



1) PASO	
Creación de la maquina virtual. Nombre de usuario y contraseña. Puertos permitidos 80,443,22.	Tipo de seguridad ⓘ Máquinas virtuales de inicio seguro Configurar características de seguridad
	Imagen * ⓘ Ubuntu Server 24.04 LTS - x64 gen. 2 Ver todas las imágenes Configurar la generación de máquinas virtuales
	Arquitectura de VM ⓘ <input type="radio"/> Arm64 <input checked="" type="radio"/> x64
	Ejecución de Azure Spot con descuento ⓘ <input type="checkbox"/>
	Tamaño * ⓘ Standard_B1s - 1 vcpu, 1 GiB de memoria (7,59 US\$/mes) (servicios gratuito... Ver todos los tamaños
	Habilitar hibernación ⓘ <input type="checkbox"/> i Actualmente, Hibernar no admite el inicio de confianza y las máquinas virtuales confidenciales para imágenes de Linux. Más información ⓘ
	Cuenta de administrador
	Tipo de autenticación ⓘ <input type="radio"/> Clave pública SSH <input checked="" type="radio"/> Contraseña
	Nombre de usuario * ⓘ administrador ✓
	Contraseña * ✓
Confirmar contraseña * ✓	
Reglas de puerto de entrada Seleccione los puertos de red de máquina virtual que son accesibles desde la red Internet pública. Puede especificar acceso de red más limitado o granular en la pestaña Red.	
Puertos de entrada públicos * ⓘ <input type="radio"/> Ninguno <input checked="" type="radio"/> Permitir los puertos seleccionados	
Seleccionar puertos de entrada * HTTP (80), HTTPS (443), SSH (22) ✓	
	⚠ Esto permitirá que todas las direcciones IP accedan a la máquina virtual. Esto solo se recomienda para las pruebas. Use los controles avanzados de la pestaña Redes a fin de crear reglas para limitar el tráfico entrante a las direcciones IP conocidas.

2) PASO	
----------------	--



Red de la máquina virtual.

Crear una máquina virtual ...



Ayuda para crear una máquina virtual de bajo coste

Ayuda para crear una VM optimizada para alta disponibilidad

Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo

Datos básicos

Discos

Redes

Administración

Supervisión

Opciones avanzadas

Etiquetas

Revisar y crear

Configure la tarjeta de interfaz de red (NIC) a fin de definir la conectividad de red para la máquina virtual. Puede controlar los puertos y la conectividad entrante y saliente con reglas de grupos de seguridad o bien aplicar una solución de equilibrio de carga ya existente. [Más información](#)

Interfaz de red

Al crear una máquina virtual, se crea una interfaz de red automáticamente.

Red virtual * ⓘ

(nuevo) samuelmv76-45-vnet

[Crear nuevo](#)

Subred * ⓘ

(nuevo) default (10.1.0.0/24)

IP pública ⓘ

(nuevo) samuelmv76-45-ip

[Crear nuevo](#)

Grupo de seguridad de red de NIC ⓘ

☐ Ninguno

☒ Básico

☐ Opciones avanzadas

Puertos de entrada públicos * ⓘ

☐ Ninguno

☒ Permitir los puertos seleccionados

Seleccionar puertos de entrada *

HTTP (80), HTTPS (443), SSH (22)



Esto permitirá que todas las direcciones IP accedan a la máquina virtual.
Esto solo se recomienda para las pruebas. Use los controles avanzados de la pestaña Redes a fin de crear reglas para limitar el tráfico entrante a las direcciones IP conocidas.

3) PASO



Disco del SO de la maquina virtual.

Crear una máquina virtual



Ayuda para crear una máquina virtual de bajo coste

Ayuda para crear una VM optimizada para alta disponibilidad

Ayudarme a elegir el tamaño de VM adecuado para mi carga de trabajo

Datos básicos **Discos** Redes Administración Supervisión Opciones avanzadas Etiquetas Revisar y crear

Las máquinas virtuales de Azure tienen un disco de sistema operativo y un disco temporal para el almacenamiento a corto plazo. Puede asociar discos de datos adicionales. El tamaño de la máquina virtual determina el tipo de almacenamiento que puede usar y la cantidad de datos que permiten los discos. [Más información](#)

Cifrado del disco de la máquina virtual

El cifrado de Azure Disk Storage cifra automáticamente los datos almacenados en los discos administrados de Azure en reposo (discos de datos y del sistema operativo) de forma predeterminada al guardarlos en la nube.

