

Integrantes:

1. Manuel Aicart
2. Arciel Navarro

Sección 1: PC Servidor.

Paso 1: Creación de un Nuevo Usuario

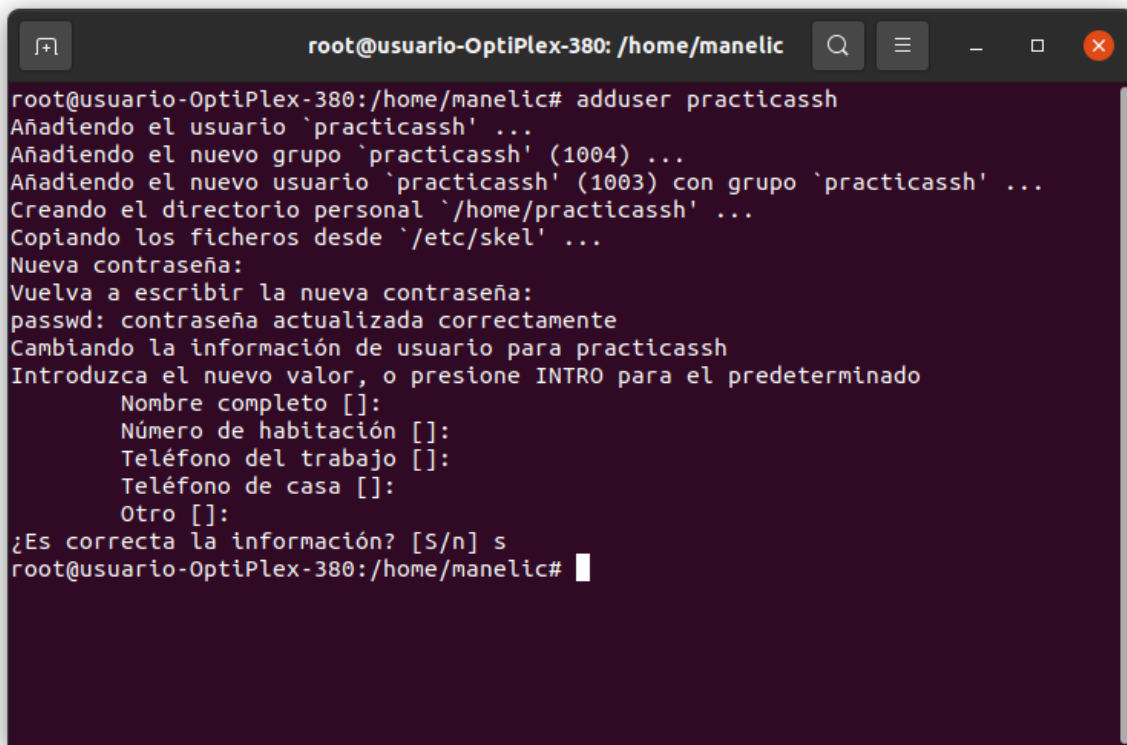
Objetivo: El primer paso en la configuración del servidor PC es crear un nuevo usuario que administrará las sesiones SSH y manejará los servicios correspondientes.

Procedimiento:

1. **Abrir la Terminal:** Iniciar una sesión como superusuario para tener los privilegios necesarios para añadir un nuevo usuario al sistema.
2. **Crear Nuevo Usuario:** Utilizar el comando `adduser` seguido del nombre de usuario deseado para iniciar el proceso de creación de un nuevo usuario. En este caso, el comando utilizado es:
 - `adduser practicassh`
3. **Asignar Contraseña:** Se solicitará establecer una contraseña para el nuevo usuario. Es importante elegir una contraseña segura que cumpla con las políticas de seguridad establecidas.
4. **Completar Información Adicional:** El sistema puede solicitar información adicional como el nombre completo, número de habitación, etc. Esta información es opcional y se puede dejar en blanco presionando ENTER para aceptar los valores predeterminados.

Resultado: Se ha creado con éxito un nuevo usuario llamado `practicassh`, con su propio grupo y directorio personal. La terminal muestra mensajes que confirman la creación del usuario y la asignación de la contraseña.

Captura de Pantalla:



```
root@usuario-OptiPlex-380: /home/manelic
root@usuario-OptiPlex-380:/home/manelic# adduser practicassh
Añadiendo el usuario 'practicassh' ...
Añadiendo el nuevo grupo 'practicassh' (1004) ...
Añadiendo el nuevo usuario 'practicassh' (1003) con grupo 'practicassh' ...
Creando el directorio personal '/home/practicassh' ...
Copiando los ficheros desde '/etc/skel' ...
Nueva contraseña:
Vuelva a escribir la nueva contraseña:
passwd: contraseña actualizada correctamente
Cambiando la información de usuario para practicassh
Introduzca el nuevo valor, o presione INTRO para el predeterminado
    Nombre completo []:
    Número de habitación []:
    Teléfono del trabajo []:
    Teléfono de casa []:
    Otro []:
¿Es correcta la información? [S/n] s
root@usuario-OptiPlex-380:/home/manelic#
```

Nota: La captura de pantalla proporcionada valida que los pasos se realizaron correctamente y que el usuario practicassh está listo para ser utilizado en las operaciones subsiguientes del servidor SSH.

Paso 2: Otorgar Permisos al Usuario Creado

Objetivo: Después de crear un nuevo usuario, el siguiente paso es asegurarse de que tenga los permisos necesarios para realizar tareas administrativas. Esto se hace añadiendo al usuario al grupo sudo, que le permitirá ejecutar comandos con privilegios de superusuario.

Procedimiento:

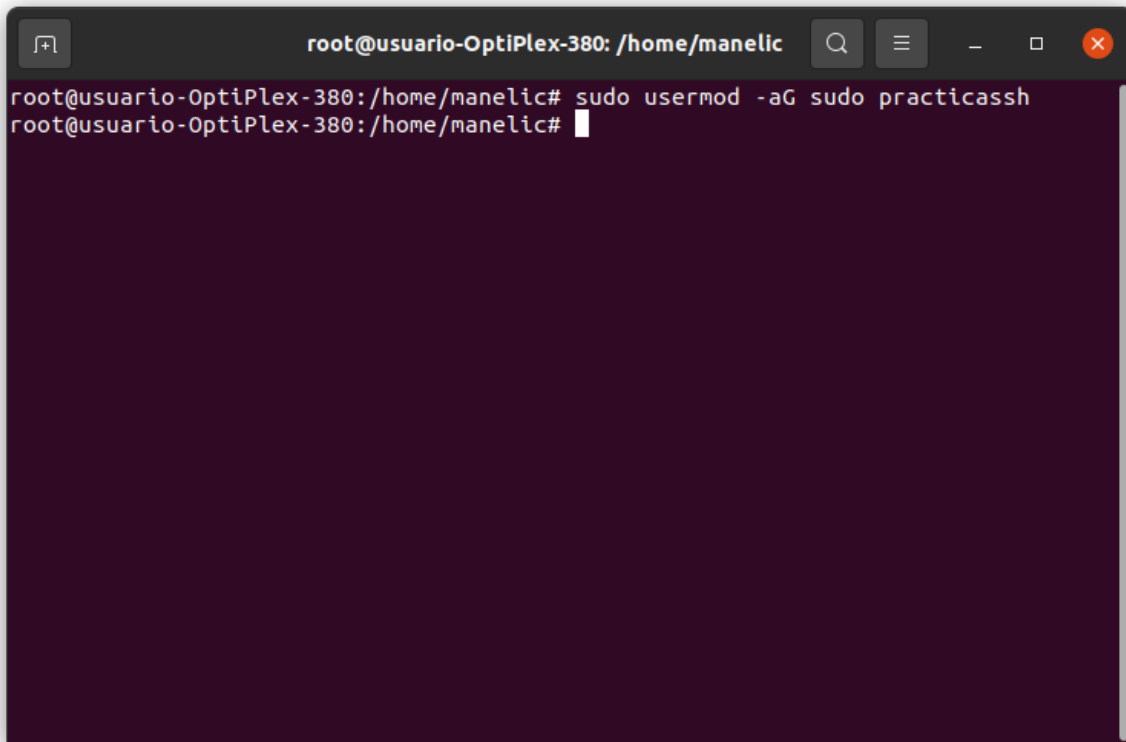
1. **Abrir la Terminal:** Mantén la sesión como superusuario o utiliza sudo para ejecutar comandos con privilegios elevados.
2. **Modificar Usuario:** Utilizar el comando usermod para añadir al usuario al grupo sudo. El comando específico es:
 - **usermod -aG sudo practicassh**

