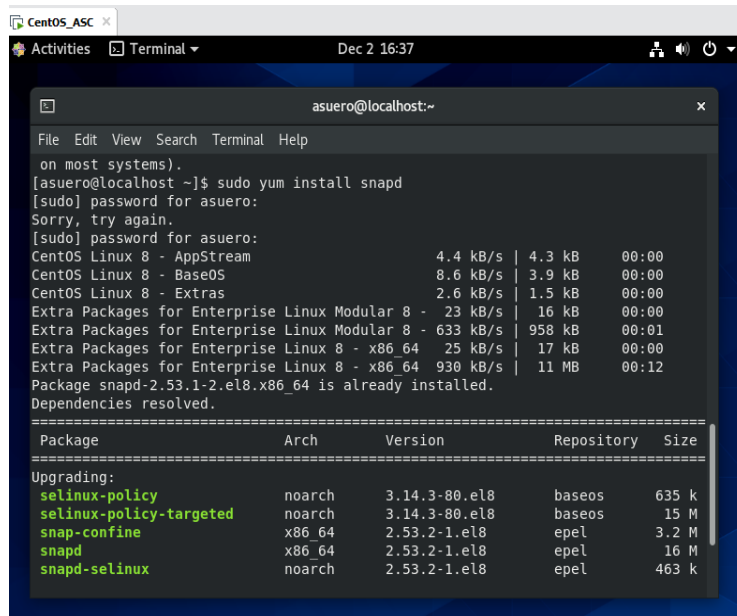
#Create a sincronization with all my sources

```
rsync --delete --log-file=$LF -avzq $SOURCE $DEST
```

-Now, install Snapd.

We will need snapd package this is a requirement to set up our cron job.

To install snapd type, **sudo apt install snapd** and **hit enter**. Wait until the download finish to install the package.



```
CentOS_ASC
Activities Terminal Dec 2 16:37
asuero@localhost:~
File Edit View Search Terminal Help
on most systems).
[asuero@localhost ~]$ sudo yum install snapd
[sudo] password for asuero:
Sorry, try again.
[sudo] password for asuero:
CentOS Linux 8 - AppStream          4.4 kB/s | 4.3 kB    00:00
CentOS Linux 8 - BaseOS            8.6 kB/s | 3.9 kB    00:00
CentOS Linux 8 - Extras            2.6 kB/s | 1.5 kB    00:00
Extra Packages for Enterprise Linux Modular 8 - 23 kB/s | 16 kB    00:00
Extra Packages for Enterprise Linux Modular 8 - 633 kB/s | 958 kB    00:01
Extra Packages for Enterprise Linux 8 - x86_64 25 kB/s | 17 kB    00:00
Extra Packages for Enterprise Linux 8 - x86_64 930 kB/s | 11 MB    00:12
Package snapd-2.53.1-2.el8.x86_64 is already installed.
Dependencies resolved.
=====
Package Arch Version Repository Size
=====
Upgrading:
selinux-policy noarch 3.14.3-80.el8 baseos 635 k
selinux-policy-targeted noarch 3.14.3-80.el8 baseos 15 M
snap-confine x86_64 2.53.2-1.el8 epel 3.2 M
snapd x86_64 2.53.2-1.el8 epel 16 M
snapd-selinux noarch 2.53.2-1.el8 epel 463 k
```

-To start the daemon cron please run this command **sudo systemctl start crond.service**

-To execute this action when the server starts type the following command: **sudo systemctl enable crond.service**

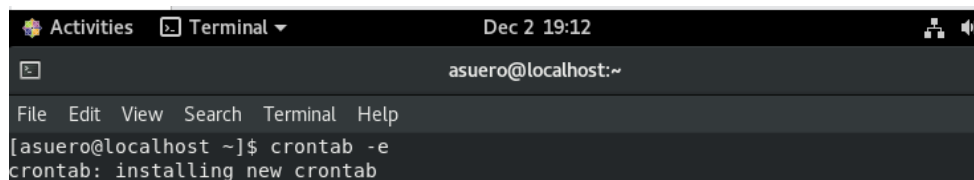
Creating the cron job

-After creating the script for generating the snapshots, please follow the next step to set up the snapshot to be made hourly

-First type **crontab -e**

-Later you will be sent to **vi** editor in there type the following **0 * * * * /home/asuero/hours.sh** later exist and save vi editor.