Cifrado en el host

☐

El cifrado en el host no está registrado para la suscripción seleccionada. [Más información](#)

Disco del SO

Tamaño del disco del SO

Valor predeterminado de la imagen (30 GiB)

Tipo de disco del sistema operativo *

SSD Premium (almacenamiento con redundancia local)

Eliminar con VM

☒

Administración de claves

Clave administrada por la plataforma

Habilitar compatibilidad con Ultra Disks

☐

Discos de datos para samuelmv76-45

Puede agregar y configurar discos de datos adicionales para su máquina virtual o asociar discos existentes. Esta máquina virtual también incluye un disco temporal.

4) PASO

Conexión a la maquina mediante putty.

PuTTY Configuration

Category: Session, Logging, Terminal, Keyboard, Bell, Features, Window, Appearance, Behaviour, Translation, Selection, Colours, Connection, Data, Proxy, SSH, Serial, Telnet, Rlogin, SUPDUP

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address) 20.75.55.176 Port 22

Connection type: SSH, Serial, Other: Telnet

Load, save or delete a stored session

Saved Sessions: 20.75.55.176(Lamp), Default Settings, 20.75.55.176(Lamp)

Close window on exit: Always, Never, Only on clean exit

About, Help, Open, Cancel

ativo : Linux (ubuntu 24.04)
ública : Standard B1s (1 vcpu, 1 GiB de memoria)
ública : 20.75.55.176
bred : samuelmv76-45-vnet/default
Sin configurar
ntenimiento : -
ción : 30/1/2025, 7:35 UTC
on IP pública : 20.75.55.176 (Interfaz de red samuelmv76-45314_z1)
on IP pública (IPv6) : -
on IP privada : 10.1.0.4



```
administrador@samuelmv76-45: ~  
login as: administrador  
administrador@20.75.55.176's password:  
Access denied  
administrador@20.75.55.176's password:  
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-1020-azure x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:        https://ubuntu.com/pro
```

5) PASO	
Comando sudo su para entrar como root a la máquina.	<pre>root@samuelmv76-45: /home/administrador administrador@samuelmv76-45:~\$ sudo su root@samuelmv76-45:/home/administrador#</pre>

6) PASO	
Comando para entrar a /etc/ssh	<pre>root@samuelmv76-45:/home/administrador# cd /etc root@samuelmv76-45:/etc# cd ssh root@samuelmv76-45:/etc/ssh#</pre>

7) PASO	
Comando para editar el archivo sshd_config.	<pre>root@samuelmv76-45:/etc/ssh# ls moduli ssh_host_ecdsa_key ssh_host_ed25519_key.pub ssh_import_id ssh_config ssh_host_ecdsa_key.pub ssh_host_rsa_key sshd_config ssh_config.d ssh_host_ed25519_key ssh_host_rsa_key.pub sshd_config.d root@samuelmv76-45:/etc/ssh# sudo nano sshd_config root@samuelmv76-45:/etc/ssh#</pre>

8) PASO	
Cambios en el archivo sshd_config. - Descomentamos la línea PermitRootLogin y en vez de prohibit-password en su lugar ponemos yes	