Aquí, -aG es una opción del comando usermod que permite añadir el usuario a un grupo suplementario, en este caso, sudo.

3. **Confirmación:** No hay una confirmación explícita en la terminal después de ejecutar este comando, pero la ausencia de mensajes de error indica que el comando se ha ejecutado con éxito.

Resultado: El usuario practicassh ahora tiene permisos para ejecutar comandos como superusuario cuando sea necesario, lo que es esencial para la administración del servidor y la instalación de software.

Captura de Pantalla:



```
root@usuario-OptiPlex-380: /home/manelic
root@usuario-OptiPlex-380:/home/manelic# sudo usermod -aG sudo practicassh
root@usuario-OptiPlex-380:/home/manelic#
```

Nota: Es una buena práctica verificar que el usuario ha sido añadido al grupo sudo correctamente. Esto se puede hacer con el comando `groups practicassh`, que listará todos los grupos a los que pertenece el usuario.

Paso 3: Identificar la IP del Servidor

Objetivo: El propósito de este paso es identificar la dirección IP del servidor, que es necesaria para establecer una conexión SSH desde el cliente, así como para configurar los servicios de red como Apache y VirtualHost más adelante.

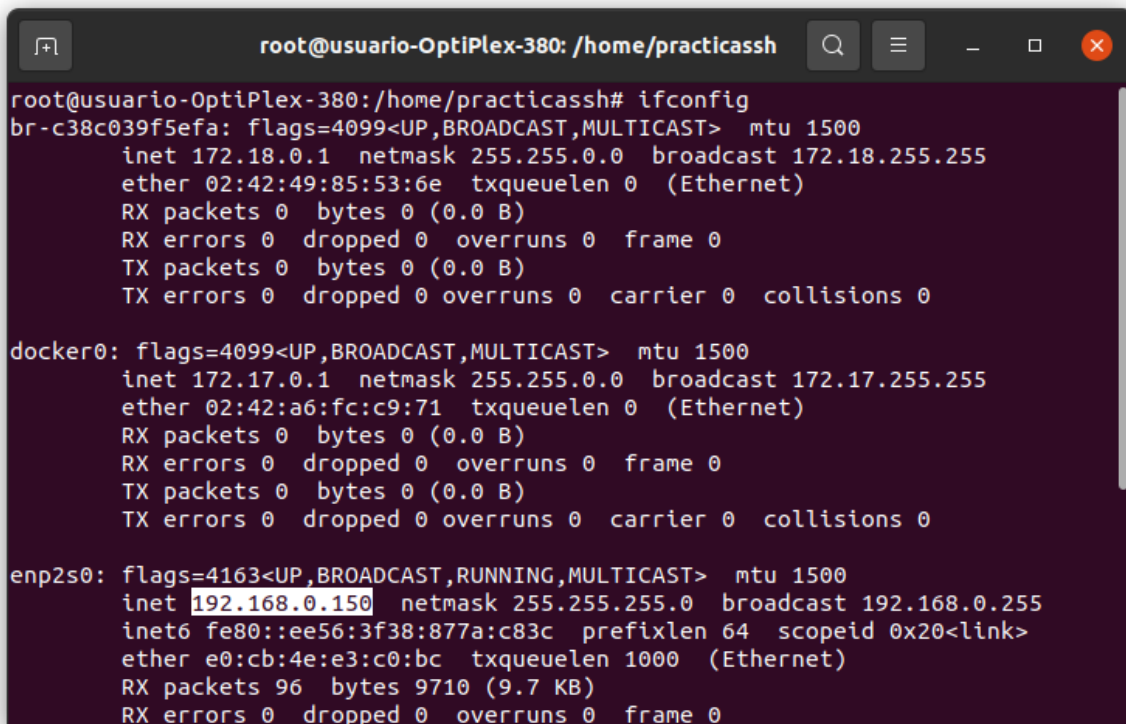
Procedimiento:

1. **Abrir la Terminal:** Continuar en la sesión de superusuario para tener acceso completo a los comandos de red.

2. **Ejecutar ifconfig:** Utilizar el comando ifconfig para listar todas las interfaces de red y sus respectivas configuraciones IP. El comando utilizado es:
 - **ifconfig**
3. **Encontrar la Dirección IP:** En la salida del comando, buscar la sección que corresponde a la interfaz de red conectada a la red local o internet (normalmente llamada eth0, ens33, enp0s3, etc.). En este caso, la interfaz relevante es **enp2s0**.
4. **Registrar la Dirección IP:** La dirección IP del servidor está listada después de inet. Es la dirección IP con la que los otros dispositivos de la red pueden comunicarse con el servidor. En este ejemplo, la dirección IP es **192.168.0.150**

Resultado: Ahora se conoce la dirección IP del servidor (192.168.0.150), que se usará para establecer la conexión SSH y configurar los servicios de red.

Captura de Pantalla:



```
root@usuario-OptiPlex-380: /home/practicassh# ifconfig
br-c38c039f5efa: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.18.0.1 netmask 255.255.0.0 broadcast 172.18.255.255
    ether 02:42:49:85:53:6e txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:a6:fc:c9:71 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp2s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.150 netmask 255.255.255.0 broadcast 192.168.0.255
    inet6 fe80::ee56:3f38:877a:c83c prefixlen 64 scopeid 0x20<link>
    ether e0:cb:4e:e3:c0:bc txqueuelen 1000 (Ethernet)
    RX packets 96 bytes 9710 (9.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
```

Nota: Es importante asegurarse de que la dirección IP del servidor sea estática o tenga una reserva DHCP para evitar que cambie con el tiempo, lo cual podría interrumpir la conectividad y los servicios que dependen de esta dirección.

