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 syncronization 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 stapd 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**.**

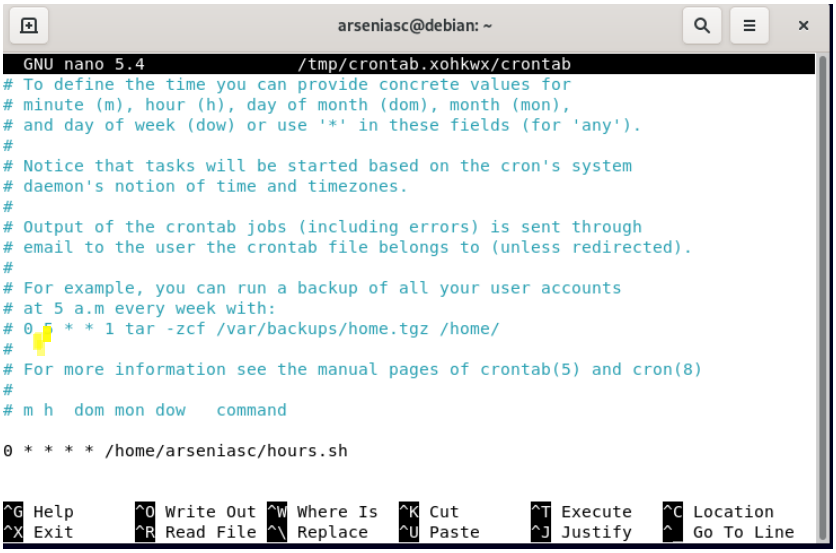
-Then type this command **crontab -e**

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

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

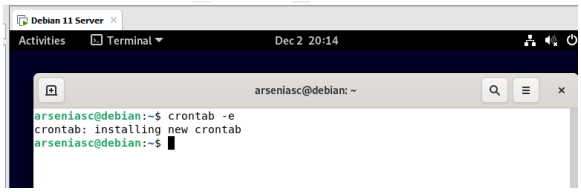
#m h dom mon down command

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



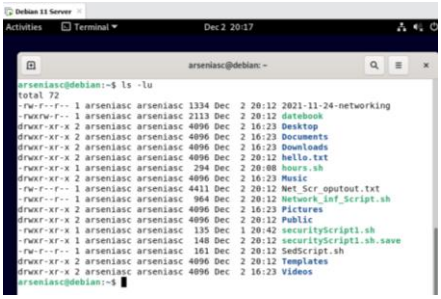
-Then save and exit editor, hit the **scape key** to exit the insert mode and type **:wq**

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



-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

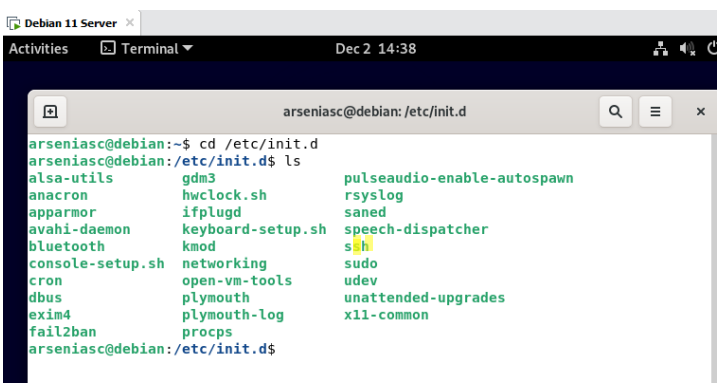


2. **Write a document that will show how to control what daemons run on boot and how to change that. assume your audience is technically inclined, but not an expert.**

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.