- Descomentamos la línea StrictModes yes
- Asegurarnos que la línea PasswordAuthentication está descomentada y ponga yes

```
root@samuelmv76-45: /etc/ssh
GNU nano 7.2 sshd_config
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2

root@samuelmv76-45: /etc/ssh
GNU nano 7.2 sshd_config *
# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in fu
#AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys

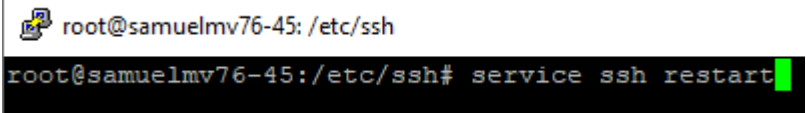
root@samuelmv76-45: /etc/ssh
GNU nano 7.2 sshd_config *
#AuthorizedKeysCommandUser nobody

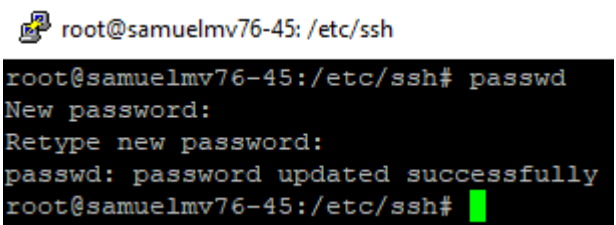
# For this to work you will also need host keys in /etc/ssh/s
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

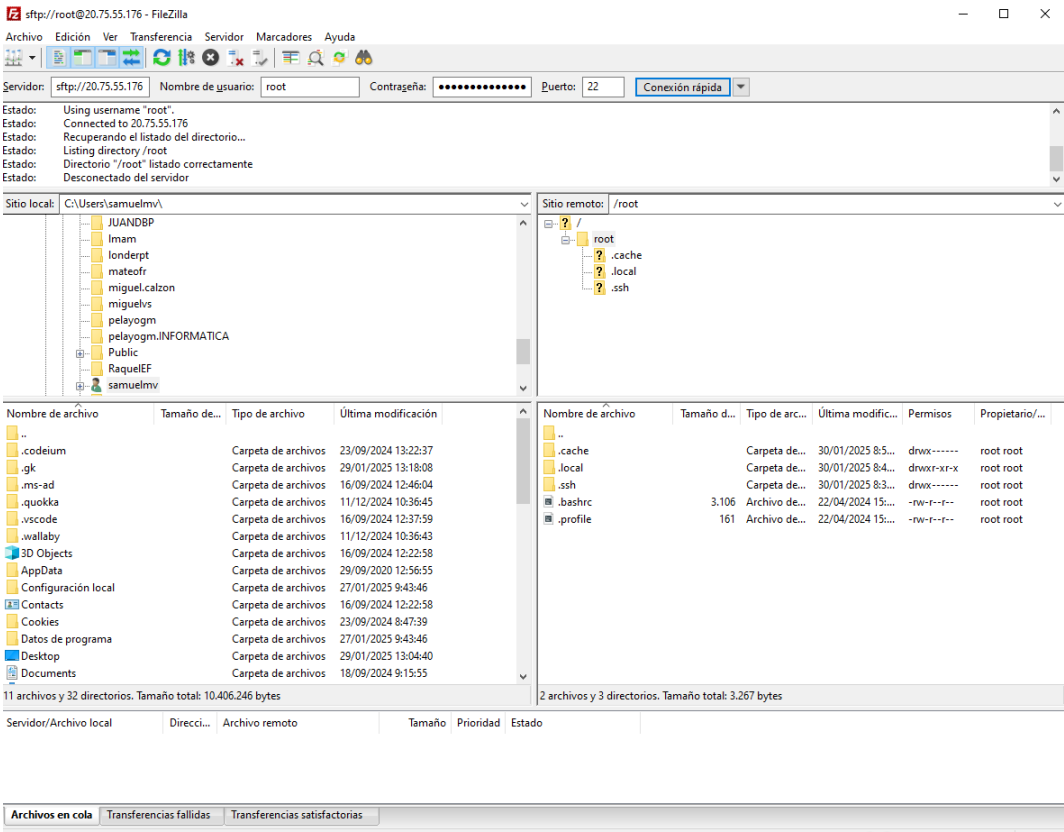
# To disable tunneled clear text passwords, change to no here
PasswordAuthentication yes
#PermitEmptyPasswords no
```



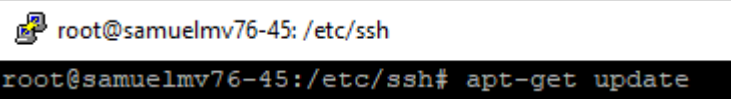
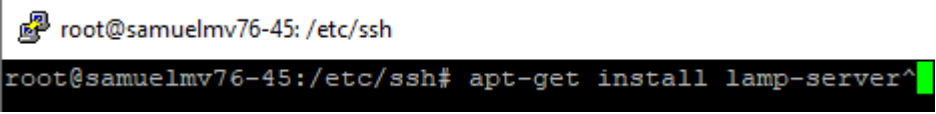

--	--

9) PASO	
Reiniciamos el servicio ssh con el comando service ssh restart.	

10) PASO	
Ponemos contraseña al usuario root con el comando passwd.	

11) PASO	
Conexión a la maquina mediante filezilla.	



12) PASO Actualizamos la maquina con apt-get update	 <pre>root@samuelmv76-45: /etc/ssh root@samuelmv76-45:/etc/ssh# apt-get update</pre>
13) PASO Instalamos el servidor lamp mediante el comando apt-get install lamp-server^	 <pre>root@samuelmv76-45: /etc/ssh root@samuelmv76-45:/etc/ssh# apt-get install lamp-server^</pre>
14) PASO Comprobamos que funciona accediendo a la maquina mediante el navegador y el puerto correcto.	 <p>The screenshot shows a web browser window with the address bar displaying '20.75.55.176:80'. The page title is 'Apache2 Default Page' and it features the Ubuntu logo. A message states 'It works!' and explains that this is the default welcome page used to test the correct operation of the Apache2 server. It also provides a 'Configuration Overview' section with details about the configuration files and their locations.</p>
15) PASO Ejecutamos en el putty el comando mysql show databases para comprobar que funciona.	



```
root@samuelmv76-45: /etc/ssh

root@samuelmv76-45:/etc/ssh# mysql show databases
mysql Ver 8.0.40-0ubuntu0.24.04.1 for Linux on x86_64 ((Ubuntu))
Copyright (c) 2000, 2024, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Usage: mysql [OPTIONS] [database]
  -?, --help          Display this help and exit.
  -I, --help          Synonym for -?
  --auto-rehash       Enable automatic rehashing. One doesn't need to use
                      'rehash' to get table and field completion, but startup
                      and reconnecting may take a longer time. Disable with
                      --disable-auto-rehash.
                      (Defaults to on; use --skip-auto-rehash to disable.)
  -A, --no-auto-rehash
                      No automatic rehashing. One has to use 'rehash' to get
                      table and field completion. This gives a quicker start of
                      mysql and disables rehashing on reconnect.
  --auto-vertical-output
                      Automatically switch to vertical output mode if the
                      result is wider than the terminal width.
  -B, --batch          Don't use history file. Disable interactive behavior.
```