Paso 4: Actualización de los Paquetes del Sistema

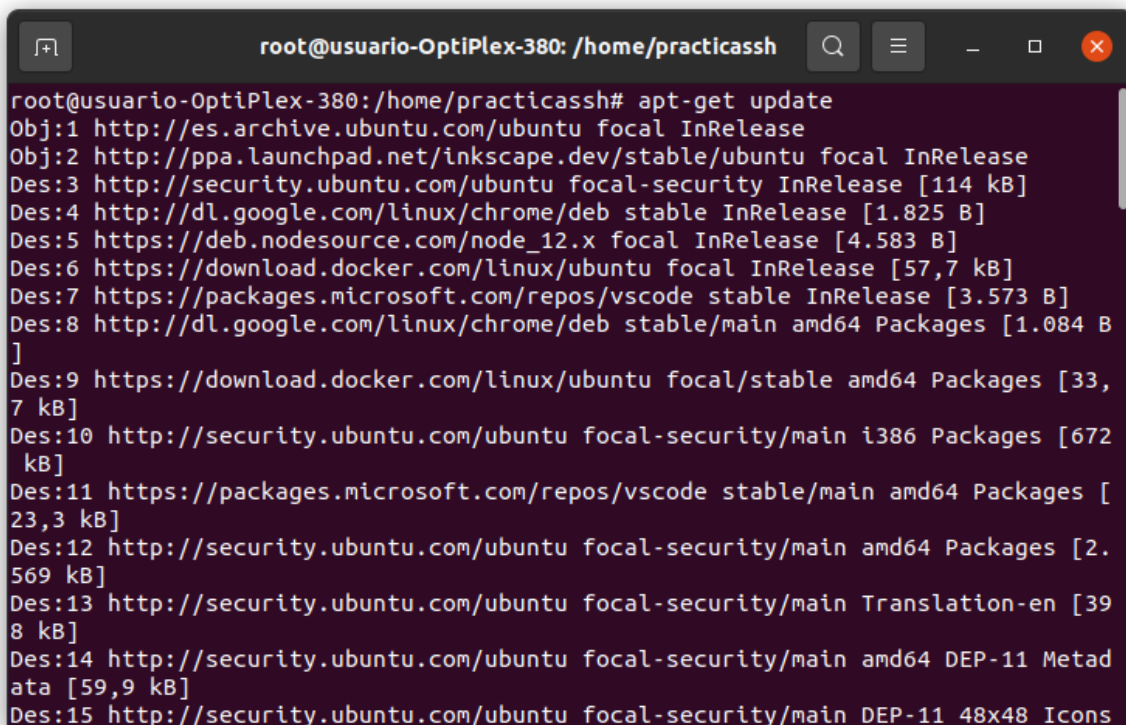
Objetivo: Antes de activar el servidor SSH y realizar otras configuraciones en el servidor, es esencial asegurarse de que todos los paquetes del sistema estén actualizados para tener las últimas versiones y parches de seguridad.

Procedimiento:

1. **Actualizar Lista de Paquetes:** Utilizar el comando `apt-get update` para actualizar la lista de paquetes disponibles y sus versiones. Esto no actualiza los paquetes en sí, sino que sincroniza la base de datos de paquetes con las fuentes configuradas en el archivo `/etc/apt/sources.list` y los archivos bajo `/etc/apt/sources.list.d/`.
 - `apt-get update`
2. **Observar el Proceso:** Durante la ejecución, la terminal muestra una lista de URLs desde las cuales está obteniendo la información más reciente. Cada entrada comienza con "Obj:" o "Des:" indicando que el proceso está funcionando correctamente.
3. **Verificación de la Actualización:** No se requiere una acción adicional después de este comando para la verificación, ya que la propia salida del comando indica el éxito de la operación.

Resultado: El sistema ha actualizado la información de los paquetes disponibles. Ahora está listo para actualizar los paquetes existentes o instalar nuevos paquetes, como el servidor SSH.

Captura de Pantalla:



```
root@usuario-OptiPlex-380: /home/practicassh# apt-get update
Obj:1 http://es.archive.ubuntu.com/ubuntu focal InRelease
Obj:2 http://ppa.launchpad.net/inkscape.dev/stable/ubuntu focal InRelease
Des:3 http://security.ubuntu.com/ubuntu focal-security InRelease [114 kB]
Des:4 http://dl.google.com/linux/chrome/deb stable InRelease [1.825 B]
Des:5 https://deb.nodesource.com/node_12.x focal InRelease [4.583 B]
Des:6 https://download.docker.com/linux/ubuntu focal InRelease [57,7 kB]
Des:7 https://packages.microsoft.com/repos/vscode stable InRelease [3.573 B]
Des:8 http://dl.google.com/linux/chrome/deb stable/main amd64 Packages [1.084 B
]
Des:9 https://download.docker.com/linux/ubuntu focal/stable amd64 Packages [33,
7 kB]
Des:10 http://security.ubuntu.com/ubuntu focal-security/main i386 Packages [672
kB]
Des:11 https://packages.microsoft.com/repos/vscode stable/main amd64 Packages [
23,3 kB]
Des:12 http://security.ubuntu.com/ubuntu focal-security/main amd64 Packages [2.
569 kB]
Des:13 http://security.ubuntu.com/ubuntu focal-security/main Translation-en [39
8 kB]
Des:14 http://security.ubuntu.com/ubuntu focal-security/main amd64 DEP-11 Metad
ata [59,9 kB]
Des:15 http://security.ubuntu.com/ubuntu focal-security/main DEP-11 48x48 Icons
```

Nota: Tras actualizar la lista de paquetes, es una buena práctica ejecutar `apt-get upgrade` o `apt-get dist-upgrade` para actualizar los paquetes instalados a las últimas versiones disponibles.

Paso 5: Instalación del Servidor SSH


Objetivo: Instalar el servidor SSH (Secure Shell) para permitir conexiones seguras y encriptadas con el servidor para la administración remota.

Procedimiento:

1. **Instalar el Servidor SSH:** Utilizar el comando `apt-get install ssh` para instalar el paquete `ssh`, que incluye tanto el cliente como el servidor SSH. El comando ejecutado es:
 - `apt-get install ssh`
2. **Monitorear la Instalación:** La salida del comando mostrará el progreso de la instalación, incluyendo la descarga del paquete y su configuración.
3. **Verificación de la Instalación:** Una vez que la instalación ha terminado, el texto "Configurando ssh" indica que el paquete se ha instalado y configurado correctamente.

Resultado: El servidor SSH ahora está instalado en el sistema. Esto permitirá que el servidor acepte conexiones entrantes a través del protocolo SSH.

Captura de Pantalla:



```
root@usuario-OptiPlex-380: /home/practicassh
root@usuario-OptiPlex-380:/home/practicassh# apt-get install ssh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  ssh
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 39 no actualizados.
Se necesita descargar 5.084 B de archivos.
Se utilizarán 121 kB de espacio de disco adicional después de esta operación.
Des:1 http://security.ubuntu.com/ubuntu focal-security/main amd64 ssh all 1:8.2p1-4ubuntu0.9 [5.084 B]
Descargados 5.084 B en 0s (14,5 kB/s)
Seleccionando el paquete ssh previamente no seleccionado.
(Leyendo la base de datos ... 374624 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../ssh_1%3a8.2p1-4ubuntu0.9_all.deb ...
Desempaquetando ssh (1:8.2p1-4ubuntu0.9) ...
Configurando ssh (1:8.2p1-4ubuntu0.9) ...
```

Nota: Después de instalar el servidor SSH, es recomendable verificar que el servicio esté en ejecución y escuchando en el puerto predeterminado (que suele ser el puerto 22). Esto se puede hacer con el comando `ss -tulpn` o `netstat -tulpn`.

Paso 6: Configuración del Servidor SSH

Objetivo: Personalizar la configuración del servidor SSH para mejorar la seguridad y especificar qué usuarios pueden utilizar SSH para conectarse al servidor.

