

debian 12 "bookworm" + KDE

first install

- `sudo apt install git simplescreenrecorder clamtk remmina flameshot vim curl python3 python3-dev python3-pip python-is-python3 python3-requests build-essential openssh-server libreoffice`
- <https://wiki.fidmag.org/fidmag:receptes:linuxserver-debian13>
- HeidiSQL - <https://www.heidisql.com/download.php>
- docker - <https://docs.docker.com/engine/install/debian/>
- bitwarden - <https://bitwarden.com/download/>
- oracle virtualbox - https://www.virtualbox.org/wiki/Linux_Downloads
- code - <https://code.visualstudio.com/download>
- dropbox - https://www.dropbox.com/en_GB/install-linux

services

[https://wiki.fidmag.org/fidmag:receptes:linuxserver: ipv6](https://wiki.fidmag.org/fidmag:receptes:linuxserver:ipv6)

ntp

```
sudo apt install -y ntp
sudo ln -s /usr/share/zoneinfo/Etc/UTC localtime_old
sudo unlink /etc/localtime
sudo ln -s /usr/share/zoneinfo/Europe/Andorra /etc/localtime
sudo systemctl restart ntp.service
```

IP

canvi IP

- [debian_13](#)

canvi hostname

```
sudo vim /etc/hostname
```

IPv6 disable

```
# comprobar estat
ip a | grep inet6

# desactivar immediatament
```

```
sudo sysctl -w net.ipv6.conf.all.disable_ipv6=1
sudo sysctl -w net.ipv6.conf.default.disable_ipv6=1
sudo sysctl -w net.ipv6.conf.lo.disable_ipv6=1

# persistencia (solo activa tras un reboot)
echo "net.ipv6.conf.all.disable_ipv6 = 1" | sudo tee -a /etc/sysctl.conf
echo "net.ipv6.conf.default.disable_ipv6 = 1" | sudo tee -a /etc/sysctl.conf
echo "net.ipv6.conf.lo.disable_ipv6=1" | sudo tee -a /etc/sysctl.conf
```

IPv4 forward disable

```
# comprobar estat
sysctl net.ipv4.ip_forward

# desactivar inmediateament
sudo sysctl -w net.ipv4.ip_forward=0

# persistència
cho "net.ipv4.ip_forward=0" | sudo tee -a /etc/sysctl.conf
```

seguridad

- instalar librería contraseñas en diccionario:

```
sudo apt install libpam-cracklib
```

- añadir/reemplazar:

[/etc/pam.d/common-password](#)

```
password requisite pam_cracklib.so retry=3 minlen=8 difok=3
```

- parámetros:
 - retry: número de intentos antes de que el sistema devuelva un error en la autenticación y nos expulse.
 - minlen: es la longitud mínima de la contraseña, por defecto está en 8 caracteres.
 - difok: número de caracteres diferentes que debe tener la nueva clave en comparación con la antigua.
 - ucredit: caracteres en mayúscula que debe tener como mínimo o máximo.
 - lcredit: caracteres en minúscula que debe tener como mínimo o máximo.
 - dcredit: el número de dígitos que debe tener como mínimo o máximo.
 - ocredit: el número de otros caracteres (símbolos) que debe tener la clave como mínimo o máximo.
 - para los credit:
 - lcredit=-2 : significa que como mínimo debe tener 2 caracteres en minúscula.
 - lcredit=+2 : significa que como máximo debe tener 2 caracteres en minúscula.
- expira la contraseña y obliga a cambio en próximo login:

```
passwd -e <USUARIO>
```

- caducidad:

```
passwd -w 5 -x 30 -i 1 <USUARIO>
```

- **w**: aviso X días antes de la caducidad
- **x**: expira cada X días
- **i**: desactiva la cuenta a los X días si no ha habido cambio de contraseña. Solo root puede reactivar.

/via:<https://www.redeszone.net/tutoriales/seguridad/configurar-politica-contrasenas-debian/>

ufw

```
sudo apt install -y ufw
sudo ufw default deny incoming
sudo ufw default allow outgoing
sudo ufw allow ssh
sudo sed -i s/IPV6=yes/IPV6=no/g /etc/default/ufw
sudo ufw enable
sudo ufw status
sudo ufw app list
```

/via: <https://community.hetzner.com/tutorials/simple-firewall-management-with-ufw>

ssh

/via: <https://community.hetzner.com/tutorials/securing-ssh>

;/etc/ssh/sshd_config

```
Protocol 2          # disables protocol 1
LoginGraceTime 30   # tiempo disponible para teclear usuario y
                    # contraseña
AllowTcpForwarding no          # Disables port forwarding.
X11Forwarding no             # Disables remote GUI view.
AllowAgentForwarding no      # Disables the forwarding of the SSH
                    # login.
MaxAuthTries 2
MaxSessions 5
AllowUsers fidmag
ClientAliveInterval 300      # Timeout por inactividad
ClientAliveCountMax 1        # cliente ssh que no responde
PermitRootLogin no
```

```
sudo sshd -t # test configuration
sudo systemctl restart sshd
```

fail2ban

```
sudo apt install -y fail2ban
sudo systemctl enable fail2ban
sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
sudo vim /etc/fail2ban/jail.local # add enabled = true in [sshd] section
```

SU

```
sudo groupadd su
sudo usermod -a -G su fidmag
sudo dpkg-statoverride --update --add root su 4750 /bin/su
```

/via: <https://www.techrepublic.com/article/how-to-limit-access-to-the-su-command-in-linux/>

From:

<https://miguelangel.torresegea.es/wiki/> - miguel angel torres egea

Permanent link:

<https://miguelangel.torresegea.es/wiki/linux:debian:install-12?rev=1780140592>

Last update: **30/05/2026 04:29**

