



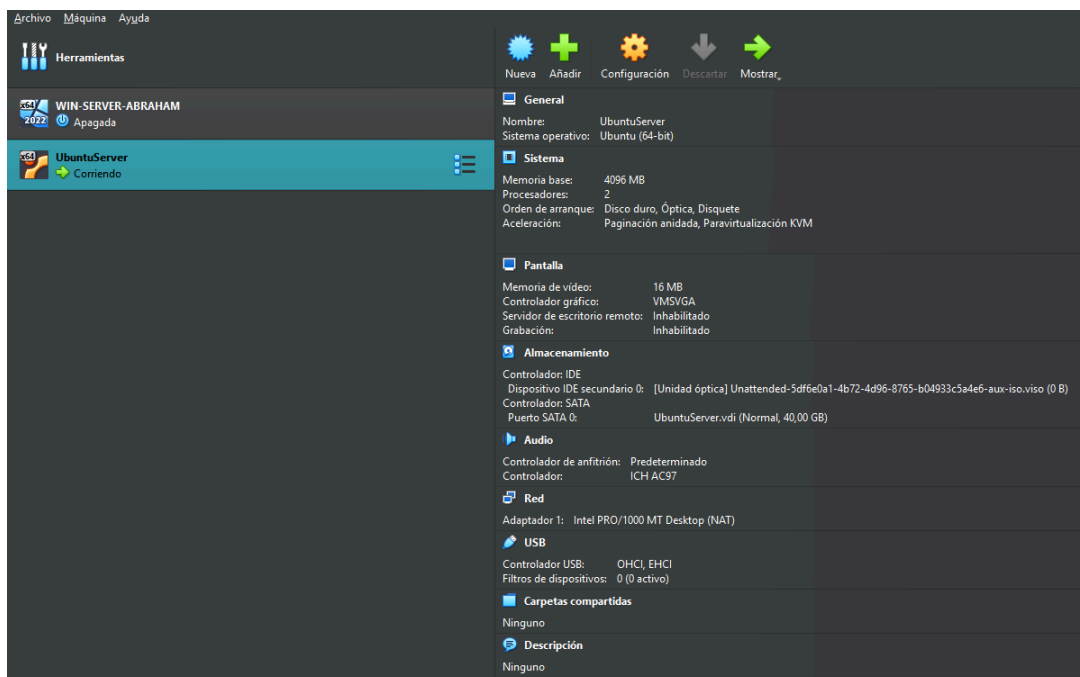
Reto Día 7: Despliegue y Preparación de un Servidor Linux para Producción



Abraham Caamaño Martínez



Fase 1: Instalación del Entorno de Pruebas



Fase 2: Configuración del Servidor



Configurar el sistema con un usuario administrador seguro:

El mismo Virtualbox crea un usuario administrador.

- ✓ Asignar una **IP estática** en la red local y probar conectividad con ping:

1. Editamos el archivo de configuración en **/etc/netplan/** de la siguiente manera con el comando:

sudo nano /etc/netplan/"nombre archivo de configuracion".yaml

```
network:
  version: 2
  ethernets:
    enp0s3:
      dhcp4: no
      addresses: [192.168.1.100/24]
      routes:
        - to: default
          via: 192.168.1.1
      nameservers:
        addresses:
          - 8.8.8.8
          - 8.8.4.4
```

2. Aplicamos con:
sudo netplan apply

3. Hacemos ping con:
ping google.com

```
Ubuntu 24.04.2 LTS UbuntuServer tty1
UbuntuServer login: vboxuser
Password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-60-generic x86_64)

* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/pro

System information as of Wed Jun 18 07:04:58 AM UTC 2025

System load:  0.0          Processes:            115
Usage of /:   6.5% of 39.07GB Users logged in:        0
Memory usage: 6%          IPv4 address for enp0s3: 192.168.1.100
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

vboxuser@UbuntuServer:~$ ping google.com
PING google.com (142.250.200.78) 56(84) bytes of data:
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=1 ttl=117 time=11.4 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=2 ttl=117 time=11.3 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=3 ttl=117 time=11.2 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=4 ttl=117 time=20.6 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=5 ttl=117 time=11.0 ms
64 bytes from mad07s24-in-f14.1e100.net (142.250.200.78): icmp_seq=6 ttl=117 time=10.9 ms
```

✓ Habilitar el acceso remoto mediante SSH y verificar conexión.