Procedimiento:

1. **Editar el Archivo de Configuración:** El archivo `/etc/ssh/sshd_config` contiene las directivas de configuración para el servidor SSH. Para editarlo, se utiliza el editor de texto **gedit**, aunque también podrían utilizarse otros como nano o vi. El comando ejecutado para abrir el archivo en gedit es:

- `gedit /etc/ssh/sshd_config &`

El signo **&** al final del comando permite que el proceso se ejecute en segundo plano, devolviendo el control a la terminal.

2. **Realizar Cambios de Configuración:** Dentro del archivo `sshd_config`, se pueden hacer varios cambios, como:
 - a. Cambiar el puerto por defecto para SSH con la directiva **Port**.
 - b. Permitir o denegar el acceso de root con **PermitRootLogin**.
 - c. Especificar qué usuarios pueden conectarse con **AllowUsers**.
 - d. Configurar la autenticación basada en claves públicas con **PubkeyAuthentication**.

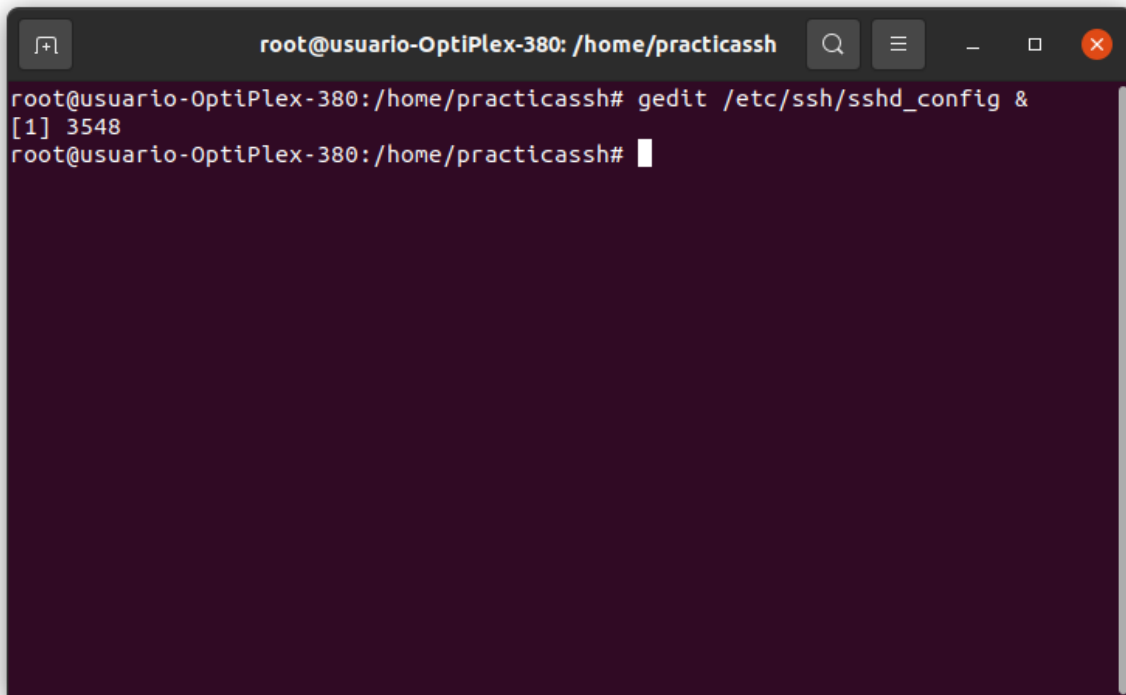
Por ejemplo, se ha añadido **AllowUsers practicassh** para restringir el acceso al usuario **practicassh**.

3. **Guardar los Cambios:** Después de realizar los cambios necesarios, se guardan y se cierra el editor.
4. **Reiniciar el Servidor SSH:** Para que los cambios surtan efecto, es necesario reiniciar el servicio SSH con el comando:
 - `systemctl restart ssh`

Resultado: La configuración de SSH se ha personalizado según las necesidades específicas. Ahora, solo el usuario **practicassh** tiene permiso para conectarse al servidor a través de SSH.

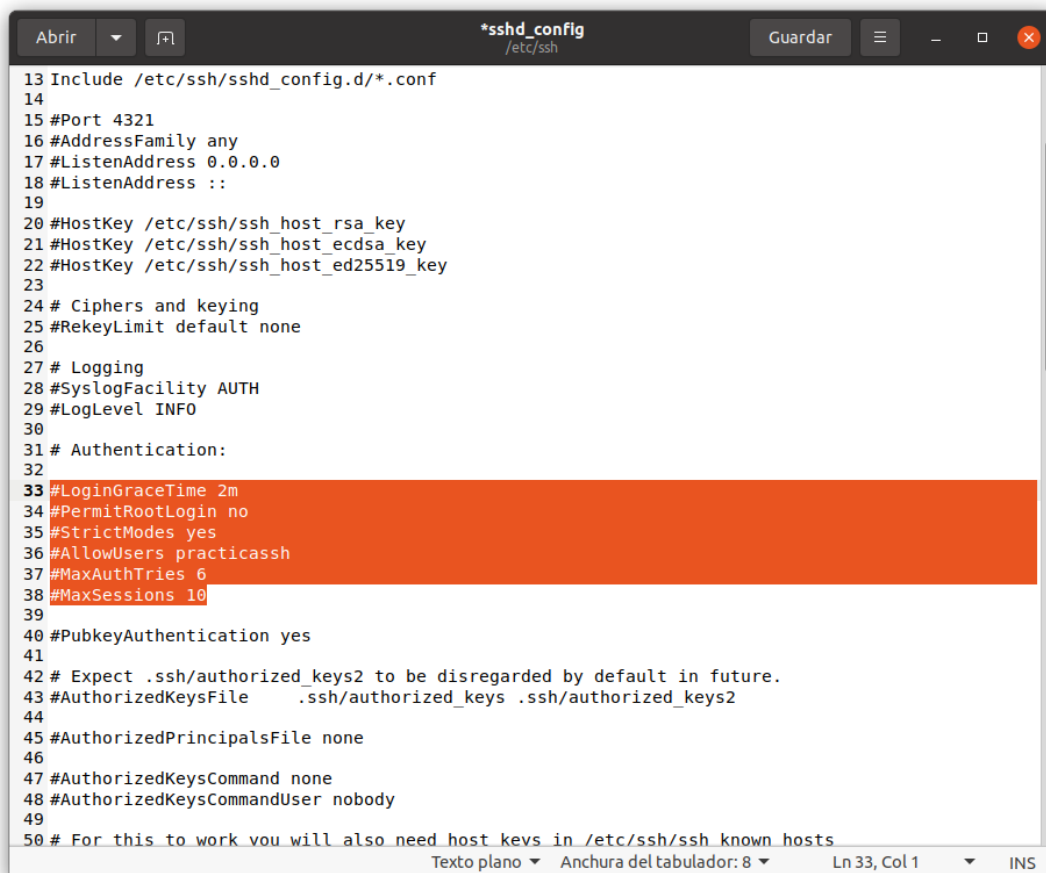
Captura de Pantalla:

Edición de la configuración SSH



```
root@usuario-OptiPlex-380: /home/practicassh
root@usuario-OptiPlex-380:/home/practicassh# gedit /etc/ssh/sshd_config &
[1] 3548
root@usuario-OptiPlex-380:/home/practicassh#
```