-Later, you will see a message on the command line saying **crontab: installing new crontab.** This confirm your crontab was created successfully.



```
Activities Terminal Dec 2 19:12
asuero@localhost:~
File Edit View Search Terminal Help
[asuero@localhost ~]$ crontab -e
crontab: installing new crontab
```

To see your cron job type the following **crontab -l**

```
CentOS_ASC
Activities Terminal Dec 2 19:14
asuero@localhost:~
File Edit View Search Terminal Help
[asuero@localhost ~]$ crontab -l
0 * * * * /home/asuero/hours.sh
[asuero@localhost ~]$
```

Showing my working cron job

-Type **ls -lu** to see the timestamps associated with the creation of each snapshot

```
CentOS_ASC
Activities Terminal Dec 2 19:39
asuero@localhost:~
File Edit View Search Terminal Help
[asuero@localhost ~]$ snap saved
Set Snap Age Version Rev Size Notes
core18 2h18m 20211028 2253 1248 -
lolcat 2h18m 100.0.1 1 1248 -
snapd 2h18m 2.53.2 14066 1248 -
[asuero@localhost ~]$ snap changes
ID Status Spawn Ready Summary
4 Done today at 17:00 EST today at 17:02 EST Auto-refresh snap "snapd"
5 Done today at 17:00 EST today at 17:00 EST Refresh all snaps: no updates
6 Done today at 17:17 EST today at 17:17 EST Snapshot all snaps
[asuero@localhost ~]$ ls -lu
total 36
-rw-rw-r--. 1 asuero asuero 2113 Dec 2 18:53 datebook
drwxr-xr-x. 2 asuero asuero 6 Dec 2 16:31 Desktop
drwxr-xr-x. 2 asuero asuero 62 Dec 2 16:31 Documents
drwxr-xr-x. 2 asuero asuero 6 Dec 2 16:31 Downloads
-rwxrwxr-x. 1 asuero asuero 354 Dec 2 19:21 hours.sh
drwxr-xr-x. 2 asuero asuero 6 Dec 2 16:31 Music
-rw-rw-r--. 1 asuero asuero 0 Nov 30 01:21 Net_Scr_oputout.txt
drwxr-xr-x. 2 asuero asuero 194 Dec 2 19:21 Pictures
drwxr-xr-x. 2 asuero asuero 6 Dec 2 18:53 Public
-rw-rw-r--. 1 asuero asuero 26132 Dec 2 18:53 remi-release-8.rpm
drwxr-xr-x. 2 asuero asuero 6 Dec 2 18:53 Templates
drwxr-xr-x. 2 asuero asuero 6 Dec 2 16:31 Videos
[asuero@localhost ~]$
```

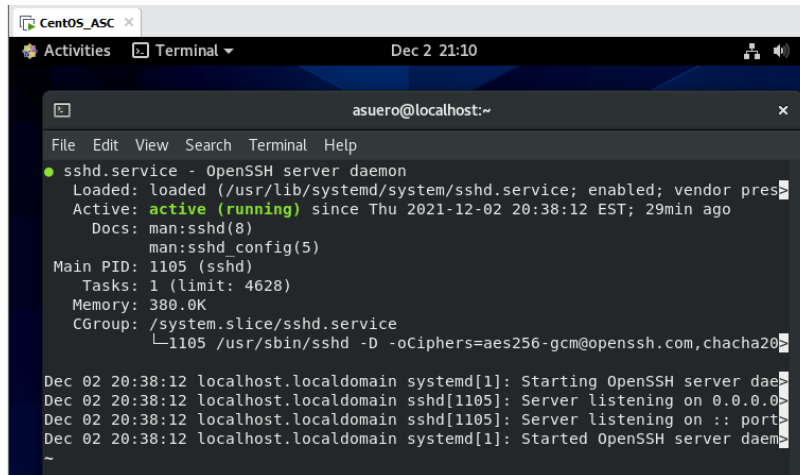
Write a document that will show how to control what daemons run on boot and how to change that. assume your audience is technically inclined, but not an expert.

