**Ejercicio 1. Crea unas claves pública/privada con frase de paso y, tras realizar las configuraciones pertinentes, realiza el acceso a una segunda máquina. Una vez dentro de ella, conecta con una tercera sin haber colocado tu clave privada en la segunda.**

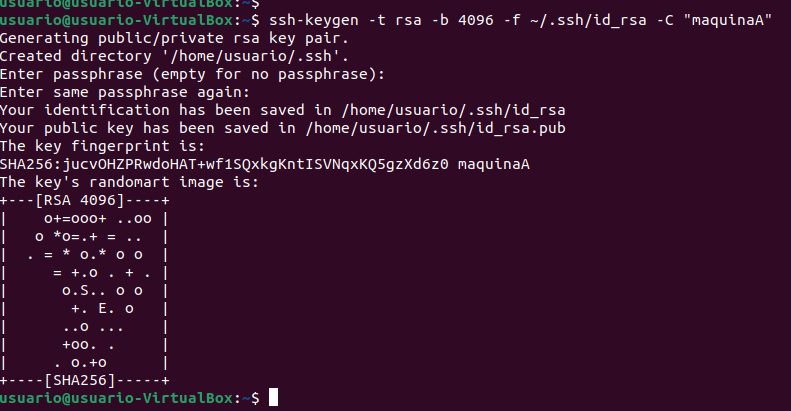
**Como punto importante, al administrador solamente se le pedirá una única vez la frase de paso, pudiendo realizar múltiples accesos sin tener que volverla a introducir.**

**Durante el desarrollo del ejercicio, toda la configuración se realizará sobre los ficheros de configuración globales**.

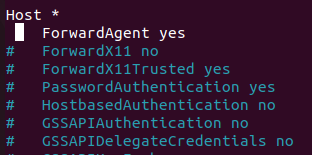
Antes de comenzar deberemos saber que la estructura consiste en:

1. **Máquina A** (Administrador): donde se generarán las claves y se realizará la conexión inicial.
2. **Máquina B** (Intermedia): recibe la conexión desde la Máquina A y se usará para conectarse a la Máquina C.
3. **Máquina C** (Destino): será accedida desde la Máquina B, pero **sin copiar la clave privada** a la Máquina B.

Comenzaremos con la configuración de la máquina 1. Para ello crearemos las claves públicas/privadas con frase, siguiendo el siguiente código:

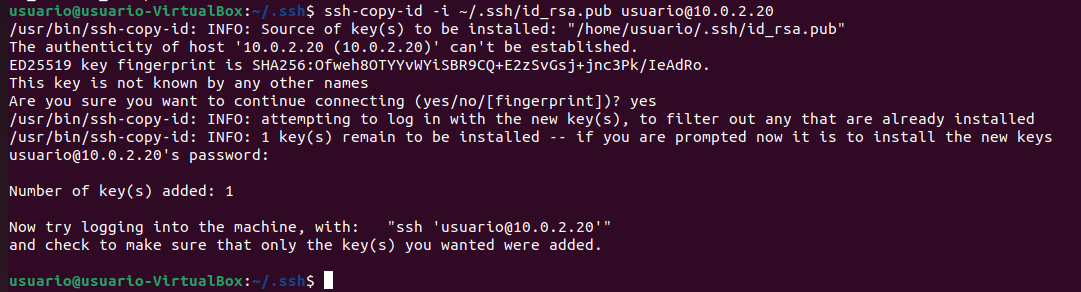


A continuación entraremos en el archivo de configuración ssh\_config, en el descomentamos la linea de ForwardAgent



Una vez descomentado guardaremos el archivo de configuración aplicando los cambios. Por último reiniciamos el servicio ssh

Antes de entrar a la máquina Servidor deberemos copiar la clave del cliente para los propios servidores. Para ello ejecutaremos:



***Máquina Servidor 2:***

En la máquina cliente editaremos el archivo /etc/ssh/sshd\_config. Dentro de este archivo permitiremos las respuestas del servidor, para ello descomentamos la línea de AllowAgentForwarding

Una vez aplicado reiniciamos el servicio sshd

***Máquina Servidor 3:***

Desde nuestra máquina servidor (maquina1) nos conectamos mediante ssh a la máquina cliente 2. Una vez dentro de Máquina 2, ejecutaremos:

ssh-copy-id -i ~/.ssh/id\_rsa.pub usuario@10.0.2.30

Para comprobar el acceso desde maquina1 a maquina3 nos conectaremos desde la maquina servidor a Cliente 3 con el comando:

ssh -A usuario@10.0.2.30

**Ejercicio 2. Repite el ejercicio anterior, aunque esta vez realiza las configuraciones dentro del ámbito del usuario**.