Sección de autenticación en el archivo sshd_config



```
Abrir *sshd_config Guardar
/etc/ssh
13 Include /etc/ssh/sshd_config.d/*.conf
14
15 #Port 4321
16 #AddressFamily any
17 #ListenAddress 0.0.0.0
18 #ListenAddress ::
19
20 #HostKey /etc/ssh/ssh_host_rsa_key
21 #HostKey /etc/ssh/ssh_host_ecdsa_key
22 #HostKey /etc/ssh/ssh_host_ed25519_key
23
24 # Ciphers and keying
25 #RekeyLimit default none
26
27 # Logging
28 #SyslogFacility AUTH
29 #LogLevel INFO
30
31 # Authentication:
32
33 #LoginGraceTime 2m
34 #PermitRootLogin no
35 #StrictModes yes
36 #AllowUsers practicassh
37 #MaxAuthTries 6
38 #MaxSessions 10
39
40 #PubkeyAuthentication yes
41
42 # Expect .ssh/authorized_keys2 to be disregarded by default in future.
43 #AuthorizedKeysFile .ssh/authorized_keys .ssh/authorized_keys2
44
45 #AuthorizedPrincipalsFile none
46
47 #AuthorizedKeysCommand none
48 #AuthorizedKeysCommandUser nobody
49
50 # For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
Texto plano Anchura del tabulador: 8 Ln 33, Col 1 INS
```


Nota: Es crucial asegurarse de que los cambios no comprometan la seguridad del servidor y de que no se produzcan errores de sintaxis en el archivo de configuración, ya que podrían impedir que el servicio SSH se inicie correctamente.

Sección 2: PC Cliente.

Paso 1: Conexión al Servidor Mediante SSH desde el PC Cliente

Objetivo: Establecer una conexión SSH desde el PC cliente al servidor para gestionar el servidor de manera remota.

Procedimiento:

1. **Abrir la Terminal en el PC Cliente:** Acceder a la línea de comandos para iniciar la sesión SSH.
2. **Conectar a través de SSH:** Utilizar el comando **ssh** junto con el nombre de usuario en el servidor y la dirección IP del servidor. El comando incluye un cambio de puerto si se ha configurado uno diferente al puerto predeterminado (22). El comando utilizado es:
 - **ssh -p 22 practicassh@192.168.0.150**

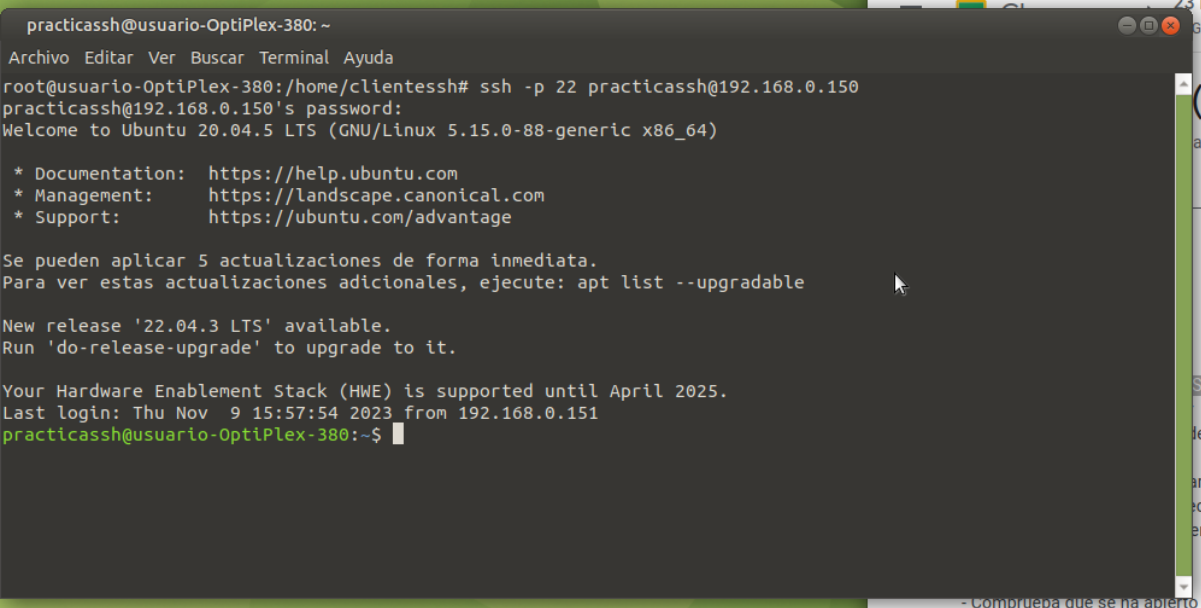
En este caso, -p 22 especifica el puerto al que se desea conectar, que es el puerto por defecto para SSH.

3. **Autenticación:** Tras ejecutar el comando, se pedirá la contraseña del usuario **practicassh** en el servidor. Una vez proporcionada la contraseña correcta, se establecerá la conexión.

Resultado: El PC cliente ahora está conectado al servidor a través de SSH, y el usuario puede ejecutar comandos en el servidor de forma segura y remota.

Captura de Pantalla:

Conexión exitosa a través de SSH desde el PC cliente



```
practicassh@usuario-OptiPlex-380: ~
Archivo Editar Ver Buscar Terminal Ayuda
root@usuario-OptiPlex-380:/home/clientessh# ssh -p 22 practicassh@192.168.0.150
practicassh@192.168.0.150's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-88-generic x86_64)

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

Se pueden aplicar 5 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Thu Nov  9 15:57:54 2023 from 192.168.0.151
practicassh@usuario-OptiPlex-380:~$
```

Nota: Si se ha configurado la autenticación basada en clave pública para SSH, el cliente intentará usar la clave privada correspondiente para autenticarse automáticamente. Si no se ha configurado, se solicitará la contraseña del usuario.

Paso 2: Instalación de Apache en el Servidor

Objetivo: Instalar el servidor web Apache en el servidor para alojar páginas web y aplicaciones web.

Procedimiento:

1. **Permanecer Conectado a través de SSH:** Asegurarse de que la sesión SSH con el servidor aún esté activa.
2. **Actualizar el Índice de Paquetes:** Antes de instalar Apache, es una buena práctica actualizar la lista de paquetes con el comando:
 - **sudo apt update**
3. **Instalar Apache:** Utilizar el gestor de paquetes apt para instalar Apache con el siguiente comando:
 - **sudo apt install apache2**Este comando descargará e instalará el servidor web Apache y todas las dependencias necesarias.
4. **Verificar la Instalación:** Una vez que el proceso de instalación haya finalizado, verificar que Apache se esté ejecutando correctamente con el comando:
 - **sudo systemctl status apache2**

También se puede verificar que Apache está sirviendo páginas web por defecto accediendo a **http://[dirección_IP_del_servidor]** desde cualquier navegador web.

Resultado: Apache debería estar instalado y en ejecución en el servidor. Cualquier cliente conectado a la red debería poder acceder a la página por defecto de Apache usando la dirección IP del servidor.

Nota: Después de instalar Apache, se pueden realizar configuraciones adicionales, como ajustar los archivos de configuración de Apache, asegurar el servidor con un certificado SSL/TLS o subir archivos de sitio web al directorio de documentos de Apache.

Paso 3: Transferencia de una Página Web al Servidor

Objetivo: Mover el contenido de una página web desde el PC cliente al servidor para ser alojada por Apache.

