

# INSTALACIÓN DE SERVICIOS EN AMAZON WEB SERVICES (AWS)

EUCLIDES VIDES

FARITH PÉREZ  
DOCENTE

UNIVERSIDAD DE LA GUAJIRA  
SEDE MAICAO  
ELECTIVA DE REDES  
MAICAO-LA GUAJIRA  
2019

## 1. INTRODUCCIÓN

Amazon S.L. (sociedad limitada) es una compañía originaria de EEUU, su mercado principal es el comercio electrónico junto a servicios de computación en la nube. Tiene como sede la ciudad de Seattle en el estado estadounidense de Washington. Amazon fue una de las primeras compañías en ofrecer y vender bienes en internet a gran escala y su lema es “De la A a la Z” (From A to Z).

Amazon es la empresa en internet de venta al por menor más grande del mundo, donde puedes encontrar prácticamente cualquier cosa que necesites pues es muy seguro que alguien la esté vendiendo. La fundación de la compañía Amazon se realizó en el año de 1994 por Jeff Bezos tras dejar su anterior empleo como vicepresidente de la empresa D.E. Shaw & Co. en ese mismo año, esa empresa era una importante firma de Wall Street.

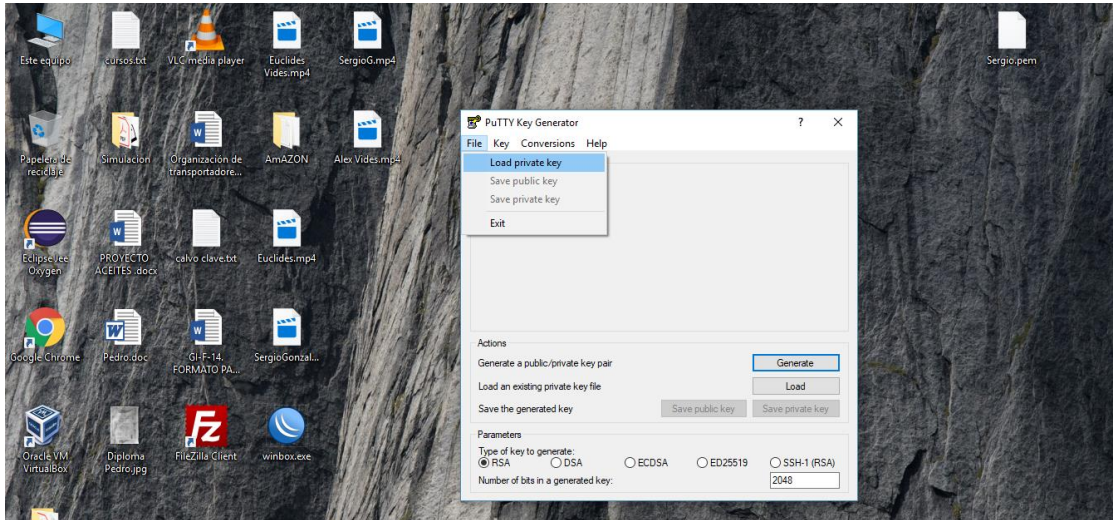
Tras su renuncia, Bezos decidió mudarse a Seattle y fue ahí en donde dio principio a la estructuración de un plan de negocios especializado a través de Internet, lo que con el tiempo se convirtió en lo que ahora todos conocemos como la empresa Amazon.com

## Tabla de contenido

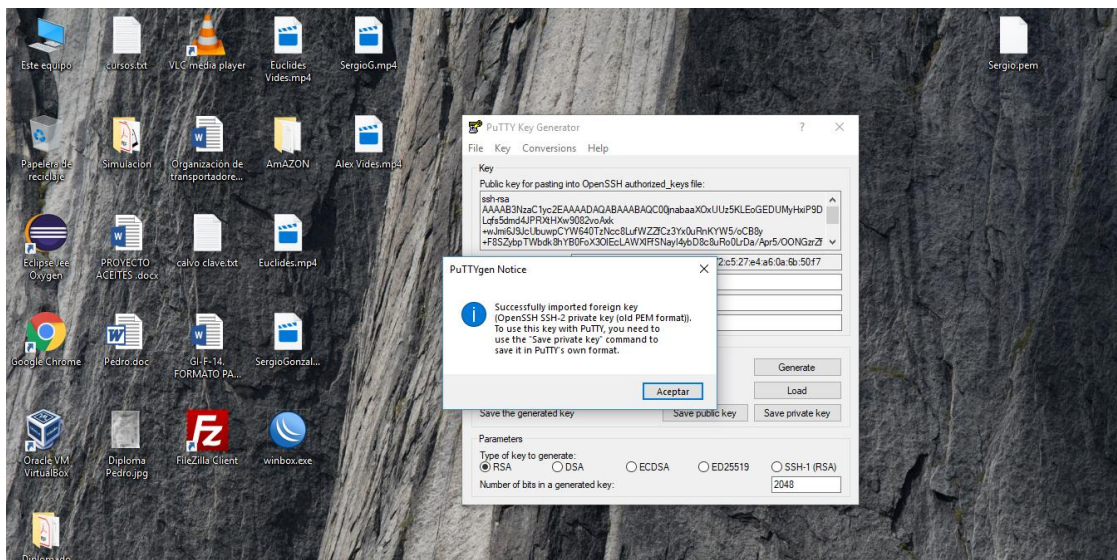
1. Introducción.....	2
2. PASOS PARA INSTALAR SERVICIOS.....	4
3. CONCLUSIÓN .....	21

## 2. PASOS PARA INSTALAR SERVICIOS

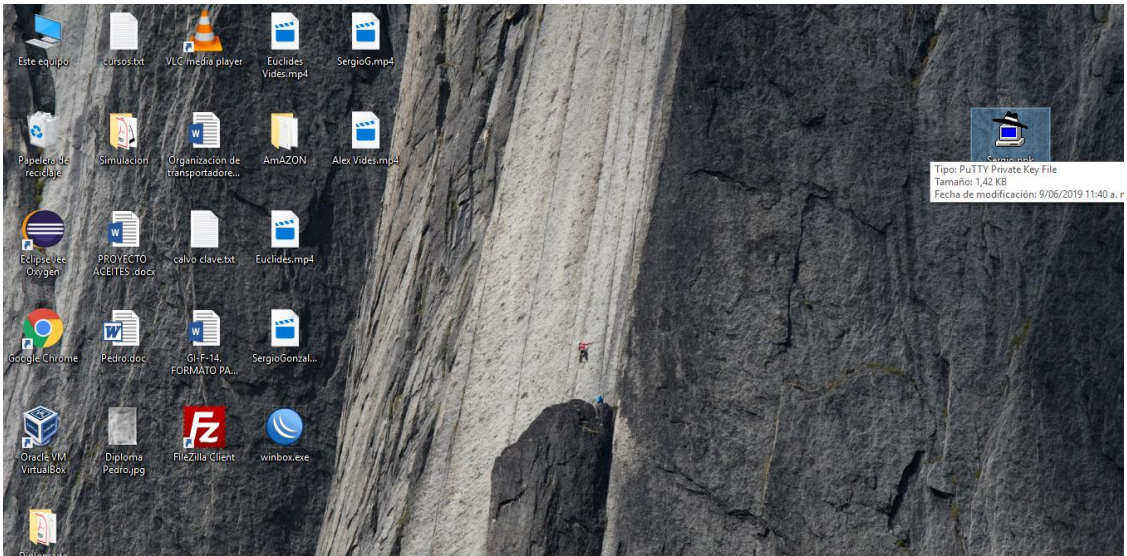
### 1. convertir la llave a formato ppk



### 2. Guardamos la contraseña convertida .



### 3. Tenemos la llave de acceso para configurar el servidor



#### 4. Verificamos que nuestra maquina este activa y chequeada

Instances | EC2 Management Console

https://us-west-1.console.aws.amazon.com/ec2/v2/home?region=us-west-1#Instances:sort=instancetype

aws Servicios Grupos de recursos

ayvides Norte de California Soporte

EC2 Dashboard  
Events  
Tags  
Reports  
Limits

INSTANCES  
Instances  
Launch Templates  
Spot Requests  
Reserved Instances  
Dedicated Hosts  
Capacity Reservations