The first thing we must know is that we can use the man pages to see information about daemons. Also, we know that daemons are programs that are execute as a background process. To control this process that is running in the background we must:

-Navigate to the **/etc/init.d** directory on your terminal for the list of available daemons on your Linux system. to go to this directory type **sudo cd /etc/init.d** and then once on this directory do a **ls** to see a list of the available daemons.

```
CentOS_ASC
Activities Terminal Dec 2 20:55
asuero@localhost:/etc/init.d
File Edit View Search Terminal Help
[asuero@localhost init.d]$ ls
functions README
[asuero@localhost init.d]$
```

To see the status of a specific daemon you can type the following command **service name of de service status** example **service sshd status**

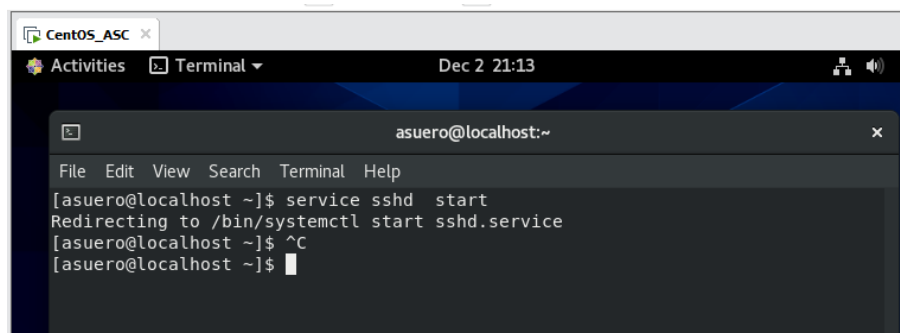


```
CentOS_ASC x
Activities Terminal Dec 2 21:10

asuero@localhost:~
File Edit View Search Terminal Help
● sshd.service - OpenSSH server daemon
   Loaded: loaded (/usr/lib/systemd/system/sshd.service; enabled; vendor pres
   Active: active (running) since Thu 2021-12-02 20:38:12 EST; 29min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Main PID: 1105 (sshd)
     Tasks: 1 (limit: 4628)
    Memory: 380.0K
   CGroup: /system.slice/sshd.service
           └─1105 /usr/sbin/sshd -D -oCiphers=aes256-gcm@openssh.com,chacha20

Dec 02 20:38:12 localhost.localdomain systemd[1]: Starting OpenSSH server dae
Dec 02 20:38:12 localhost.localdomain sshd[1105]: Server listening on 0.0.0.0
Dec 02 20:38:12 localhost.localdomain sshd[1105]: Server listening on :: port
Dec 02 20:38:12 localhost.localdomain systemd[1]: Started OpenSSH server daem
```

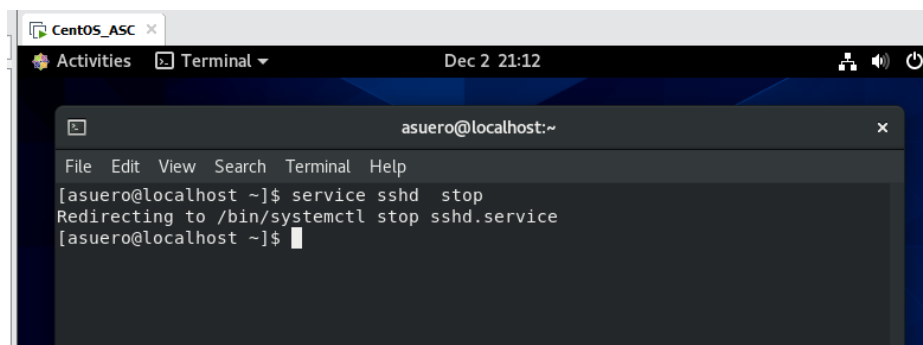
-If you want to **start** the ssh daemon type the following **service sshd start**



```
CentOS_ASC x
Activities Terminal Dec 2 21:13

asuero@localhost:~
File Edit View Search Terminal Help
[asuero@localhost ~]$ service sshd start
Redirecting to /bin/systemctl start sshd.service
[asuero@localhost ~]$ ^C
[asuero@localhost ~]$
```