Procedimiento:

1. **Utilizar SCP para la Transferencia:** Desde el PC cliente, utilizar el comando `scp` para transferir de forma segura el directorio de la página web al servidor. El comando utilizado es:
 - **`scp -r /home/clientessh/Escritorio/SasukeUchiha/practicassh@192.168.0.150:/home/practicassh/`**Aquí, `-r` indica que se debe copiar de manera recursiva (todos los archivos y subdirectorios).
2. **Ingresar la Contraseña:** Se solicitará la contraseña del usuario **practicassh** en el servidor para autorizar la transferencia.
3. **Verificación de Transferencia:** Observar la salida del comando **scp** para asegurarse de que todos los archivos se hayan transferido correctamente, lo cual se indica por el progreso de transferencia mostrado para cada archivo.
4. **Mover la Página Web al Directorio de Apache:** Una vez transferidos los archivos, conectarse al servidor vía SSH y mover el directorio de la página web al directorio donde Apache sirve los archivos (`/var/www/`). El comando utilizado es:
 - **`sudo mv /home/practicassh/Escritorio/SasukeUchiha/ /var/www/`**

Resultado: La página web ahora reside en el directorio correcto en el servidor y Apache puede servir su contenido.

Captura de Pantalla:

Transferencia de archivos de la página web al servidor

```
clientessh@usuario-OptiPlex-380: ~
Archivo Editar Ver Buscar Terminal Ayuda
clientessh@usuario-OptiPlex-380:~$ ls
Descargas Escritorio Música Público Videos
Documentos Imágenes Plantillas snap
clientessh@usuario-OptiPlex-380:~$ pwd
/home/clientessh
clientessh@usuario-OptiPlex-380:~$ sudo scp -r /home/clientessh/Escritorio/SasukeUchiha/ practicassh@192.168.0.150:~/Escritorio
[sudo] contraseña para clientessh:
practicassh@192.168.0.150's password:
Sasuke Eternal-Mangekyou-Sharingan.jpg      100% 56KB 7.5MB/s 00:00
Sasuke and Naruto.jpg                      100% 269KB 5.5MB/s 00:00
Susano'o Sasuke Uchiha.jfif                100% 92KB 10.2MB/s 00:00
Símbolo Uchiha.png                         100% 277KB 10.8MB/s 00:00
Sasuke_gif.gif                             100% 688KB 11.0MB/s 00:00
Stapas.jfif                                100% 215KB 10.8MB/s 00:00
Uchiha Sasuke.html                         100% 19KB 7.6MB/s 00:00
Sasuke_Rinnegan.gif                        100% 2369KB 11.2MB/s 00:00
clientessh@usuario-OptiPlex-380:~$
```

Moviendo la página web al directorio de Apache

```
practicassh@usuario-OptiPlex-380: ~/Escritorio
Archivo Editar Ver Buscar Terminal Ayuda
clientessh@usuario-OptiPlex-380:~$ ssh practicassh@192.168.0.150
practicassh@192.168.0.150's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.15.0-88-generic x86_64)

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

Se pueden aplicar 5 actualizaciones de forma inmediata.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

New release '22.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Your Hardware Enablement Stack (HWE) is supported until April 2025.
Last login: Thu Nov 9 19:38:03 2023 from 192.168.0.151
practicassh@usuario-OptiPlex-380:~$ cd /home/practicassh/Escritorio/
practicassh@usuario-OptiPlex-380:~/Escritorio$ ls
hosts 'Practica ssh' SasukeUchiha
practicassh@usuario-OptiPlex-380:~/Escritorio$ sudo mv /home/practicassh/Escritorio/SasukeUchiha/ /var/www/
[sudo] contraseña para practicassh:
practicassh@usuario-OptiPlex-380:~/Escritorio$ ls
hosts 'Practica ssh'
practicassh@usuario-OptiPlex-380:~/Escritorio$ ls /var/www/
Electricidad.html newdora 'Sasuke Uchiha' SasukeUchiha
practicassh@usuario-OptiPlex-380:~/Escritorio$
```

Nota: Es importante asegurarse de que los permisos de los archivos y directorios transferidos sean correctos para que Apache pueda leer y servir el contenido sin problemas. Comandos como **chown** y **chmod** pueden ser necesarios para ajustar los permisos.

Paso 4: Creación de un VirtualHost para la Página Web

Objetivo: Configurar un VirtualHost en Apache para que la página web sea accesible desde un dominio o subdominio específico.

Procedimiento:

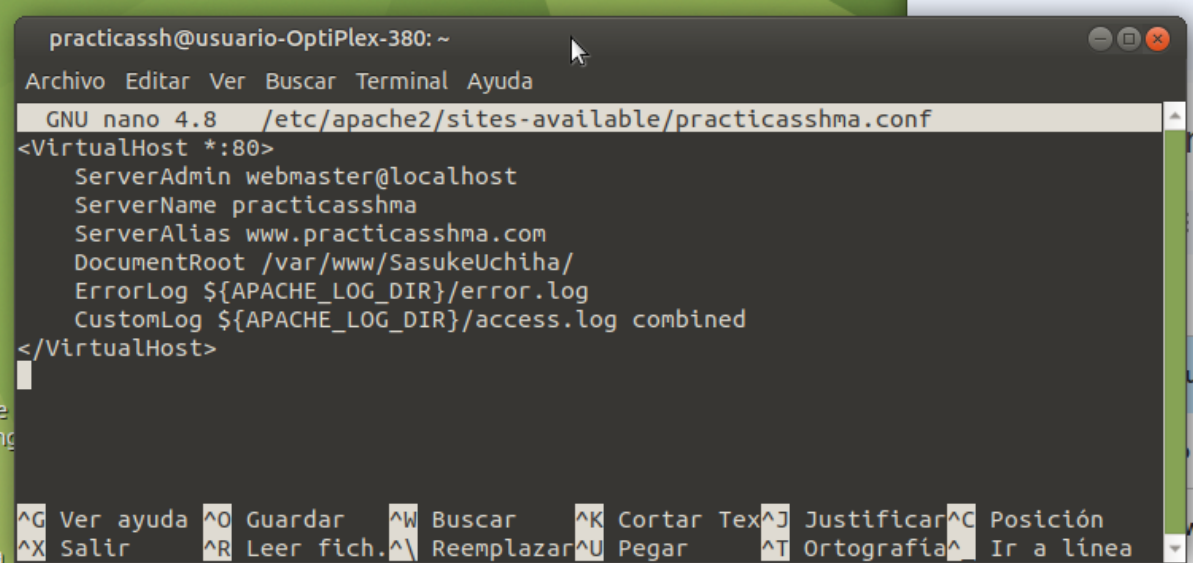
1. **Abrir el Archivo de Configuración del VirtualHost:** Utilizar un editor de texto, como nano, para crear o modificar el archivo de configuración del VirtualHost. El comando utilizado para abrir o crear este archivo es:
 - **sudo nano /etc/apache2/sites-available/practicassh.conf**

2. **Escribir la Configuración del VirtualHost:** Dentro del archivo de configuración, definir los parámetros necesarios para el VirtualHost, como ServerAdmin, ServerName, ServerAlias, DocumentRoot, y las rutas para los archivos de log.