IMAGES  
AMIs  
Bundle Tasks

ELASTIC BLOCK STORE  
Volumes  
Snapshots

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

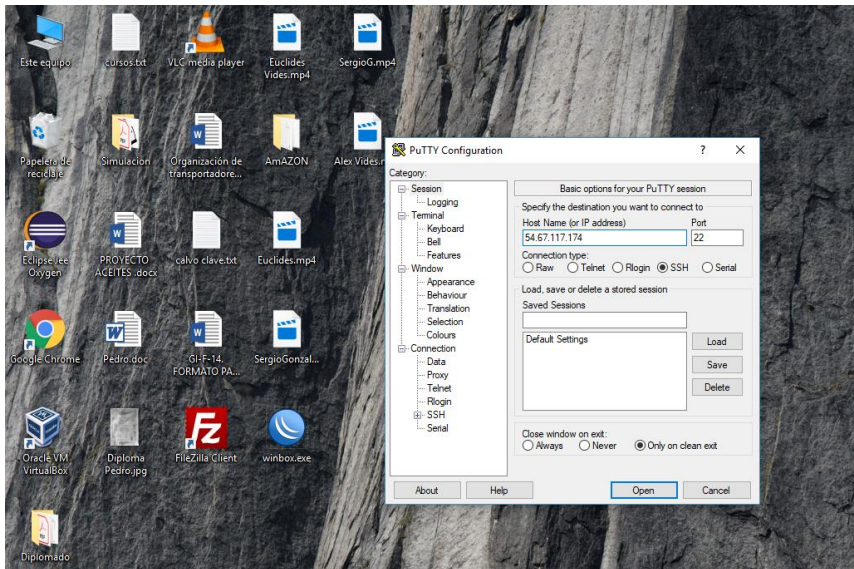
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4
	i-0935f1bd6b70feec	t2.micro	us-west-1a	running	2/2 checks ...	None	ec2-54-67-117-174.us-...	54.6

Instance: i-0935f1bd6b70feec Public DNS: ec2-54-67-117-174.us-west-1.compute.amazonaws.com

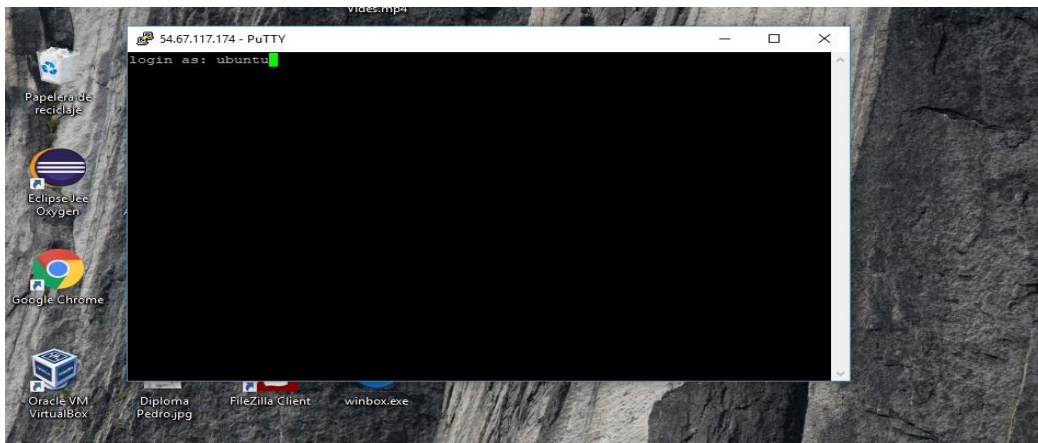
Description Status Checks Monitoring Tags

Instance ID	i-0935f1bd6b70feec	Public DNS (IPv4)	ec2-54-67-117-174.us-west-1.compute.amazonaws.com
Instance state	running	IPv4 Public IP	54.67.117.174

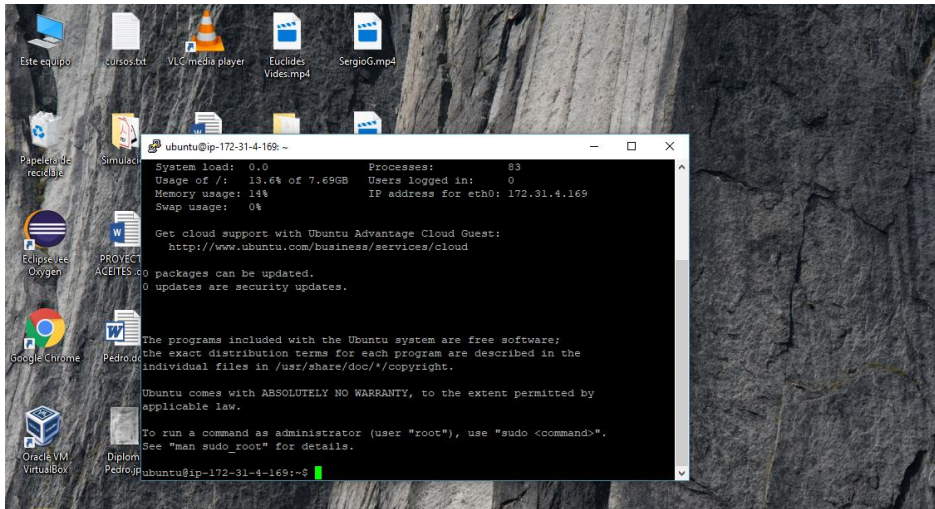
5. Verificamos la IP del servidor y la ingresamos al putty