1. Instalar el servidor SSH con el comando:
sudo apt install openssh-server

```

Fetched 880 kB in 0s (2,391 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openssh-sftp-server.
(Reading database ... 83990 files and directories currently installed.)
Preparing to unpack .../openssh-sftp-server_1%3a9.6p1-3ubuntu13.12_amd64.deb ...
Unpacking openssh-sftp-server (1:9.6p1-3ubuntu13.12) ...
Selecting previously unselected package libwrap0:amd64.
Preparing to unpack .../libwrap0_7.6.q-33_amd64.deb ...
Unpacking libwrap0:amd64 (7.6.q-33) ...
Selecting previously unselected package openssh-server.
Preparing to unpack .../openssh-server_1%3a9.6p1-3ubuntu13.12_amd64.deb ...
Unpacking openssh-server (1:9.6p1-3ubuntu13.12) ...
Selecting previously unselected package ncurses-term.
Preparing to unpack .../ncurses-term_6.4+20240113-1ubuntu2_all.deb ...
Unpacking ncurses-term (6.4+20240113-1ubuntu2) ...
Selecting previously unselected package ssh-import-id.
Preparing to unpack .../ssh-import-id_5.11-0ubuntu2.24.04.1_all.deb ...
Unpacking ssh-import-id (5.11-0ubuntu2.24.04.1) ...
Setting up openssh-sftp-server (1:9.6p1-3ubuntu13.12) ...
Setting up ssh-import-id (5.11-0ubuntu2.24.04.1) ...
Setting up libwrap0:amd64 (7.6.q-33) ...
Setting up ncurses-term (6.4+20240113-1ubuntu2) ...
Setting up openssh-server (1:9.6p1-3ubuntu13.12) ...

Creating config file /etc/ssh/sshd_config with new version
Created symlink /etc/systemd/system/sockets.target.wants/ssh.socket → /usr/lib/systemd/system/ssh.socket.
Created symlink /etc/systemd/system/ssh.service.requires/ssh.socket → /usr/lib/systemd/system/ssh.socket.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Processing triggers for libc-bin (2.39-0ubuntu0.4) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
vboxuser@UbuntuServer:~$ sudo systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/usr/lib/systemd/system/ssh.service; disabled; preset: enabled)
   Active: inactive (dead)
   TriggeredBy: ● ssh.socket
     Docs: man:sshd(8)
           man:sshd_config(5)
vboxuser@UbuntuServer:~$

```

2. Ver si el servicio esta activo:
sudo systemctl status ssh

3. Nos conectamos con el comando:
ssh vboxuser@192.168.1.100

```
vboxuser@UbuntuServer:~$ ssh vboxuser@192.168.1.100
The authenticity of host '192.168.1.100 (192.168.1.100)' can't be established.
ED25519 key fingerprint is SHA256:hx4b3Bc4iPCWRugehfxUVTlYsKBJVvYizx1PGIkMLtY.
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
Warning: Permanently added '192.168.1.100' (ED25519) to the list of known hosts.
vboxuser@192.168.1.100's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Jun 18 07:14:33 AM UTC 2025

System load:  0.0               Processes:           113
Usage of /:   6.5% of 39.07GB   Users logged in:    1
Memory usage: 7%               IPv4 address for enp0s3: 192.168.1.100
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

vboxuser@UbuntuServer:~$ _
```



Fase 3: Gestión de usuarios y seguridad



Crear tres usuarios con diferentes permisos en el servidor.

