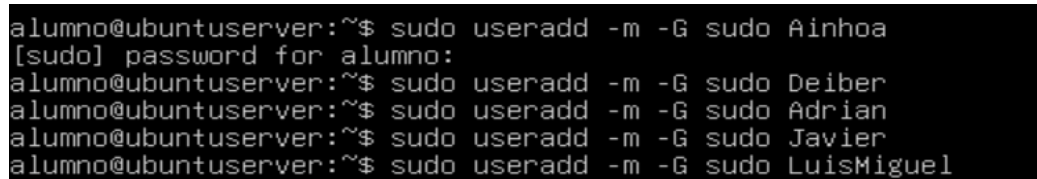


# SISTEMAS SPRINT 1

## Usuarios y grupo sudo:

Primero usaremos los siguientes comandos para crear a los distintos usuarios y añadirlos al grupo sudo.

```
sudo useradd -m -G sudo Ainhoa
sudo useradd -m -G sudo Deiber
sudo useradd -m -G sudo Adrian
sudo useradd -m -G sudo Javier
sudo useradd -m -G sudo LuisMiguel
```



```
alumno@ubuntuserver:~$ sudo useradd -m -G sudo Ainhoa
[sudo] password for alumno:
alumno@ubuntuserver:~$ sudo useradd -m -G sudo Deiber
alumno@ubuntuserver:~$ sudo useradd -m -G sudo Adrian
alumno@ubuntuserver:~$ sudo useradd -m -G sudo Javier
alumno@ubuntuserver:~$ sudo useradd -m -G sudo LuisMiguel
```

Una vez creados les ponemos una contraseña mediante este comando. La contraseña será el nombre en minúscula.

```
sudo passwd Ainhoa
sudo passwd Deiber
sudo passwd Adrian
sudo passwd Javier
sudo passwd LuisMiguel
```

## Actualizaciones:

Actualizar repositorios: `sudo apt update`

```
alumno@ubuntuserver:~$ sudo apt update
[sudo] password for alumno:
Obj:1 http://es.archive.ubuntu.com/ubuntu noble InRelease
Des:2 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Des:3 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Des:4 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Des:5 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [919 kB]
Des:6 http://es.archive.ubuntu.com/ubuntu noble-updates/main Translation-en [206 kB]
Des:7 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Des:8 http://es.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Packages [759 kB]
Des:9 http://es.archive.ubuntu.com/ubuntu noble-updates/restricted Translation-en [152 kB]
Des:10 http://es.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Des:11 http://es.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1.041 kB]
Des:12 http://es.archive.ubuntu.com/ubuntu noble-updates/universe Translation-en [261 kB]
Des:13 http://es.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [364 kB]
Des:14 http://es.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Packages [30,1 kB]
Des:15 http://es.archive.ubuntu.com/ubuntu noble-updates/multiverse Translation-en [5.884 B]
Des:16 http://es.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Des:17 http://es.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Des:18 http://es.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [212 B]
Des:19 http://es.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Packages [14,2 kB]
Des:20 http://es.archive.ubuntu.com/ubuntu noble-backports/universe Translation-en [12,1 kB]
Des:21 http://es.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [20,0 kB]
Des:22 http://es.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Des:23 http://security.ubuntu.com/ubuntu noble-security/main amd64 Packages [668 kB]
Des:24 http://security.ubuntu.com/ubuntu noble-security/main Translation-en [128 kB]
Des:25 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [9.012 B]
Des:26 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Packages [719 kB]
Des:27 http://security.ubuntu.com/ubuntu noble-security/restricted Translation-en [143 kB]
Des:28 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Des:29 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Packages [823 kB]
Des:30 http://security.ubuntu.com/ubuntu noble-security/universe Translation-en [177 kB]
Des:31 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [51,9 kB]
Des:32 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Packages [26,2 kB]
Des:33 http://security.ubuntu.com/ubuntu noble-security/multiverse Translation-en [4.892 B]
Des:34 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [208 B]
Descargados 7.066 kB en 3s (2.291 kB/s)
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 144 paquetes. Ejecute «apt list --upgradable» para verlos.
```

Instalar actualizaciones disponibles: `sudo apt upgrade`

Listar actualizaciones: `sudo apt list --upgradable`

```
alumno@ubuntuserver:~$ sudo apt list --upgradable
Listando... Hecho
alumno@ubuntuserver:~$
```

`sudo apt install *nombre del paquete*`

Las actualizaciones no se deberían de automatizar debido a que nunca deberías de actualizar sin tener idea porque puede causar fallos de seguridad o inestabilidad si no sabes qué cambios hay.