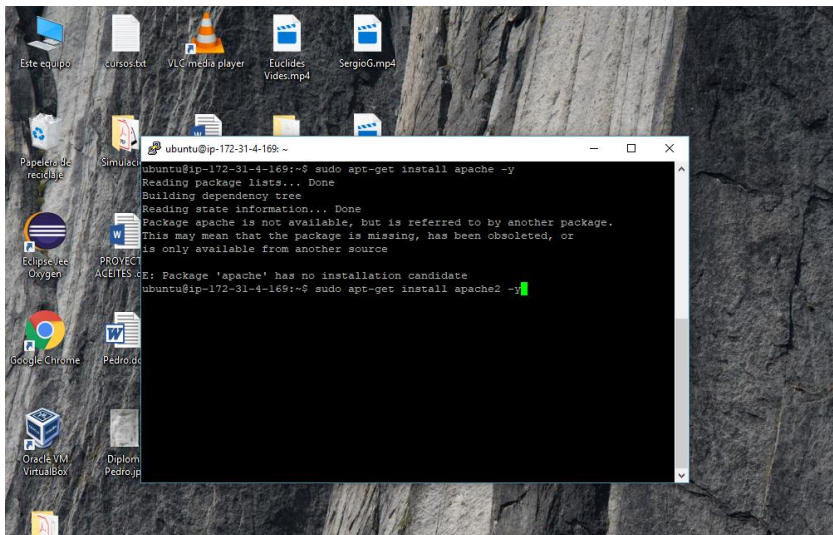
6. Ingresamos el nombre de usuario por defecto que es ubuntu



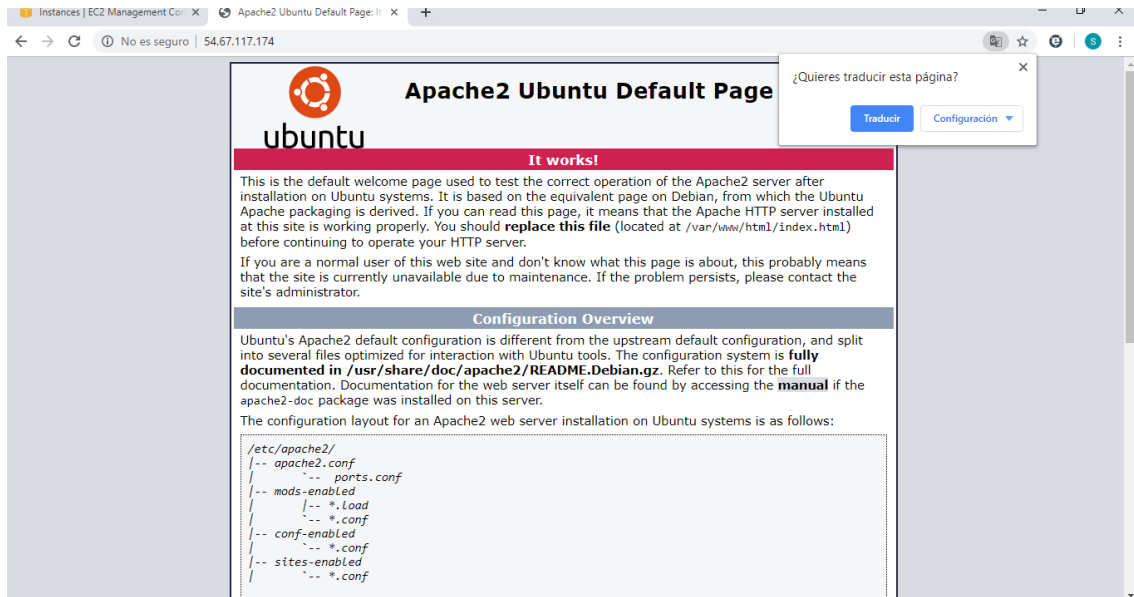
7. Vemos el mensaje de bienvenida al momento de ingresar a la máquina virtual



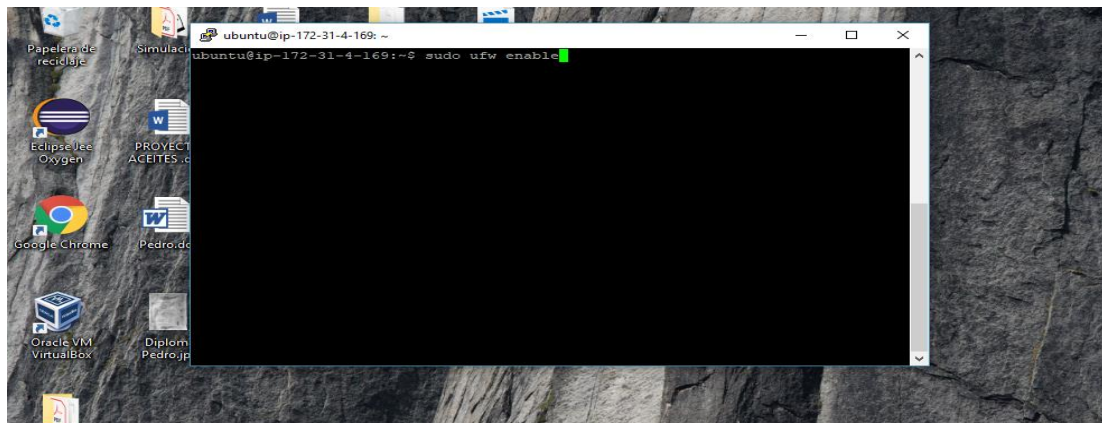
8. Ingresamos el código el cual nos va a instalar el apache