1. Creamos los usuarios de la siguiente forma:

sudo adduser abraham

sudo adduser abraham2

sudo adduser abraham3

```
vboxuser@ubuntuServer:~$ sudo adduser abraham
[sudo] password for vboxuser:
info: Adding user 'abraham' ...
info: Selecting UID/GID from range 1000 to 5999 ...
info: Adding new group 'abraham' (1001) ...
info: Adding new user 'abraham' (1001) with group 'abraham (1001)' ...
info: Creating home directory '/home/abraham' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for abraham
Enter the new value, or press ENTER for the default
  Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user 'abraham' to supplemental / extra groups 'users' ...
info: Adding user 'abraham' to group 'users' ...
vboxuser@ubuntuServer:~$ sudo adduser abraham2
info: Adding user 'abraham2' ...
info: Selecting UID/GID from range 1000 to 5999 ...
info: Adding new group 'abraham2' (1002) ...
info: Adding new user 'abraham2' (1002) with group 'abraham2 (1002)' ...
info: Creating home directory '/home/abraham2' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for abraham2
Enter the new value, or press ENTER for the default
  Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user 'abraham2' to supplemental / extra groups 'users' ...
info: Adding user 'abraham2' to group 'users' ...
vboxuser@ubuntuServer:~$ _
```

```
Enter the new value, or press ENTER for the default
  Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user 'abraham2' to supplemental / extra groups 'users' ...
info: Adding user 'abraham2' to group 'users' ...
vboxuser@ubuntuServer:~$ sudo adduser abraham2
info: Adding user 'abraham2' ...
info: Selecting UID/GID from range 1000 to 5999 ...
info: Adding new group 'abraham2' (1002) ...
info: Adding new user 'abraham2' (1002) with group 'abraham2 (1002)' ...
info: Creating home directory '/home/abraham2' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for abraham2
Enter the new value, or press ENTER for the default
  Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user 'abraham2' to supplemental / extra groups 'users' ...
info: Adding user 'abraham2' to group 'users' ...
vboxuser@ubuntuServer:~$ sudo adduser abraham3
info: Adding user 'abraham3' ...
info: Selecting UID/GID from range 1000 to 5999 ...
info: Adding new group 'abraham3' (1003) ...
info: Adding new user 'abraham3' (1003) with group 'abraham3 (1003)' ...
info: Creating home directory '/home/abraham3' ...
info: Copying files from '/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for abraham3
Enter the new value, or press ENTER for the default
  Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user 'abraham3' to supplemental / extra groups 'users' ...
info: Adding user 'abraham3' to group 'users' ...
vboxuser@ubuntuServer:~$
```

 **Asignar permisos específicos a cada usuario y probar accesos.**

(Los permisos se explican en la segunda parte del reto)

Conectamos el usuario abraham2 por ejemplo con:

ssh abraham2@192.168.1.100

```
vboxuser@UbuntuServer:~$ ssh abraham2@192.168.1.100
abraham2@192.168.1.100's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

System information as of Wed Jun 18 07:18:59 AM UTC 2025

System load:  0.01               Processes:            119
Usage of /:   6.6% of 39.07GB    Users logged in:     1
Memory usage: 7%                IPv4 address for enp0s3: 192.168.1.100
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

abraham2@UbuntuServer:~$ _
```

✓ Configurar el firewall con UFW y permitir solo las conexiones necesarias.

1. Verificamos el estado del firewall con:

sudo ufw status

2. Denegamos todo el tráfico entrante y permitimos todo el saliente con:

sudo ufw default deny incoming
sudo ufw default allow outgoing

3. Permitimos el acceso SSH:

sudo ufw allow ssh (Permite el puerto 22)
sudo ufw allow http (Permite el puerto 80)
sudo ufw allow https (Permite el puerto 443)

4. Activamos el firewall:

sudo ufw enable

5. Verificamos las reglas que están activas:

sudo ufw status verbose

```
vboxuser@UbuntuServer:~$ sudo ufw status
[sudo] password for vboxuser:
Status: inactive
vboxuser@UbuntuServer:~$ sudo ufw default deny incoming
Default incoming policy changed to 'deny'
(be sure to update your rules accordingly)
vboxuser@UbuntuServer:~$ sudo ufw default allow outgoing
Default outgoing policy changed to 'allow'
(be sure to update your rules accordingly)
vboxuser@UbuntuServer:~$ sudo ufw allow ssh
Rules updated
Rules updated (v6)
vboxuser@UbuntuServer:~$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
vboxuser@UbuntuServer:~$ sudo ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

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

vboxuser@UbuntuServer:~$
```


Parte 2



Fase 1: Instalación del sistema base



- ✓ Verificar que el sistema arranque sin errores y actualiza sus paquetes (`apt update` & `apt upgrade`).

Actualizamos Ubuntu Server con:
sudo apt update && sudo apt upgrade -y

```
vboxuser@UbuntuServer:~$ sudo apt update
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://es.archive.ubuntu.com/ubuntu noble InRelease
Get:3 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease [126 kB]
Hit:4 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease
Fetched 126 kB in 1s (150 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1 package can be upgraded. Run 'apt list --upgradable' to see it.
vboxuser@UbuntuServer:~$ sudo apt upgrade
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Calculating upgrade... Done
The following upgrades have been deferred due to phasing:
  ubuntu-drivers-common
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
vboxuser@UbuntuServer:~$
```



Fase 2: Configuración de red y acceso remoto



- ✓ Configurar el archivo `/etc/hosts` correctamente con el nombre del servidor.