## Instalar software:

Instalaremos un software básico, como los editores de texto vim y nano, el monitor de procesos htop, y net-tools, el cual incluye comandos como ifconfig.

`sudo apt update && sudo apt install -y vim nano htop net-tools`

```
alumno@ubuntuuserver:~$ sudo apt update && sudo apt install vim nano htop net-tools
[sudo] password for alumno:
Des:1 http://security.ubuntu.com/ubuntu noble-security InRelease [126 kB]
Obj:2 http://es.archive.ubuntu.com/ubuntu noble InRelease
Des:3 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Des:4 http://security.ubuntu.com/ubuntu noble-security/main amd64 Components [8.980 B]
Des:5 http://security.ubuntu.com/ubuntu noble-security/restricted amd64 Components [212 B]
Des:6 http://security.ubuntu.com/ubuntu noble-security/universe amd64 Components [52,0 kB]
Des:7 http://security.ubuntu.com/ubuntu noble-security/multiverse amd64 Components [212 B]
Des:8 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease [126 kB]
Des:9 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 Packages [919 kB]
Des:10 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 Components [151 kB]
Des:11 http://es.archive.ubuntu.com/ubuntu noble-updates/restricted amd64 Components [212 B]
Des:12 http://es.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Packages [1.041 kB]
Des:13 http://es.archive.ubuntu.com/ubuntu noble-updates/universe amd64 Components [364 kB]
Des:14 http://es.archive.ubuntu.com/ubuntu noble-updates/multiverse amd64 Components [940 B]
Des:15 http://es.archive.ubuntu.com/ubuntu noble-backports/main amd64 Components [208 B]
Des:16 http://es.archive.ubuntu.com/ubuntu noble-backports/restricted amd64 Components [216 B]
Des:17 http://es.archive.ubuntu.com/ubuntu noble-backports/universe amd64 Components [19,9 kB]
Des:18 http://es.archive.ubuntu.com/ubuntu noble-backports/multiverse amd64 Components [212 B]
Descargados 2.937 kB en 2s (1.591 kB/s)
```

## Backups:

Para hacer un backup y automatizarlo tenemos que hacer uso del crontab. Pongamos que queremos hacer una copia de seguridad a las 2AM de /etc y /home:

`sudo crontab -e`

Después, seleccionamos el editor que prefiramos, en este caso “nano” y escribimos cuando se va a realizar, y el comando a realizar.

```
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# 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 2 * * * tar -czvf /backup/backup_$(date +%F).tar.gz /etc /home
```

## Configurar red:

Ubuntu Server usa Netplan para configurar la red, así que modificamos este archivo con el editor “nano” para asignar una IP estática. Aplicamos los cambios con “sudo netplan apply”.

```
# This file is generated from information provided by the datasource. Changes
# to it will not persist across an instance reboot. To disable cloud-init's
# network configuration capabilities, write a file
# /etc/cloud/cloud.cfg.d/99-disable-network-config.cfg with the following:
# network: {config: disabled}
network:
  ethernets:
    enp0s3:
      dhcp4: true
      dhcp-identifier: mac
      addresses:
        - 10.0.2.15/24
      gateway: 10.0.2.1
  version: 2
```

```
      dhcp-identifier: mac
      addresses:
        - 10.0.2.15/24
      gateway4: 10.0.2.1
  version: 2

alumno@ubuntu-server:~$ sudo netplan apply

** (generate:1690): WARNING **: 13:13:27.283: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:1688): WARNING **: 13:13:27.628: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.

** (process:1688): WARNING **: 13:13:27.740: `gateway4` has been deprecated, use default routes instead.
See the 'Default routes' section of the documentation for more details.
alumno@ubuntu-server:~$
```

## Seguridad:

### iptables:

Para ver las reglas actuales:

```
sudo iptables -L -v
```

Para guardar las reglas:

```
sudo iptables-save | sudo tee /etc/iproute2/rt_tables
```

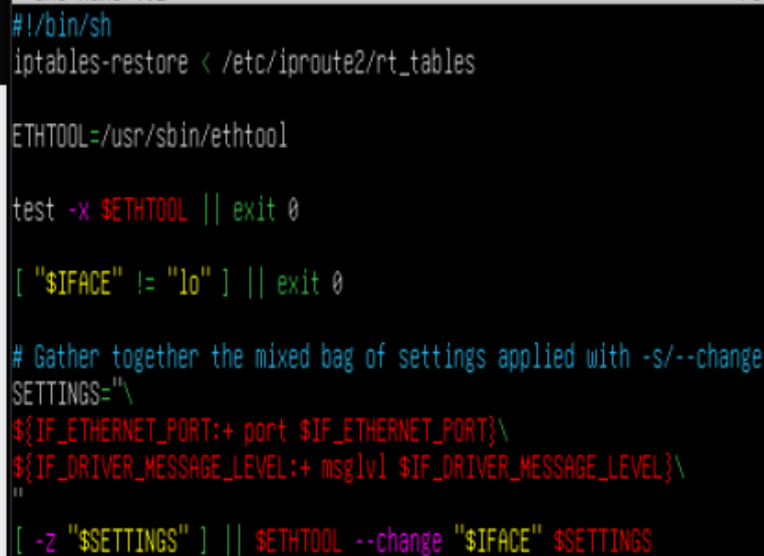
Para restaurarlas al inicio:

```
sudo nano /etc/network/if-pre-up.d/ethtool
```