9. Ingresamos la dirección IP para verificar si se instaló el apache

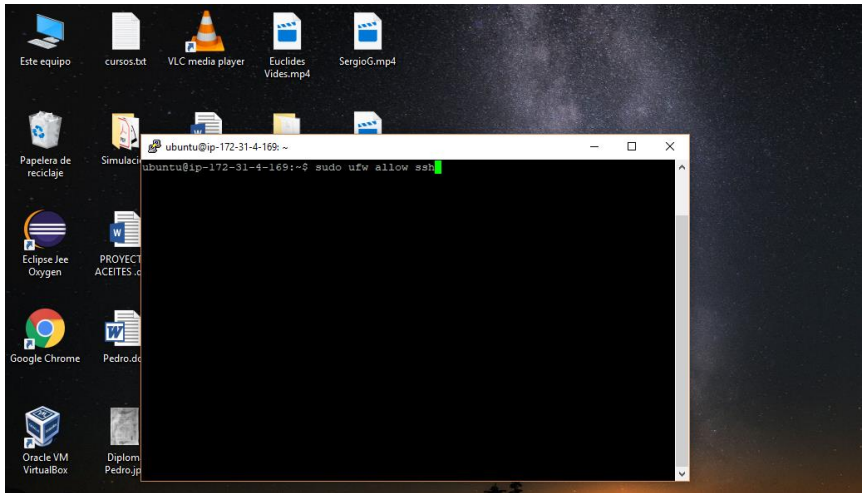


## 10. Esta es la instalación del firewall

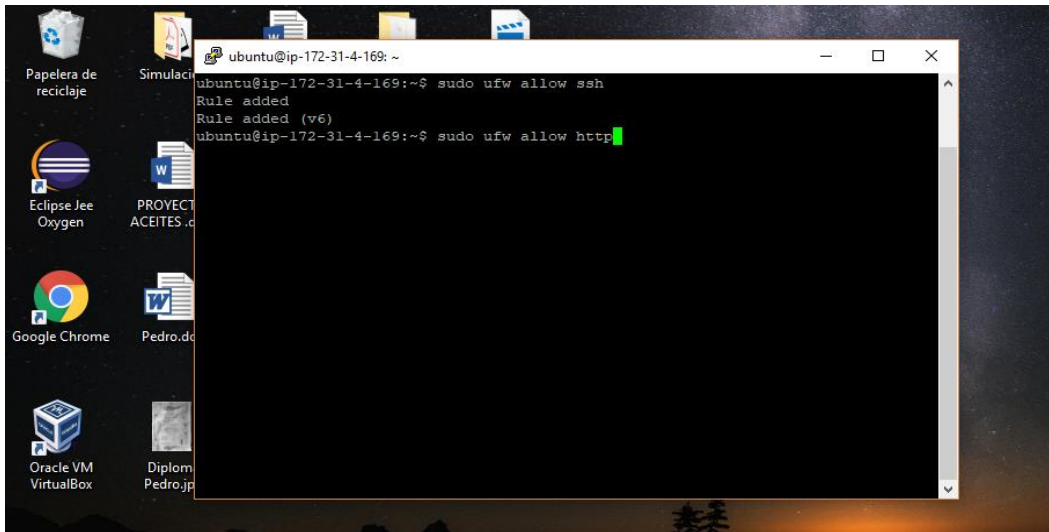


## 11. Instalamos el servicio de ssh

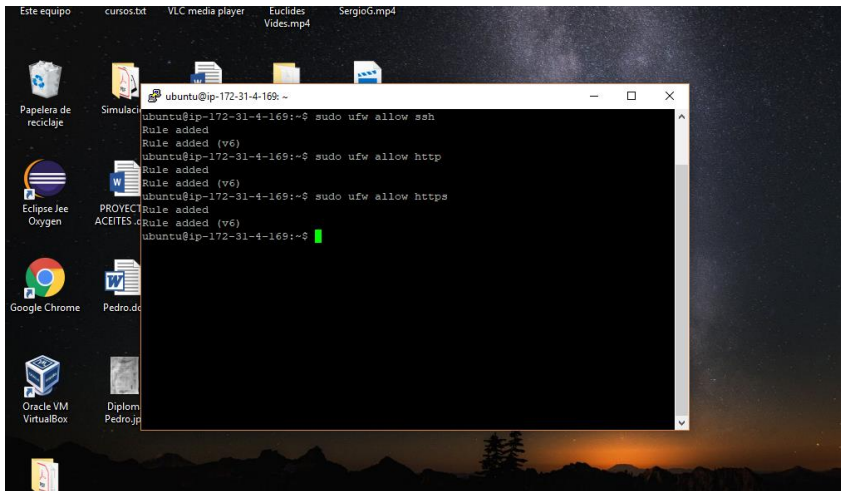




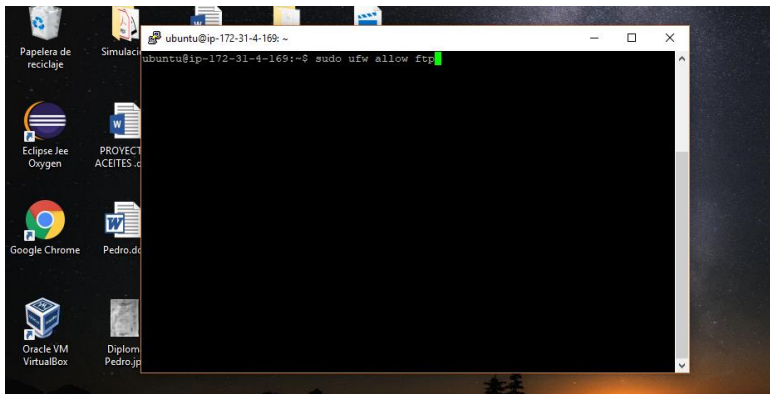
## 12.Instalamos el servicio de http



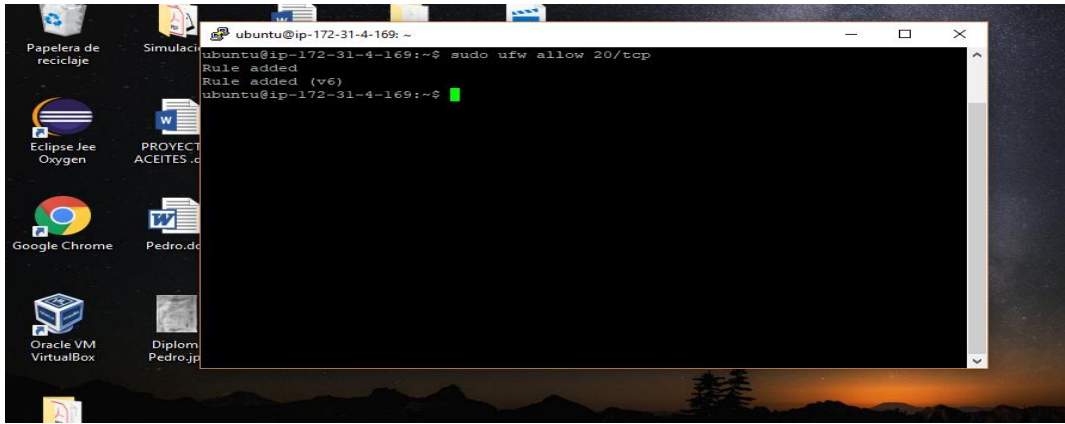
## 13.Aquí en sudo instalamos el servicio https



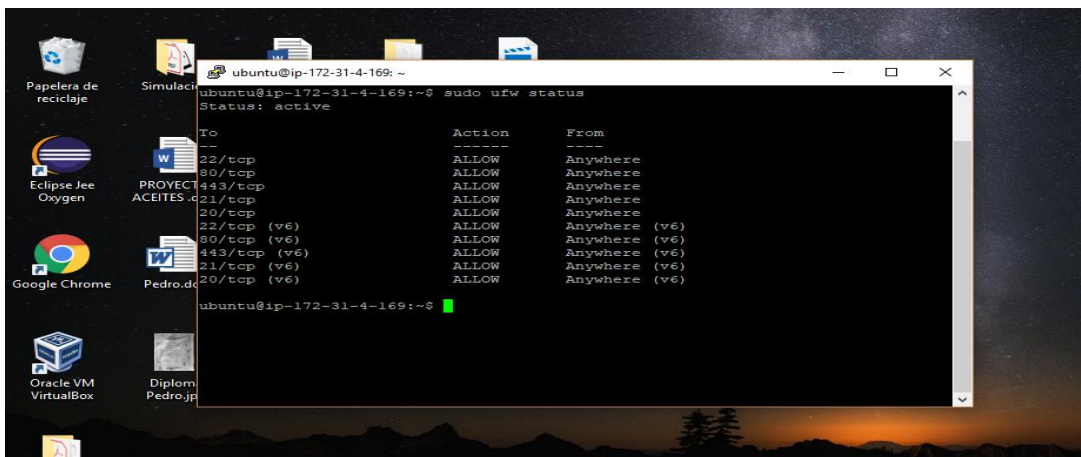
14. Aquí en sudo instalamos el servicio ftp