Aquí, **ServerName** es el dominio principal y **ServerAlias** es cualquier otro dominio que debería resolver al mismo sitio web.
3. **Guardar y Cerrar el Archivo:** Guardar los cambios en el archivo y cerrar el editor.
4. **Habilitar el Nuevo VirtualHost:** Ejecutar el siguiente comando para habilitar el sitio utilizando el módulo **a2ensite**:
 - **sudo a2ensite practicassh.conf**
5. **Reiniciar Apache:** Para que los cambios surtan efecto, reiniciar el servidor Apache con el comando:
 - **sudo systemctl restart apache2**

Resultado: El VirtualHost ha sido configurado y habilitado, lo que significa que la página web ahora debería ser accesible desde el dominio especificado en la configuración.

Captura de Pantalla:



The screenshot shows a terminal window with the nano text editor open. The title bar indicates the user is 'practicassh@usuario-OptiPlex-380' in the '~' directory. The editor's status line shows 'GNU nano 4.8' and the file path '/etc/apache2/sites-available/practicasshma.conf'. The content of the file is an Apache VirtualHost configuration for *:80. The configuration includes: ServerAdmin webmaster@localhost, ServerName practicasshma, ServerAlias www.practicasshma.com, DocumentRoot /var/www/SasukeUchiha/, ErrorLog \${APACHE_LOG_DIR}/error.log, and CustomLog \${APACHE_LOG_DIR}/access.log combined. The bottom of the screen displays nano editor shortcuts: ^G Ver ayuda, ^O Guardar, ^W Buscar, ^K Cortar Tex, ^J Justificar, ^C Posición, ^X Salir, ^R Leer fich., ^_ Reemplazar, ^U Pegar, ^T Ortografía, and ^_ Ir a línea.

```
practicassh@usuario-OptiPlex-380: ~
Archivo  Editar  Ver  Buscar  Terminal  Ayuda
GNU nano 4.8 /etc/apache2/sites-available/practicasshma.conf
<VirtualHost *:80>
    ServerAdmin webmaster@localhost
    ServerName practicasshma
    ServerAlias www.practicasshma.com
    DocumentRoot /var/www/SasukeUchiha/
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
^G Ver ayuda ^O Guardar ^W Buscar ^K Cortar Tex ^J Justificar ^C Posición
^X Salir ^R Leer fich. ^_ Reemplazar ^U Pegar ^T Ortografía ^_ Ir a línea
```

Nota: Para que el dominio o subdominio (practicassh.com en este caso) resuelva correctamente al servidor, es necesario configurar los registros DNS apropiados para apuntar al servidor web.

Paso 5: Activación y Recarga de la Configuración de Apache

Objetivo: Activar la nueva configuración del VirtualHost y recargar el servicio Apache para aplicar los cambios.

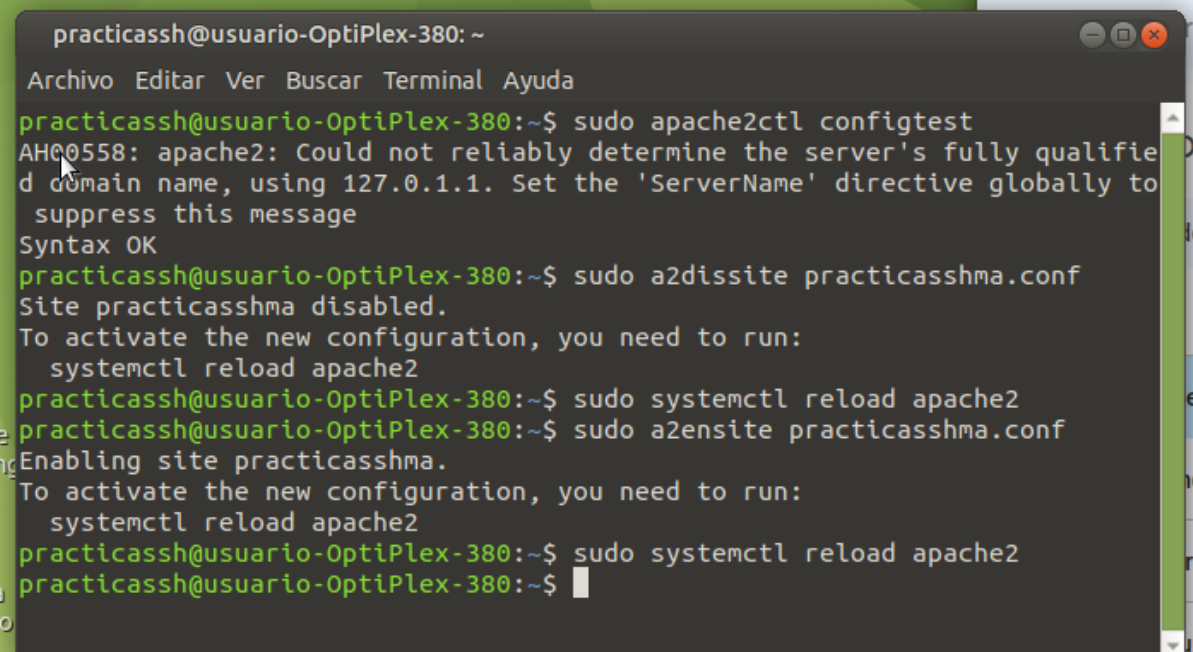
Procedimiento:

1. **Comprobar la Sintaxis de la Configuración:** Antes de activar el nuevo sitio, es importante asegurarse de que no hay errores en los archivos de configuración. Esto se hace con el comando:
 - **sudo apache2ctl configtest**La salida debe indicar "Syntax OK" para confirmar que no hay errores de sintaxis.
2. **Deshabilitar Sitios Antiguos (si es necesario):** Si se necesita deshabilitar un sitio anterior, usar el comando `a2dissite` seguido del nombre de la configuración del sitio:
 - **sudo a2dissite nombre_del_sitio.conf**
3. **Habilitar el Nuevo Sitio:** Usar el comando `a2ensite` para habilitar el nuevo sitio VirtualHost:
 - **sudo a2ensite practicasshma.conf**
4. **Recargar el Servicio Apache:** Para aplicar los cambios sin necesidad de reiniciar el servicio completamente, usar el comando:
 - **sudo systemctl reload apache2**Esto hace que Apache recargue su configuración sin interrumpir el servicio activo.

Resultado: La configuración del nuevo VirtualHost ahora está activa y el servicio Apache ha recargado su configuración, aplicando los cambios.

Captura de Pantalla:

Activación y recarga de la configuración de Apache



```
practicassh@usuario-OptiPlex-380: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
practicassh@usuario-OptiPlex-380:~$ sudo apache2ctl configtest  
AH00558: apache2: Could not reliably determine the server's fully qualified  
domain name, using 127.0.1.1. Set the 'ServerName' directive globally to  
suppress this message  
Syntax OK  
practicassh@usuario-OptiPlex-380:~$ sudo a2dissite practicasshma.conf  
Site practicasshma disabled.  
To activate the new configuration, you need to run:  
systemctl reload apache2  
practicassh@usuario-OptiPlex-380:~$ sudo systemctl reload apache2  
practicassh@usuario-OptiPlex-380:~$ sudo a2ensite practicasshma.conf  
Enabling site practicasshma.  
To activate the new configuration, you need to run:  
systemctl reload apache2  
practicassh@usuario-OptiPlex-380:~$ sudo systemctl reload apache2  
practicassh@usuario-OptiPlex-380:~$
```

Nota: Tras recargar Apache, es recomendable verificar que el sitio está accesible y funcionando como se espera, visitando el dominio configurado en el navegador web.