16) PASO

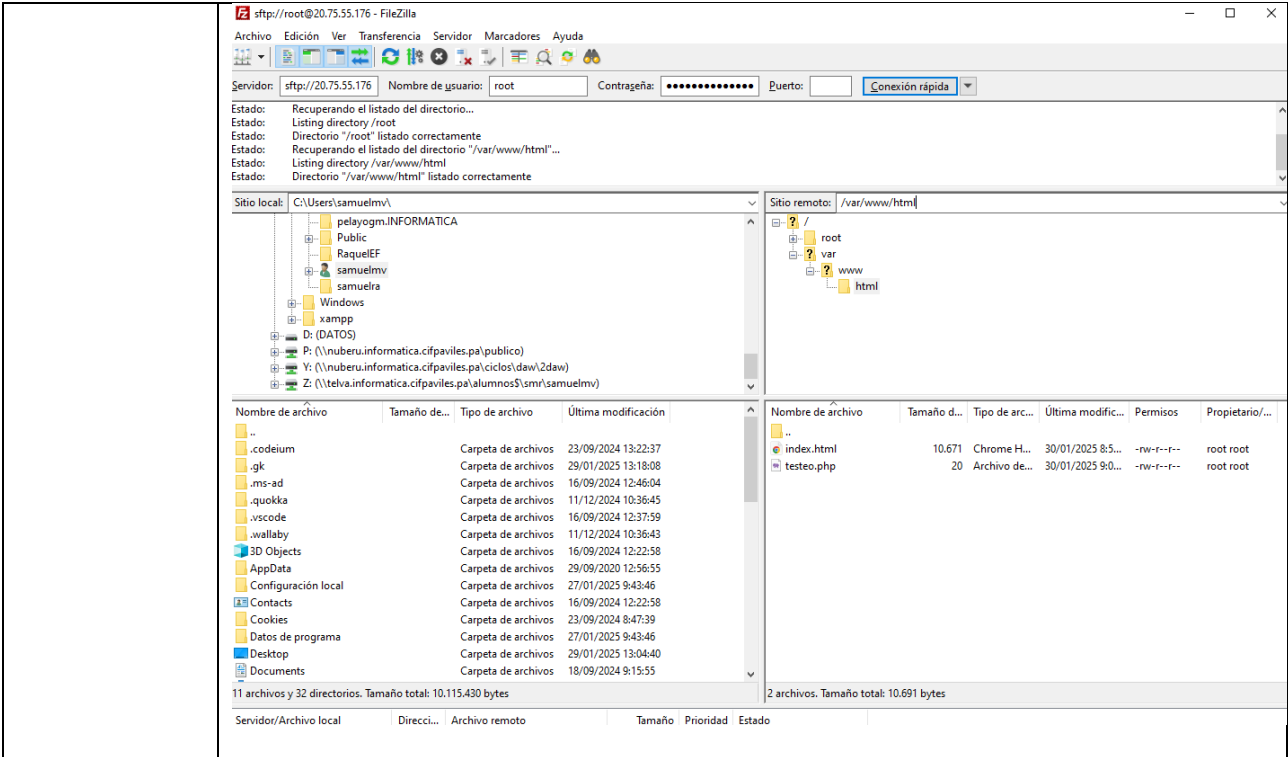
En la carpeta /var/www/html

- Creamos un fichero .php poner como nombre tu nombre de usuario y puesto
- Editamos remotamente el fichero creado y creamos un pequeño script que muestre las variables de entorno que tiene en esos momentos php.

```
root@samuelmv76-45: /var/www/html

root@samuelmv76-45:/etc/ssh# cd /var/www/html
root@samuelmv76-45:/var/www/html# ls
index.html
root@samuelmv76-45:/var/www/html# nano testeo.php
root@samuelmv76-45:/var/www/html#
```

```
GNU nano 7.2 testeo.php
?php
phpinfo();
?>
```

17) PASO

Desde el navegador llamamos al fichero creado .php y comprobamos que el php Funciona.