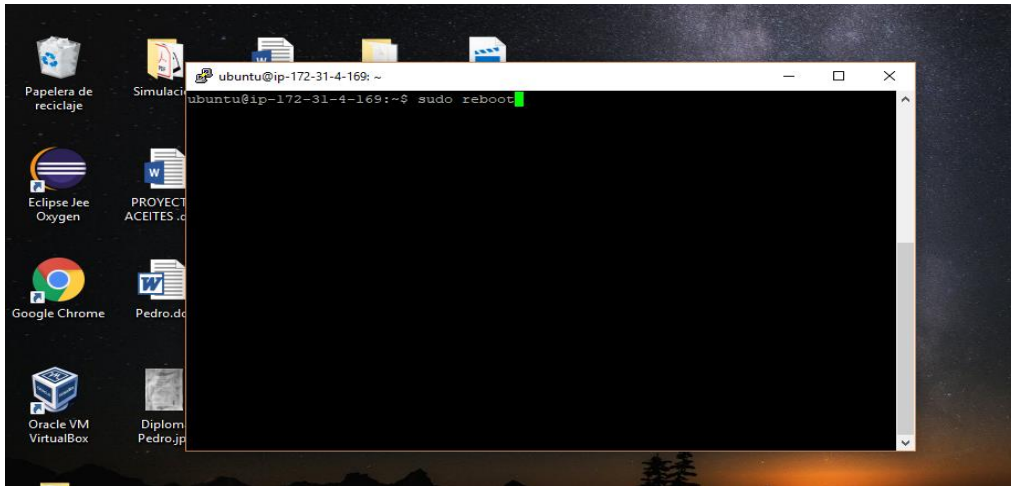
15. Habilitamos los puertos del ftp en la máquina virtual



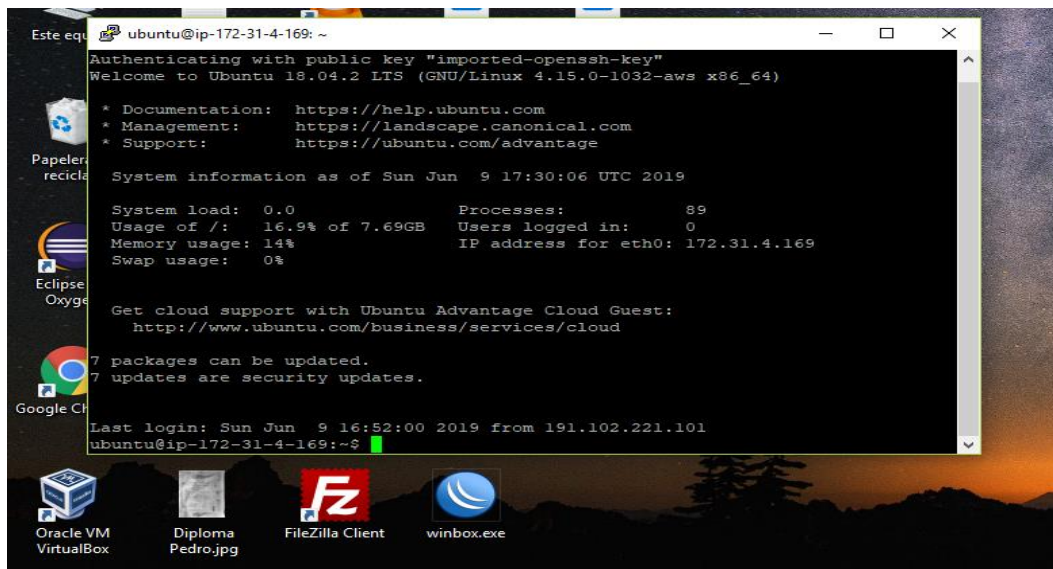
16. Aquí nos muestra los puertos habilitados



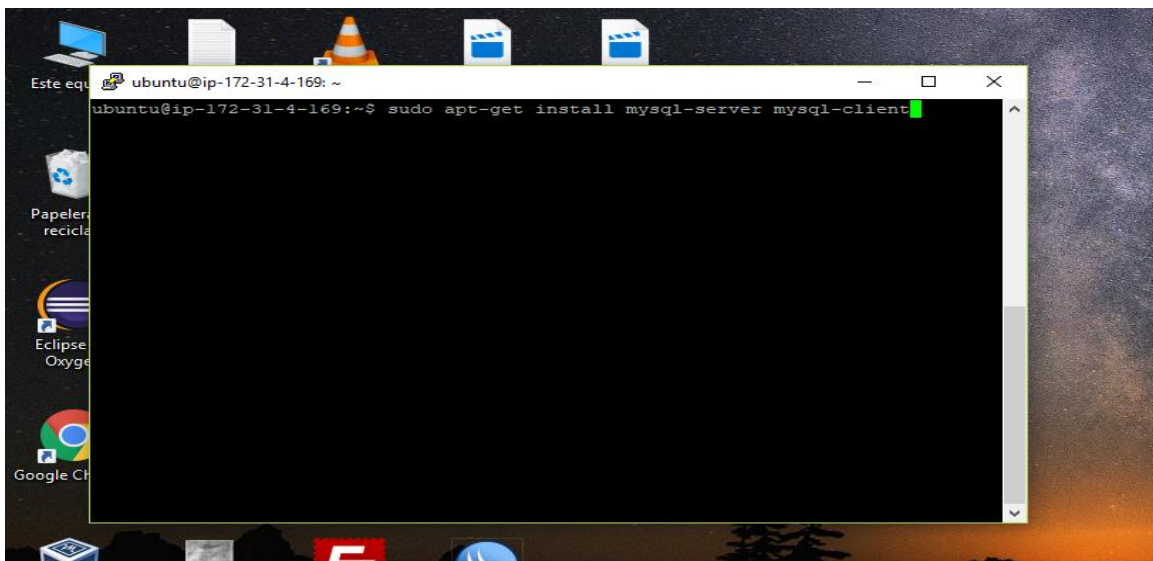
17. Se reinicia la maquina virtual para que se guarde los cambios