Añadir lo siguiente:

```
#!/bin/sh
```

```
iptables-restore < /etc/iproute2/rt_tables
```



```
#!/bin/sh
iptables-restore < /etc/iproute2/rt_tables

ETHTOOL=/usr/sbin/ethtool

test -x $ETHTOOL || exit 0

[ "$IFACE" != "lo" ] || exit 0

# Gather together the mixed bag of settings applied with -s/--change
SETTINGS="\
${IF_ETHERNET_PORT:+ port $IF_ETHERNET_PORT}\
${IF_DRIVER_MESSAGE_LEVEL:+ msglvl $IF_DRIVER_MESSAGE_LEVEL}\
"

[ -z "$SETTINGS" ] || $ETHTOOL --change "$IFACE" $SETTINGS
```

Cambiar permisos:

```
sudo chmod +x /etc/network/if-pre-up.d/ethtool
```

Habría que bloquear todo menos las peticiones de ssh 22/tcp y las de 443/tcp y 80/tcp ya que són las de página web y por ende son las que deberíamos tener abiertas. En las ufw se haría lo mismo.

Además, por seguridad cambiaríamos el puerto ssh al 2022 ya que así es más seguro.

## ufw:

Permitir ssh:

```
sudo ufw allow 22/tcp
```

Activar el firewall:

```
sudo ufw enable
```

Ver estado:

```
sudo ufw status
```

```
alumno@ubuntu:~$ sudo chmod +x /etc/network/if-pre-up.d/ethtool
alumno@ubuntu:~$ sudo ufw allow 22/tcp
Rule added
Rule added (v6)
alumno@ubuntu:~$ sudo ufw enable
Firewall is active and enabled on system startup
alumno@ubuntu:~$ sudo ufw status
Status: active

To Action From
--
22 ALLOW Anywhere
22/tcp ALLOW Anywhere
22 (v6) ALLOW Anywhere (v6)
22/tcp (v6) ALLOW Anywhere (v6)

alumno@ubuntu:~$
```

## Conexión ssh:

Generar clave ssh:

```
ssh-keygen -t rsa -b 4096
```

Copiar clave pública al servidor:

```
ssh-copy-id usuario@192.168.1.100
```

```
alumno@ubuntu:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/alumno/.ssh/id_rsa): /home/alumno/.ssh/id_rsa
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/alumno/.ssh/id_rsa
Your public key has been saved in /home/alumno/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:KtQVfgRQHEfM3bt+vugKFbZvF0DrNNb3nDhwjxvtw alumno@ubuntu:~$
The key's randomart image is:
+---[RSA 4096]-----+
|      .+=*+. 0      |
|      ..+0 0 =      |
|      0 .0 * 0      |
|      . . . . = + 0 |
|      . . $ 0 . =. |
|      . . + . 0.+ |
|      . . . = = E+ |
|      . . =.=.= |
|      .++. *+ |
+---[SHA256]-----+
alumno@ubuntu:~$ ssh-copy-id alumno@10.0.2.15
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/alumno/.ssh/id_rsa.pub"
The authenticity of host '10.0.2.15 (10.0.2.15)' can't be established.
ED25519 key fingerprint is SHA256:Q17QRjMP3RIRSNv+UOLmCDh2xKo+YMxdKCIXAKkBC8Y.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
alumno@10.0.2.15's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'alumno@10.0.2.15'"
and check to make sure that only the key(s) you wanted were added.

alumno@ubuntu:~$
```

Editar configuración:

```
sudo nano /etc/ssh/sshd_config
```

Cambiar esto:

```
PermitRootLogin no
```



PasswordAuthentication no

```
# To disable tunneled clear text passwords, change to no here!  
#PasswordAuthentication no  
#PermitEmptyPasswords no  
#PermitRootLogin no  
  
# Change to yes to enable challenge-response passwords (beware issues with  
# some PAM modules and threads)  
KbdInteractiveAuthentication no
```

Reiniciar ssh:

sudo systemctl restart ssh