-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**

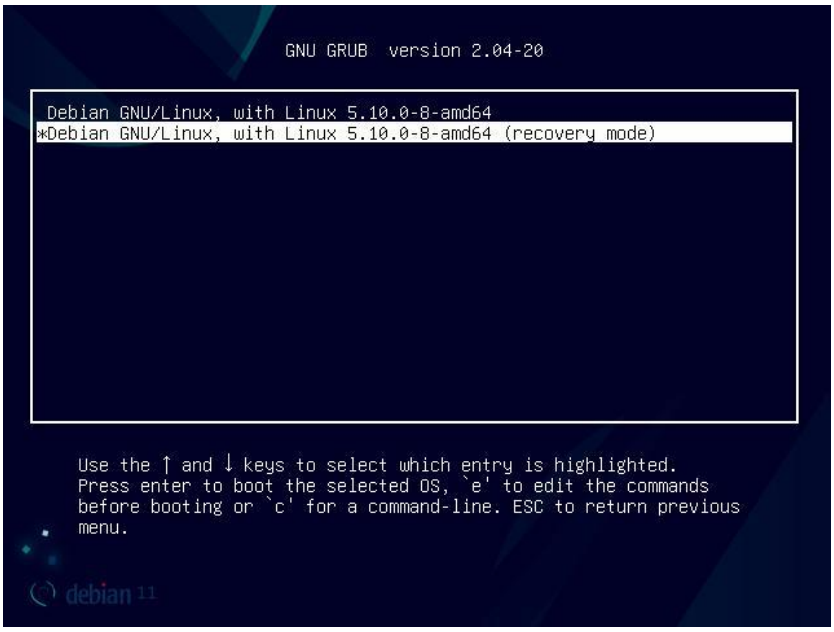
3. **Find out how to boot into emergency mode for both your servers. Write a one-page (or less) document on how to do that. Include 1 paragraph executive summary on why you might want to.**

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

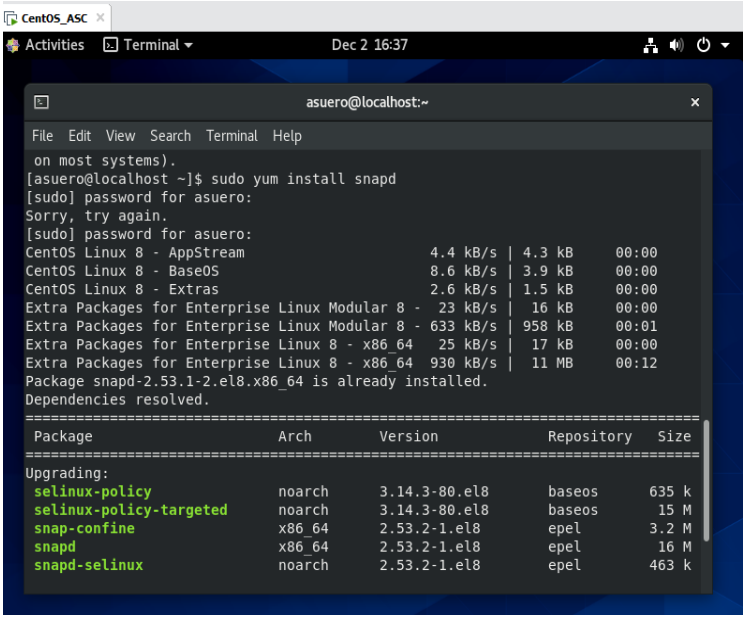
The first thing you must do is create the **script** to generate the snapshot
This is basically the command for the script.

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



-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**

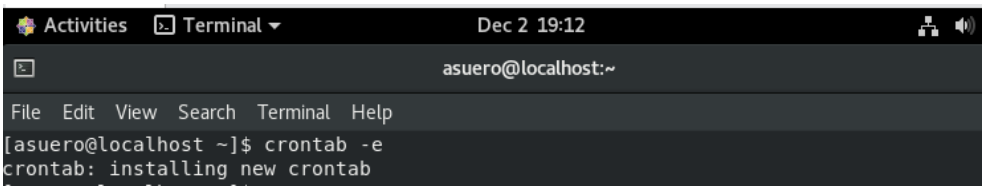
Creating the cron job

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

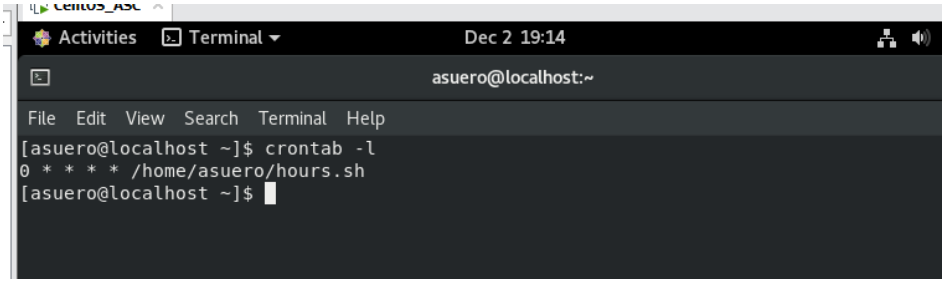
-First type **crontab -e**

-Later you will be sent to **vi** editor in there type the fallowing **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.