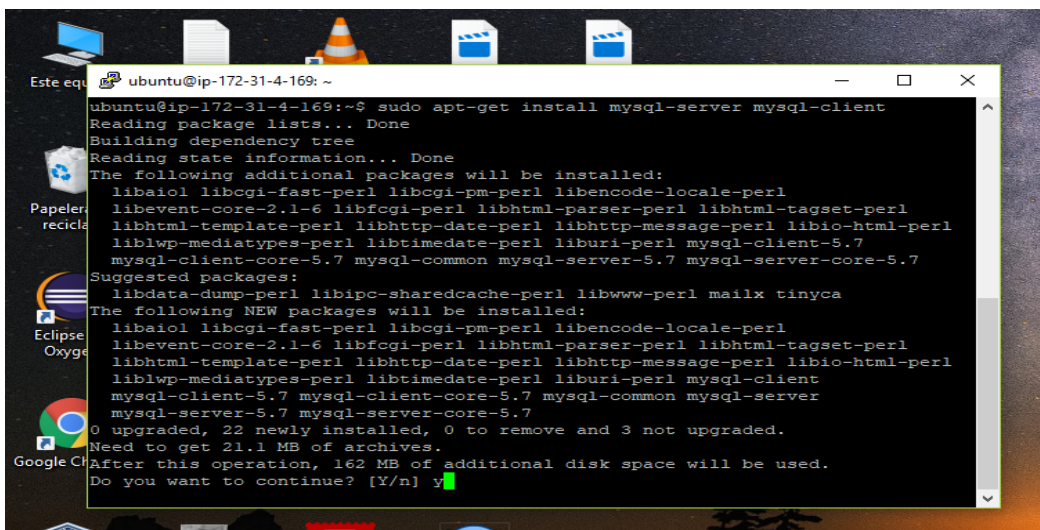
18. Ingresamos a la maquina virtual



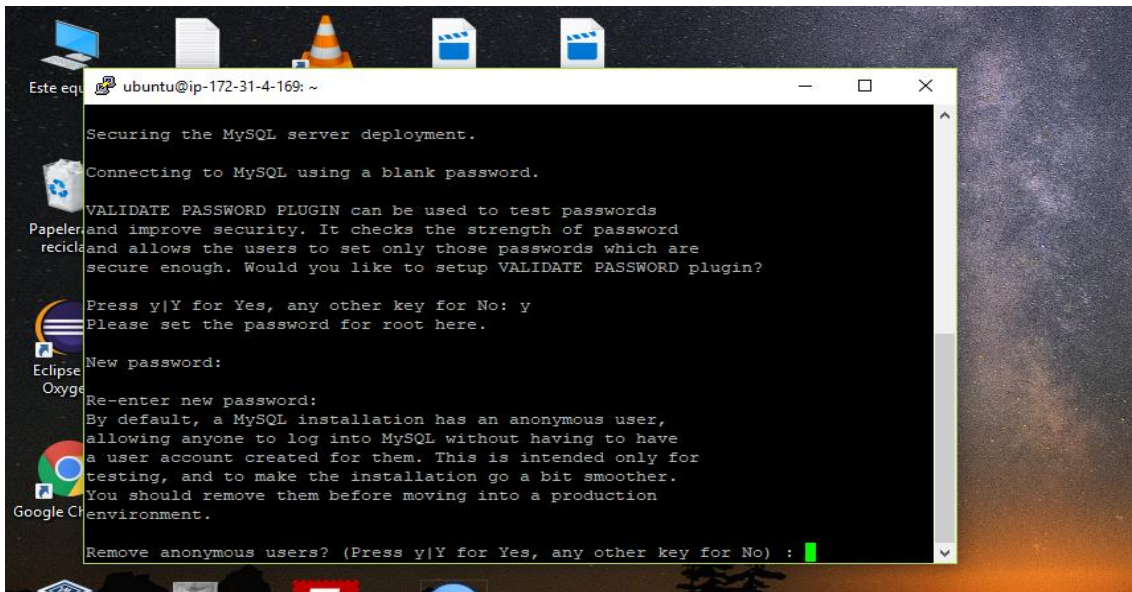
19. Instalamos Mysql



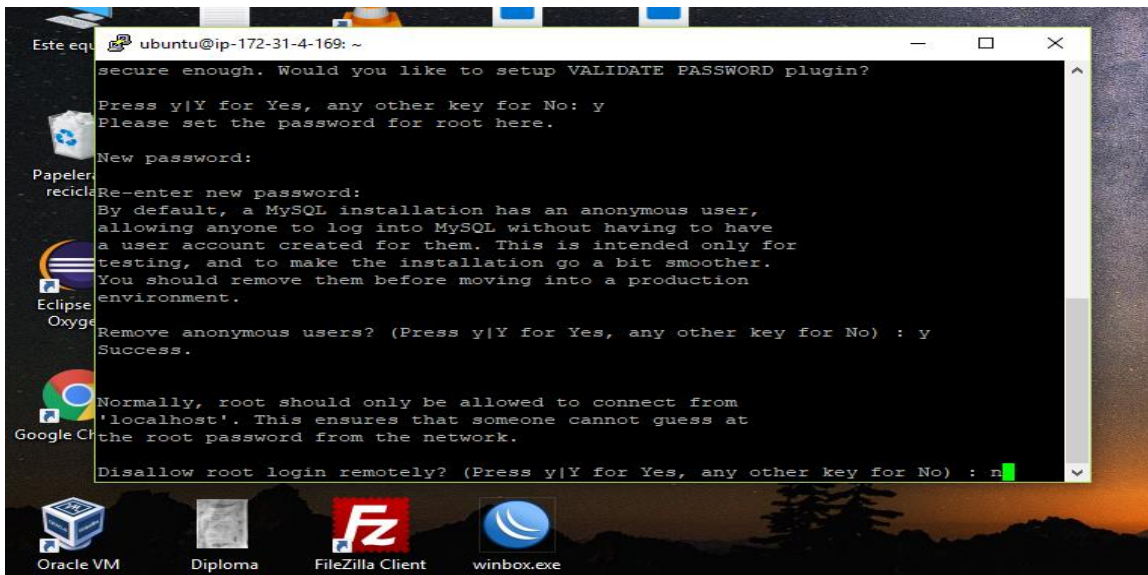
20. Aceptamos la instalación de paquete de Mysql



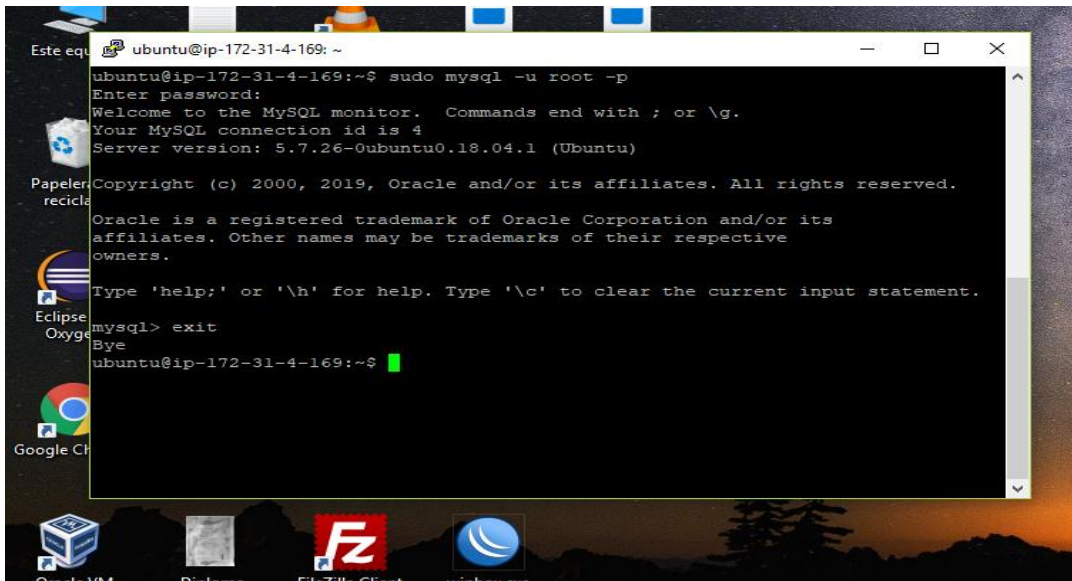
21. Esta es la instalación de seguridad paquete de Mysql



22. Ingresamos la contraseña para la base de datos



23. Ingresamos a nuestra base de datos



## 24. Aca ingresamos el código para ingresar la configurar el ftp

**Prerequisites**

To follow along with this tutorial you will need:

- **An Ubuntu 18.04 server, and a non-root user with sudo privileges:** You can learn more about how to set up a user with these privileges in our [Linux user guide](#).