Paso 6: Modificar el Archivo Hosts del Cliente

Objetivo: Actualizar el archivo `/etc/hosts` en el PC cliente para resolver el dominio del sitio web al servidor correcto mediante su dirección IP.

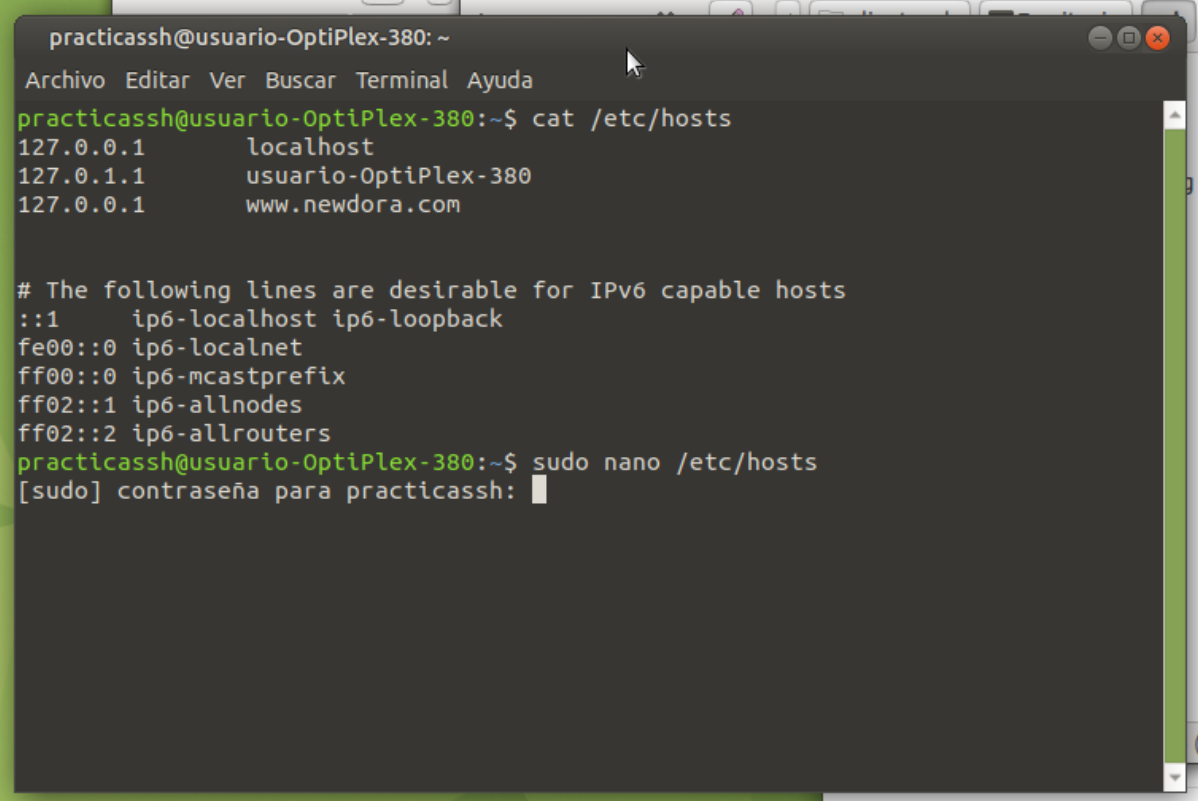
Procedimiento:

1. **Verificar el Archivo Hosts Existente:** Primero, es útil ver el contenido actual del archivo `hosts` para entender qué entradas ya están presentes. Esto se hace con el comando:
 - `cat /etc/hosts`
2. **Editar el Archivo Hosts:** Abrir el archivo `/etc/hosts` con un editor de texto con privilegios de superusuario para agregar la nueva entrada. En este caso, se utiliza `nano`:
 - `sudo nano /etc/hosts`
3. **Agregar la Nueva Entrada:** En el editor, agregar una línea con la dirección IP del servidor seguida del dominio o subdominio que se ha configurado en el `VirtualHost` de Apache. Por ejemplo:
 - `192.168.0.150 practicasshma.com www.practicasshma.com`Guardar el archivo y salir del editor.

4. **Verificar los Cambios:** Para confirmar que la nueva entrada está en efecto, se puede volver a mostrar el contenido del archivo con:
- **cat /etc/hosts**

Resultado: Después de modificar el archivo **/etc/hosts**, el PC cliente resolverá cualquier solicitud al dominio especificado (practicasshma.com en este caso) directamente a la dirección IP del servidor, lo que es útil para probar el sitio web antes de que se actualicen los registros DNS globalmente.

Capturas de Pantalla:
Viendo el archivo hosts

A screenshot of a terminal window titled 'practicassh@usuario-OptiPlex-380: ~'. The window has a menu bar with 'Archivo', 'Editar', 'Ver', 'Buscar', 'Terminal', and 'Ayuda'. The terminal shows the command 'cat /etc/hosts' being executed. The output lists three entries: '127.0.0.1 localhost', '127.0.1.1 usuario-OptiPlex-380', and '127.0.0.1 www.newdora.com'. Below these, there is a comment about IPv6 and a list of IPv6 addresses and their corresponding hostnames. The terminal then shows the command 'sudo nano /etc/hosts' being entered, followed by a password prompt '[sudo] contraseña para practicassh:' with a cursor.

Archivo hosts después de la edición


```
clientessh@usuario-OptiPlex-380: ~
Archivo Editar Ver Buscar Terminal Ayuda
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
practicassh@usuario-OptiPlex-380:~$ sudo nano /etc/hosts
[sudo] contraseña para practicassh:
practicassh@usuario-OptiPlex-380:~$ cat /etc/hosts
127.0.0.1      localhost
127.0.1.1      usuario-OptiPlex-380
127.0.0.1      www.newdora.com
127.0.0.1      www.practicasshma.com

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
practicassh@usuario-OptiPlex-380:~$ exit
logout
Connection to 192.168.0.150 closed.
clientessh@usuario-OptiPlex-380:~$
```

Nota: Este cambio solo afecta al PC cliente en el que se edita el archivo /etc/hosts. No afecta la resolución de DNS en otros dispositivos o en Internet. Para que los cambios sean globales, se debe actualizar la configuración de DNS en el proveedor de servicios de Internet o en el servicio de DNS que se esté utilizando.

Paso 7: Abrir la Página Web en el Navegador del Servidor

Objetivo: Verificar que la página web está correctamente alojada y accesible en el servidor.

Procedimiento:

1. **Acceder al Navegador Web del Servidor:** En el servidor, abrir un navegador web.
2. **Ingresar la URL de la Página Web:** Escribir la dirección del sitio web configurado en el VirtualHost (en este caso, es **www.practicasshma.com**) en la barra de direcciones del navegador.
3. **Navegar a la Página:** Presionar Enter para que el navegador cargue la página web.

Resultado: La página web debería mostrarse correctamente en el navegador si todos los pasos anteriores se han ejecutado correctamente y la configuración de Apache está correcta.

Captura de Pantalla:

Página web cargada en el navegador



Nota: Al abrir la página web directamente en el servidor, se está accediendo a ella a través del localhost. Si se ha modificado el archivo /etc/hosts en el servidor con la dirección IP y el dominio correspondiente, también debería resolverse correctamente.