Edite el archivo `/etc/hosts` con:
sudo nano /etc/hosts

```
GNU nano 7.2
127.0.0.1 localhost
127.0.0.1 vrboxuser
192.168.1.100 vrboxuser
```

Añadimos la línea:
192.168.1.100 vrboxuser

✓ Instalar y habilitar el servicio SSH.

(Ya realizado antes)

✓ Verificar la conexión remota desde otro sistema con
ssh.

(Ya realizado antes)

Fase 3: Seguridad mínima obligatoria

✓ Configurar UFW

Permitiremos solo el tráfico por puerto 22 (SSH) y puerto 80 (HTTP):

sudo ufw allow 22/tcp

sudo ufw allow 80/tcp

```
vboxuser@UbuntuServer:~$ sudo ufw allow 22/tcp
Skipping adding existing rule
Skipping adding existing rule (v6)
vboxuser@UbuntuServer:~$ sudo ufw allow 80/tcp
Rule added
Rule added (v6)
vboxuser@UbuntuServer:~$ sudo ufw status
Status: active
```

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

```
vboxuser@UbuntuServer:~$ _
```

- ✓ **Crear un nuevo usuario llamado desarrollador, con acceso limitado y sin permisos de superusuario.**

Creamos el usuario:

sudo adduser desarrollador

```
vboxuser@UbuntuServer:~$ sudo adduser desarrollador
info: Adding user `desarrollador' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `desarrollador' (1004) ...
info: Adding new user `desarrollador' (1004) with group `desarrollador (1004)' ..
info: Creating home directory `/home/desarrollador' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for desarrollador
Enter the new value, or press ENTER for the default
    Full Name []:
    Room Number []:
    Work Phone []:
    Home Phone []:
    Other []:
Is the information correct? [Y/n] y
info: Adding new user `desarrollador' to supplemental / extra groups `users' ...
info: Adding user `desarrollador' to group `users' ...
vboxuser@UbuntuServer:~$ _
```

- 

sudo nano /etc/ssh/sshd_config

Quedaría algo así:

```
GNU nano 7.2 /etc/ssh/sshd_config *
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

Include /etc/ssh/sshd_config.d/*.conf

# When systemd socket activation is used (the default), the socket
# configuration must be re-generated after changing Port, AddressFamily, or
# ListenAddress.
#
# For changes to take effect, run:
#
#   systemctl daemon-reload
#   systemctl restart ssh.socket
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:
#AuthenticationMethods publickey
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

```
sudo ufw allow 2222/tcp
```

```
vboxuser@UbuntuServer:~$ sudo ufw allow 2222/tcp
Rule added
Rule added (v6)
vboxuser@UbuntuServer:~$
```

Reiniciamos con:

sudo systemctl restart sshd

Y probamos que funcione correctamente:

ssh "usuario"@192.168.1.100 -p 2222

```
vboxuser@UbuntuServer:~$ ssh vboxuser@192.168.1.100 -p 2222
ssh: connect to host 192.168.1.100 port 2222: Connection refused
vboxuser@UbuntuServer:~$ _
```



Fase 4: Estructura de carpetas y servicios iniciales



✓ Crear una estructura de carpetas en /srv/

Creamos los directorios con:

sudo mkdir -p /srv/www /srv/repositorios /srv/docs

```
vboxuser@UbuntuServer:~$ sudo mkdir -p /srv/www /srv/repositorios /srv/docs
```



✓ Establecer permisos específicos:

Vamos a dar acceso de escritura para “desarrollador” con:

sudo chown -R desarrollador /srv/www

sudo chmod -R 775 /srv/www

Y acceso exclusivo a nuestro usuario administrador con:

sudo chown -R vboxuser /srv/repositorios

sudo chmod -R 770 /srv/repositorios

```
vboxuser@UbuntuServer:~$ sudo chown -R desarrollador /srv/www
vboxuser@UbuntuServer:~$ sudo chmod -R 775 /srv/www
vboxuser@UbuntuServer:~$ sudo chown -R vboxuser /srv/www
vboxuser@UbuntuServer:~$ sudo chown -R vboxuser /srv/repositorios
vboxuser@UbuntuServer:~$ sudo chmod -R 770 /srv/repositorios
vboxuser@UbuntuServer:~$
```

 **Instalar el servidor web Apache2 o NGINX (a elegir) y colocar una página de prueba en /srv/www.**

Instalamos NGINX:

sudo apt install nginx -y