### Step 1 – Installing vsftpd

Let's start by updating our package list and installing the vsftpd

```
$ sudo apt update  
$ sudo apt install vsftpd
```

When the installation is complete, let's copy the configuration configuration, saving the original as a backup:

```
$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig
```

With a backup of the configuration in place, we're ready to con

```
ubuntu@ip-172-31-4-169:~$ sudo apt install vsftpd
```

## 25. Configuramos el puerto 990 para el ftp

Instances | EC2 Management Co... | Apache2 Ubuntu Default Page | Instalar MySQL y Workbench en... | How To Set Up vsftpd for a User

DigitalOcean, LLC [US] | https://www.digitalocean.com/community/tutorials/how-to-set-up-vsftpd-for-a-user-s-directory-on-ubuntu-18-04

## Prerequisites

To follow along with this tutorial you will need:

- **An Ubuntu 18.04 server, and a non-root user with sudo privileges:** You can learn more about how to set up a user with these privileges in our [Linux user guide](#).

## Step 1 – Installing vsftpd

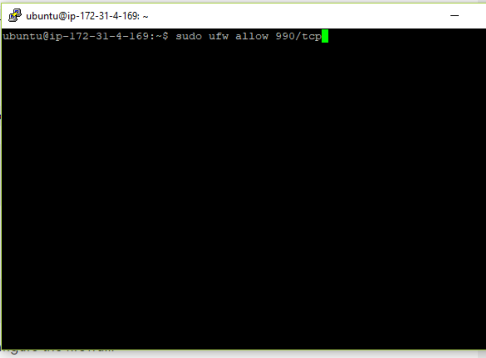
Let's start by updating our package list and installing the vsftpd

```
$ sudo apt update
$ sudo apt install vsftpd
```

When the installation is complete, let's copy the configuration configuration, saving the original as a backup:

```
$ sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.orig
```

With a backup of the configuration in place, we're ready to con...



## 26. Activamos los puertos 40000 y 50000 para el ftp

Instances | EC2 Management Co... | Apache2 Ubuntu Default Page | Instalar MySQL y Workbench en... | How To Set Up vsftpd for a User

DigitalOcean, LLC [US] | https://www.digitalocean.com/community/tutorials/how-to-set-up-vsftpd-for-a-user-s-directory-on-ubuntu-18-04

You may have other rules in place or no firewall rules at all. Since only SSH traffic is permitted in this case, we'll need to add rules for FTP traffic.

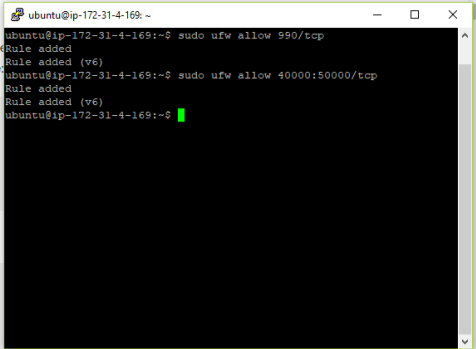
Let's open ports 20 and 21 for FTP, port 990 for when we enable the range of passive ports we plan to set in the configuration file:

```
$ sudo ufw allow 20/tcp
$ sudo ufw allow 21/tcp
$ sudo ufw allow 990/tcp
$ sudo ufw allow 40000:50000/tcp
$ sudo ufw status
```

Our firewall rules should now look like this:

```
Output
Status: active

To Action From
--
OpenSSH ALLOW Anywhere
990/tcp ALLOW Anywhere
20/tcp ALLOW Anywhere
21/tcp ALLOW Anywhere
40000:50000/tcp ALLOW Anywhere
```





## 27. Miramos el estado de todos los puertos para ver si están instalados

You may have other rules in place or no firewall rules at all. Since only SSH traffic is permitted in this case, we'll need to add rules for FTP traffic.

Let's open ports 20 and 21 for FTP, port 990 for when we enable the range of passive ports we plan to set in the configuration file.

```
$ sudo ufw allow 20/tcp
$ sudo ufw allow 21/tcp
$ sudo ufw allow 990/tcp
$ sudo ufw allow 40000:50000/tcp
$ sudo ufw status
```

Our firewall rules should now look like this:

```
Output
Status: active

To Action From
--
20/tcp ALLOW Anywhere
21/tcp ALLOW Anywhere
990/tcp ALLOW Anywhere
40000:50000/tcp ALLOW Anywhere
22/tcp (v6) ALLOW Anywhere (v6)
80/tcp (v6) ALLOW Anywhere (v6)
443/tcp (v6) ALLOW Anywhere (v6)
21/tcp (v6) ALLOW Anywhere (v6)
20/tcp (v6) ALLOW Anywhere (v6)
990/tcp (v6) ALLOW Anywhere (v6)
40000:50000/tcp (v6) ALLOW Anywhere (v6)
```

## 28. Habilitamos los puertos 990, 40000 y 50000 a la instancia

Type	Protocol	Port Range	Source	Description
HTTP	TCP	80	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTP	TCP	80	:::0	e.g. SSH for Admin Desktop
SSH	TCP	22	0.0.0.0/0	e.g. SSH for Admin Desktop
Custom TCP f	TCP	21	0.0.0.0/0	Puerto ftp
Custom TCP f	TCP	21	:::0	Puerto ftp
Custom TCP f	TCP	20	0.0.0.0/0	puerto ftp
Custom TCP f	TCP	990	0.0.0.0/0	Puerto ftp
Custom TCP f	TCP	990	:::0	Puerto ftp
Custom TCP f	TCP	40000 - 50000	0.0.0.0/0	Puerto ftp
Custom TCP f	TCP	40000 - 50000	:::0	Puerto ftp
HTTPS	TCP	443	0.0.0.0/0	e.g. SSH for Admin Desktop
HTTPS	TCP	443	:::0	e.g. SSH for Admin Desktop

NOTE: Any edits made on existing rules will result in the edited rule being deleted and a new rule created with the new details. This will cause traffic that depends on that rule to be dropped for a very brief period of time until the new rule can be created.

### 30. Creamos el usuario ftp y asignamos la contraseña

With vsftpd installed and the necessary ports open, let's move on to creating a dedicated FTP user.

### Step 3 – Preparing the User Directory

We will create a dedicated FTP user, but you may already have a user. If you do, we recommend that you start with a new user until you've configured vsftpd.

First, add a test user:

```
$ sudo adduser sammy
```

Assign a password when prompted. Feel free to press ENTER through the prompts.

FTP is generally more secure when users are restricted to a specific directory. vsftpd accomplishes this with `chroot` jails. When `chroot` is enabled for a user, they are restricted to their home directory by default. However, because of the way `vsftpd` secures the directory, it must not be writable by the user. This is fine for a new user who should only connect via FTP, but an existing user may need to write to their home folder if they also have shell access.

In this example, rather than removing write privileges from the home directory, let's create an `ftp` directory to serve as the `chroot` and a writable `files` directory to hold the actual files.