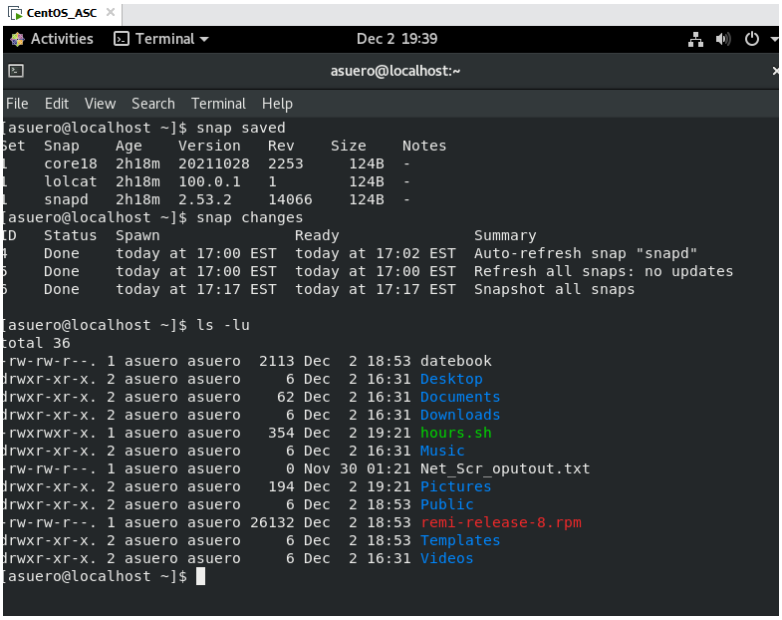


To see your cron job type the following **crontab -l**



Showing my working cron job

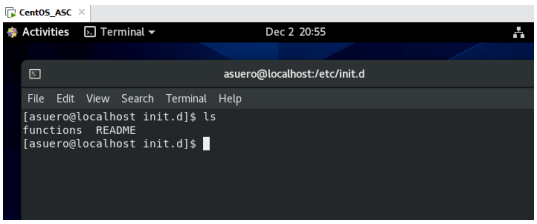
-Type **ls -lu to** see the timestamps associated with the creation of each snapshot



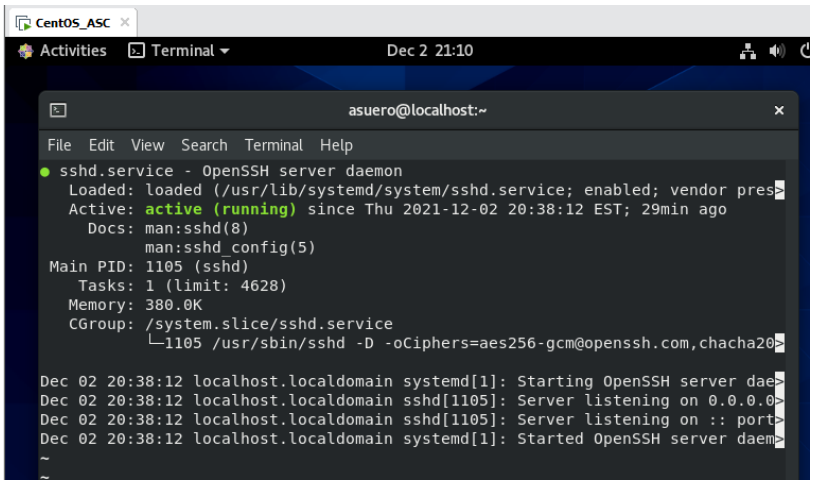
Write a document that will show how to control what daemons run on boot and how to change that. assume your audience is technically inclined, but not an expert.