```
vboxuser@UbuntuServer:~$ sudo apt install nginx -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  nginx-common
Suggested packages:
  fcgiwrap nginx-doc ssl-cert
The following NEW packages will be installed:
  nginx nginx-common
0 upgraded, 2 newly installed, 0 to remove and 1 not upgraded.
Need to get 551 kB of archives.
After this operation, 1,596 kB of additional disk space will be used.
Get:1 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 nginx-common all 1.24.0-2ubuntu7.3 [31.2 kB]
Get:2 http://es.archive.ubuntu.com/ubuntu noble-updates/main amd64 nginx amd64 1.24.0-2ubuntu7.3 [520 kB]
Fetched 551 kB in 0s (1,682 kB/s)
Preconfiguring packages ...
Selecting previously unselected package nginx-common.
(Reading database ... 86905 files and directories currently installed.)
Preparing to unpack .../nginx-common_1.24.0-2ubuntu7.3_all.deb ...
Unpacking nginx-common (1.24.0-2ubuntu7.3) ...
Selecting previously unselected package nginx.
Preparing to unpack .../nginx_1.24.0-2ubuntu7.3_amd64.deb ...
Unpacking nginx (1.24.0-2ubuntu7.3) ...
Setting up nginx (1.24.0-2ubuntu7.3) ...
Setting up nginx-common (1.24.0-2ubuntu7.3) ...
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /usr/lib/systemd/system/nginx.service.
Processing triggers for ufw (0.36.2-6) ...
Processing triggers for man-db (2.12.0-4build2) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
vboxuser@UbuntuServer:~$
```

Editamos el archivo de configuración de NGINX

sudo nano /etc/nginx/sites-available/default

y cambiamos la linea que dice “root /var/www/html;” borrando solo “html”

```
GNU nano 7.2 /etc/nginx/sites-available/default *
##
# You should look at the following URL's in order to grasp a solid understanding
# of Nginx configuration files in order to fully unleash the power of Nginx.
# https://www.nginx.com/resources/wiki/start/
# https://www.nginx.com/resources/wiki/start/topics/tutorials/config_pitfalls/
# https://wiki.debian.org/Nginx/DirectoryStructure
#
# In most cases, administrators will remove this file from sites-enabled/ and
# leave it as reference inside of sites-available where it will continue to be
# updated by the nginx packaging team.
#
# This file will automatically load configuration files provided by other
# applications, such as Drupal or Wordpress. These applications will be made
# available underneath a path with that package name, such as /drupal8.
#
# Please see /usr/share/doc/nginx-doc/examples/ for more detailed examples.
##

# Default server configuration
#
server {
    listen 80 default_server;
    listen [::]:80 default_server;

    # SSL configuration
    #
    # listen 443 ssl default_server;
    # listen [::]:443 ssl default_server;
    #
    # Note: You should disable gzip for SSL traffic.
    # See: https://bugs.debian.org/773332
    #
    # Read up on ssl_ciphers to ensure a secure configuration.
    # See: https://bugs.debian.org/765782
    #
    # Self signed certs generated by the ssl-cert package
    # Don't use them in a production server!
    #
    # include snippets/snakeoil.conf;

    root /srv/www;

    # Add index.php to the list if you are using PHP
    index index.html index.htm index.nginx-debian.html;

    server_name _;
}
```

Verificamos que este todo correcto y reiniciamos NGINX con estos comandos:

sudo nginx -t

sudo systemctl restart nginx

```
vboxuser@UbuntuServer:~$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
vboxuser@UbuntuServer:~$ sudo systemctl restart nginx
vboxuser@UbuntuServer:~$
```

Ahora crearemos un archivo index.html con:

sudo tee /srv/www/index.html

```
vboxuser@UbuntuServer:~$ sudo nginx -t
nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
nginx: configuration file /etc/nginx/nginx.conf test is successful
vboxuser@UbuntuServer:~$ sudo systemctl restart nginx
vboxuser@UbuntuServer:~$ sudo tee /srv/www/index.html
```

El comando “tee” es para escribir en una ubicación protegida.

Para comprobar que funciona correctamente, vamos a un navegador web, en mi caso el de mi máquina local, y al escribir la dirección IP del servidor nos debería de aparecer la pagina de prueba.