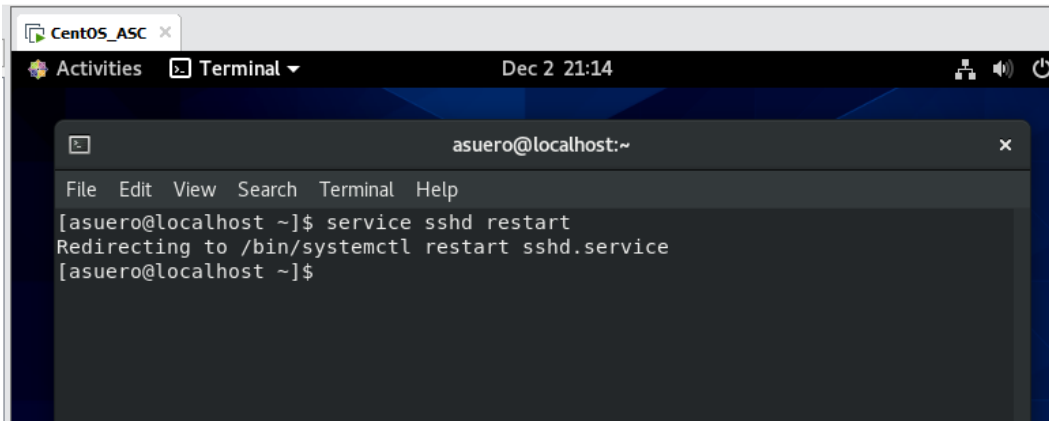
-If you want to **stop** the ssh daemon type the following **service sshd stop**



```
CentOS_ASC x
Activities Terminal Dec 2 21:12

asuero@localhost:~
File Edit View Search Terminal Help
[asuero@localhost ~]$ service sshd stop
Redirecting to /bin/systemctl stop sshd.service
[asuero@localhost ~]$
```


Also, if you want to **restart** the daemon you can type the following command **service sshd restart**



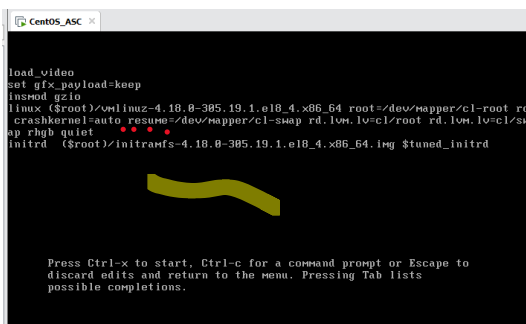
```
CentOS_ASC x
Activities Terminal Dec 2 21:14
asuerdo@localhost:~
File Edit View Search Terminal Help
[asuerdo@localhost ~]$ service sshd restart
Redirecting to /bin/systemctl restart sshd.service
[asuerdo@localhost ~]$
```

Find out how to boot into emergency mode for both your servers. Write a one-page (or less) document on how to do that. Include 1 paragraph executive summary on why you might want to.

For Fedora, CentOS and Arch Linux, there's no recovery mode in the boot-menu. Instead, user need to edit the menu entry to boot with given parameters.

Start or re-start your computer and press Esc on keyboard to get into Grub boot-menu. When you're there, press **e** on the keyboard to edit the default entry.

After you are being typed **e**, go down to the last line of the file between the last line and previous to the last line input a blank space and then the following command '**systemd.unit=emergency.target**'.



```
CentOS_ASC x
load_video
set gfx_payload=keep
insmod gzio
linux ($root)/vmlinuz-4.18.0-385.19.1.el8_4.x86_64 root=/dev/mapper/cl-root ro
crashkernel=auto resume=/dev/mapper/cl-swap rd.lvm.lv=cl/root rd.lvm.lv=cl/sw
ap rhgb quiet
initrd ($root)/initramfs-4.18.0-385.19.1.el8_4.x86_64.img $tuned_initrd

Press Ctrl-x to start, Ctrl-c for a command prompt or Escape to
discard edits and return to the menu. Pressing Tab lists
possible completions.
```

After adding the new boot parameter, press **Ctrl+X** to boot with the entry instructions you typed. It will bring you into the rescue mode and ask for typing root password. Once you have typed the password, you will be all set, you will be right on the recovery mode!

Sources:

<https://linuxize.com/post/scheduling-cron-jobs-with-crontab/>

<https://fostips.com/boot-rescue-emergency-mode-ubuntu-fedora/>

<https://www.hostinger.com/tutorials/how-to-use-rsync>