SCROLL TO TOP

### 31. Creamos la carpeta ftp y le asignaremos el documento ftp text

Verify the permissions:

```
$ sudo ls -la /home/sammy/ftp
```

Output

```
total 8
dr-xr-xr-x 2 nobody nogroup 4096 Aug 24 21:29
drwxr-xr-x 3 sammy sammy 4096 Aug 24 21:29
```

Next, let's create the directory for file uploads and assign permissions:

```
$ sudo mkdir /home/sammy/ftp/files
$ sudo chown sammy:sammy /home/sammy/ftp/files
```

A permissions check on the `ftp` directory should return:

```
$ sudo ls -la /home/sammy/ftp
```

Output

```
total 12
dr-xr-xr-x 3 nobody nogroup 4096 Aug 26 14:01 .
```

Terminal window showing commands:

```
ubuntu@ip-172-31-4-169:~$ sudo mkdir /home/ftpsergio/ftp
ubuntu@ip-172-31-4-169:~$ sudo chown nobody:nogroup /home/ftpsergio/ftp
chown: cannot access '/home/ftpsergio/ftp': No such file or directory
ubuntu@ip-172-31-4-169:~$ sudo chown nobody:nogroup /home/ftpsergio/ftp
ubuntu@ip-172-31-4-169:~$ sudo chmod a-w /home/ftpsergio/ftp
ubuntu@ip-172-31-4-169:~$ sudo ls -la /home/ftpsergio/ftp
total 8
dr-xr-xr-x 2 nobody nogroup 4096 Jun 9 17:52 .
drwxr-xr-x 3 ftpsergio ftpsergio 4096 Jun 9 17:52 ..
ubuntu@ip-172-31-4-169:~$ sudo mkdir /home/ftpsergio/ftp/archivos
ubuntu@ip-172-31-4-169:~$ sudo chown ftpsergio:ftpsergio /home/ftpsergio/ftp/archivos
ubuntu@ip-172-31-4-169:~$ sudo ls -la /home/ftpsergio/ftp
total 12
dr-xr-xr-x 3 nobody nogroup 4096 Jun 9 17:59 .
drwxr-xr-x 3 ftpsergio ftpsergio 4096 Jun 9 17:52 ..
drwxr-xr-x 2 ftpsergio ftpsergio 4096 Jun 9 17:59 archivos
ubuntu@ip-172-31-4-169:~$
```

### 32. Le damos acceso al usuario ftp par a tener acceso a la carpeta

The screenshot shows a browser window with a tutorial page from DigitalOcean. A yellow note states: "Note: In step 2, we opened the ports that we set here for the passive port range. If you change the values, be sure to update your firewall settings." Below the note, text explains that FTP access is configured on a case-by-case basis by adding users to a list. A terminal window shows the configuration of `/etc/vsftpd.conf` with the following settings:

```
...
userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

Text below the terminal explains that `userlist_deny` toggles the logic: when set to YES, users on the list are denied; when set to NO, only users on the list are allowed access. It also mentions adding the user to `/etc/vsftpd.userlist` using the `-a` flag. Another terminal window shows the full configuration of `/etc/vsftpd.conf` with the following settings:

```
# encrypted connections.
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
ssl_enable=NO

# Uncomment this to indicate that vsftpd use a utf8 filesystem.
#utf8_filesystem=YES

user_sub_token=$USER
local_root=/home/$USER/ftp

pasv_min_port=40000
pasv_max_port=50000

userlist_enable=YES
userlist_file=/etc/vsftpd.userlist
userlist_deny=NO
```

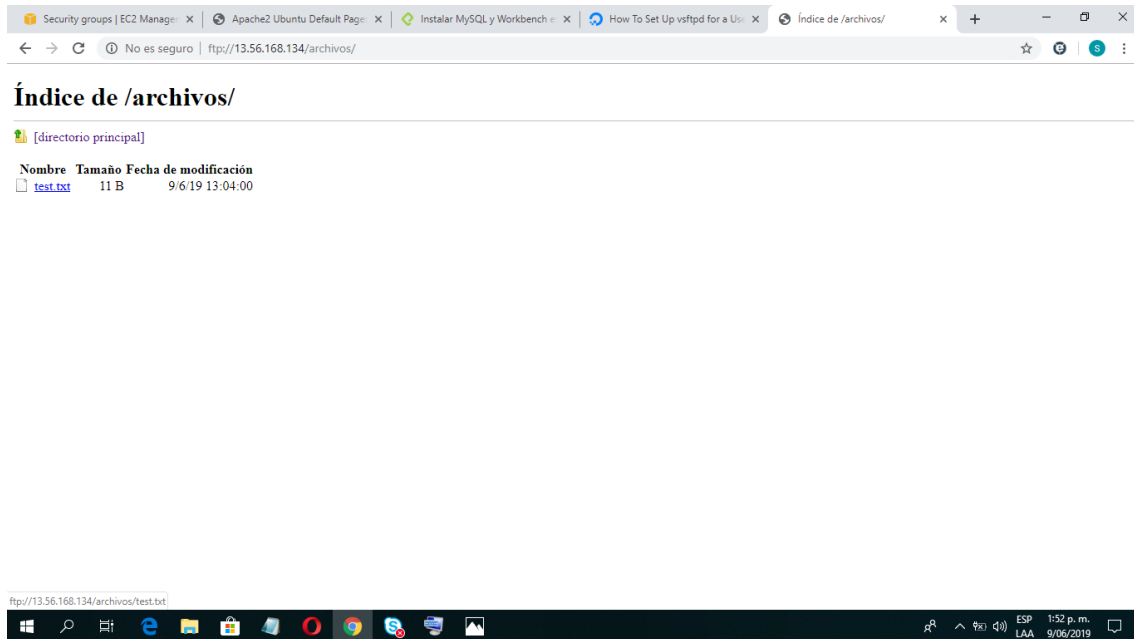
### 33. verificamos los usuarios ingresados

The screenshot shows a terminal window with the command `sudo systemctl restart vsftpd` being executed. Below the terminal, text explains that with the configuration in place, it's time to test FTP access. It mentions that the user `anonymous` should be able to access the directory. The terminal shows the following sequence of commands and output:

```
ubuntu@ip-172-31-4-169:~$ sudo systemctl restart vsftpd
ubuntu@ip-172-31-4-169:~$ cd /home/
ubuntu@ip-172-31-4-169:~/home$ ls
ftpsergio ubuntu
ubuntu@ip-172-31-4-169:~/home$ sudo nano /etc/vsftpd.userlist
ubuntu@ip-172-31-4-169:~/home$ sudo systemctl restart vsftpd
Unknown operation restart.
ubuntu@ip-172-31-4-169:~/home$ sudo systemctl restart vsftpd
Failed to restart vsftpd.service: Unit vsftpd.service not found.
ubuntu@ip-172-31-4-169:~/home$ sudo systemctl restart vsftpd
ubuntu@ip-172-31-4-169:~/home$ clear
```

At the bottom of the terminal, a prompt is visible: `Name (203.0.113.0:default): anonymous`.

## 35. Vemos los archivos que están montados en el ftp



The screenshot shows a web browser window with the address bar displaying `ftp://13.56.168.134/archivos/`. The page title is "Índice de /archivos/". Below the title, there is a link for "[directorio principal]". A table lists the files in the directory:

Nombre	Tamaño	Fecha de modificación
<a href="#">test.txt</a>	11 B	9/6/19 13:04:00

The Windows taskbar is visible at the bottom, showing the time as 1:52 p.m. on 9/06/2019.

### 3. CONCLUSIÓN

Se instaló de manera correcta todos los servicios, se realizó los pasos a pasos que para su correcta instalación. Los servicios activados fueron ssh, ftp, http y http.

