# Initial Server Setup with Ubuntu 22.04

## Introducción

Cuando crea por primera vez un nuevo servidor Ubuntu 22.04, debe realizar algunos pasos de configuración importantes como parte de la configuración inicial. Estos pasos aumentarán la seguridad y la facilidad de uso de su servidor y le brindarán una base sólida para acciones posteriores.

## Paso 1: iniciar sesión como root

Para iniciar sesión en su servidor, necesitará conocer la dirección IP pública de su servidor. También necesitará la contraseña o la clave privada para la cuenta del usuario root si instaló una clave SSH para la autenticación. Si aún no ha iniciado sesión en su servidor.

Si no está conectado a su servidor actualmente, inicie sesión como usuario raíz usando el siguiente comando. Sustituya la parte resaltada de your\_server\_ip del comando con la dirección IP pública de su servidor:

$ ssh root@your\_server\_ip

Si la conexión es rechazada, instale SSH con el comando:

$ sudo apt install ssh

Vuelva a intentar la conexión. El puerto usado para ssh es el puerto 22. Deberemos habilitar el firewall para poder acceder a ese puerto en caso de querer acceder remotamente.

$ sudo ufw allow ssh

Si el firewall no está activo lo habilitamos:

$ sudo ufw enable

Volvemos a intentar la conexión ssh al servidor.

Acepte la advertencia sobre la autenticidad del host si aparece. Si su servidor usa autenticación de contraseña, proporcione su contraseña raíz para iniciar sesión. Si usa una clave SSH que está protegida con una frase de contraseña, es posible que deba ingresar la frase de contraseña la primera vez que use la clave en cada sesión. Si es la primera vez que inicia sesión en el servidor con una contraseña, es posible que también deba cambiar la contraseña de root. Siga las instrucciones para cambiar la contraseña si recibe un aviso.

#### Acerca de root

El usuario raíz es el usuario administrativo en un entorno Linux con privilegios elevados. Debido a los mayores privilegios de la cuenta raíz, se desaconseja que la use regularmente. La cuenta raíz puede realizar cambios muy destructivos, incluso por accidente.

El siguiente paso es configurar una nueva cuenta de usuario con privilegios reducidos para el uso diario.

## Step 2 — Creando un nuevo usuario

Una vez que inicie sesión como raíz, podrá agregar la nueva cuenta de usuario. En el futuro, iniciaremos sesión con esta nueva cuenta en lugar de root.

Este ejemplo crea un nuevo usuario llamado alumno, pero debe reemplazarlo con un nombre de usuario que le guste:

# adduser alumno

Se le harán algunas preguntas, comenzando con la contraseña de la cuenta.

Ingrese una contraseña segura y, opcionalmente, complete cualquier información adicional si lo desea. Esta información no es obligatoria y puede presionar ENTER en cualquier campo que desee omitir.

## Step 3 — Concediendo privilegios administrativos

Ahora tiene una nueva cuenta de usuario con privilegios de cuenta normales. Sin embargo, a veces necesitará realizar tareas administrativas como usuario root.

Para evitar cerrar la sesión de su usuario habitual y volver a iniciar sesión como cuenta raíz, puede configurar lo que se conoce como privilegios de superusuario o raíz para la cuenta habitual de su usuario. Estos privilegios le permitirán a su usuario normal ejecutar comandos con privilegios administrativos poniendo la palabra sudo antes del comando.

Para agregar estos privilegios a su nuevo usuario, deberá agregar el usuario al grupo del sistema sudo. De forma predeterminada en Ubuntu 22.04, los usuarios que son miembros del grupo sudo pueden usar el comando sudo.

Como root, ejecute este comando para agregar su nuevo usuario al grupo sudo (sustituya el nombre de usuario destacado de alumno con su nuevo usuario):

usermod -aG sudo alumno

Ahora puede escribir sudo antes de los comandos para ejecutarlos con privilegios de superusuario cuando inicie sesión como su usuario habitual.

## Step 4 — Configurando el firewall

Los servidores Ubuntu 22.04 pueden usar el firewall de netfilter y sus aplicaciones iptables o UFW para garantizar que solo se permitan conexiones a ciertos servicios. Puede configurar un cortafuegos básico utilizando esta aplicación.

Las aplicaciones pueden registrar sus perfiles con UFW al momento de la instalación. Estos perfiles permiten que UFW administre estas aplicaciones por nombre. OpenSSH, el servicio que le permite conectarse a su servidor, tiene un perfil registrado en UFW.

Puede examinar la lista de perfiles UFW instalados escribiendo:

ufw app list

Output

Available applications:

OpenSSH

Deberá asegurarse de que el firewall permita conexiones SSH para que pueda iniciar sesión en su servidor la próxima vez. Permita estas conexiones escribiendo

ufw allow OpenSSH

Ahora habilite el firewall escribiendo la orden:

ufw enable

Escriba y y presione ENTER para continuar. Puede ver que las conexiones SSH todavía están permitidas escribiendo:

ufw status

Output

Status: active

To Action From

-- ------ ----

OpenSSH ALLOW Anywhere

OpenSSH (v6) ALLOW Anywhere (v6)

## El cortafuegos actualmente está bloqueando todas las conexiones excepto SSH.

## Step 5 — Enabling External Access for Your Regular User

Ahora que tiene un usuario regular para el uso diario, deberá asegurarse de que puede acceder directamente a la cuenta mediante SSH.

Nota: hasta que verifique que puede iniciar sesión y usar sudo con su nuevo usuario, le recomendamos que permanezca conectado como root. Si tiene problemas para conectarse, puede solucionarlos y realizar los cambios necesarios como root. Si usa un Droplet de DigitalOcean y experimenta problemas con su conexión SSH raíz, puede recuperar el acceso a los Droplets usando la Consola de recuperación.

La configuración del acceso SSH para su nuevo usuario depende de si la cuenta raíz de su servidor usa una contraseña o claves SSH para la autenticación.

Si la cuenta raíz usa autenticación de contraseña

Si inició sesión en su cuenta raíz con una contraseña, la autenticación de contraseña está habilitada para SSH. Puede usar SSH en su nueva cuenta de usuario abriendo una nueva sesión de terminal y usando SSH con su nuevo nombre de usuario:

ssh alumno@your\_server\_ip

Después de ingresar su contraseña de usuario habitual, iniciará sesión. Recuerde, si necesita ejecutar un comando con privilegios administrativos, escriba sudo antes de este:

sudo command\_to\_run

Recibirá una solicitud de su contraseña de usuario normal cuando use sudo por primera vez en cada sesión (y periódicamente después).