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:

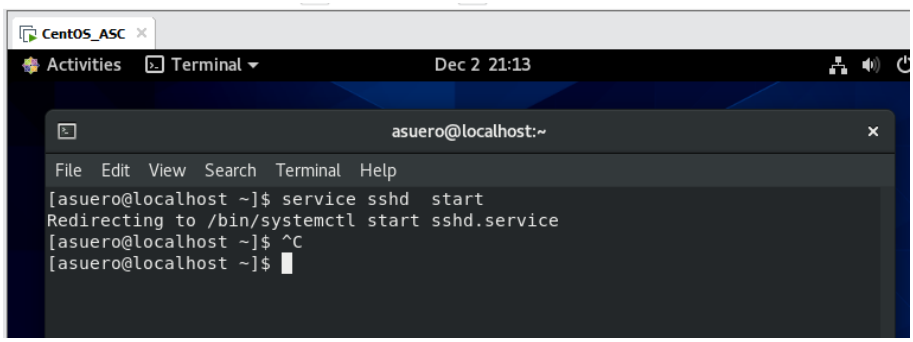
-Navigate to the **/etc/init.d** directory on your terminal for the list of available daemons on your Linux system. to go to this directory type **sudo cd /etc/init.d** and then once on this directory do a **ls** to see a list of the available daemons.



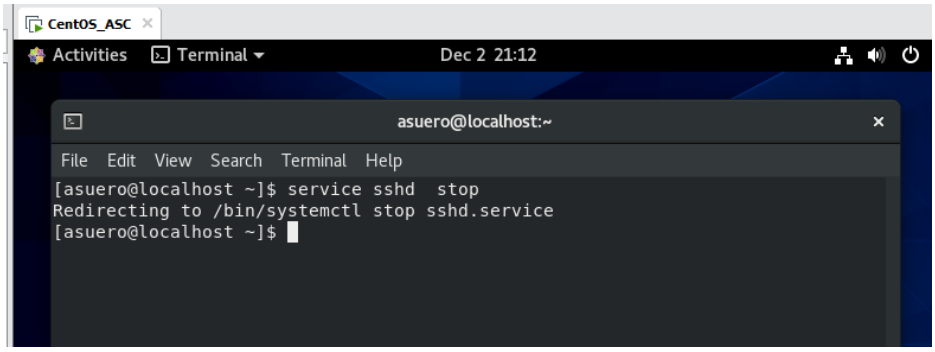
To see the status of a specific daemon you can type the fallowing command **service name of de service status** example **service sshd status**



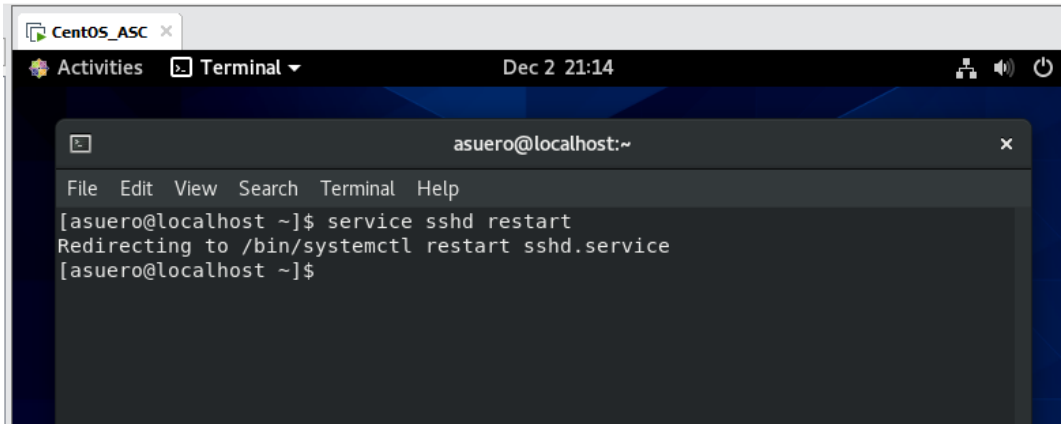
-If you want to **start** the ssh daemon type the fallowing **service sshd start**



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



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



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 fallowing command '**systemd.unit=emergency.target**'.

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