Para este ejercicio comenzaremos generando claves públicas/privadas, al igual que hicimos en el ejercicio anterior.

ssh-keygen -t rsa -b 2048

Una vez creadas, editaremos los ficheros de configuración del cliente SSH en el ámbito del usuario, en el archivo /.ssh/config.

En este archivo añadiremos la línea de comando: ForwardAgent yes

Una vez editado este archivo copiaremos las claves públicas de las dos maquinas clientes con los comandos vistos anteriormente:

ssh-copy-id -i ~/.ssh/id\_rsa.pub usuarioB@IP\_B

ssh-copy-id -i ~/.ssh/id\_rsa.pub usuarioC@IP\_C

Para realizar la comprobación de este ejercicio usaremos el comando ssh usando la IP de cualquiera de las dos máquinas clientes

**Ejercicio 3. Modifica el ejercicio 2 para que el administrador, una vez que realiza la**

**conexión SSH, pueda abrir aplicaciones gráficas desde la terminal. Este ejercicio lo**

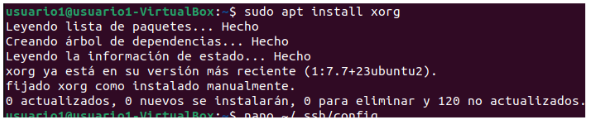
**realizaremos evitando utilizar la opción -X en la cadena de conexión.**

Pasos para habilitar la ejecución de aplicaciones gráficas desde el servidor remoto

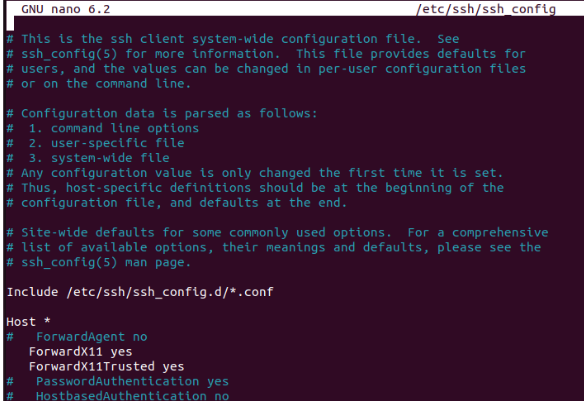
sin usar -X:

1. **Configuración en el Cliente (usuario1 en 10.0.2.10)**

Instalación del servidor X11 (si no estaba instalado): En el cliente, nos aseguramos de tener un servidor gráfico X11, que permitirá la ejecución de aplicaciones gráficas enviadas desde los servidores.

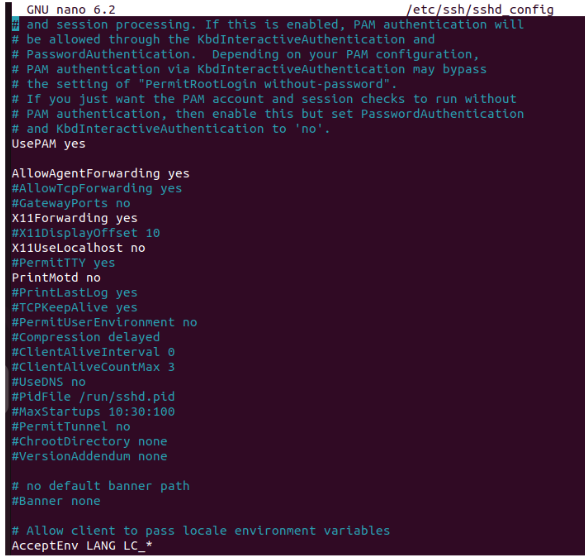


Habilitación del reenvío de X11 en la configuración de SSH: Editamos el archivo de configuración de SSH global en el cliente:



Edición del archivo de configuración SSH del servidor: En ambos servidores,

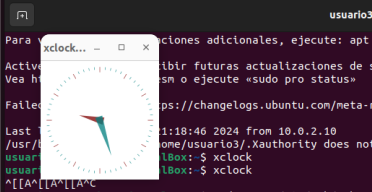
editamos el archivo global /etc/ssh/sshd\_config para habilitar el reenvío de X11:



Por último, desde el cliente (usuario en 10.0.2.10), nos conectamos al Servidor B:

Verificamos que el reenvío de X11 está funcionando correctamente ejecutando

una aplicación gráfica en el servidor remoto:



**Ejercicio 4. Investiga sobre las siguientes opciones de configuración del cliente SSH:**

* **SendEnv. →** Permite enviar variables de entorno al servidor

*Uso práctico:* SendEnv LANG LC\_\*

* **HashKnownHosts. →** Oculta los nombres de los hosts conocidos para mayor privacidad.

*Uso práctico:* HashKnownHosts yes

* **EscapeChar.** → Define el carácter de escape para la sesión SSH.

*Uso práctico:* EscapeChar ~

* **GlobalKnownHostsFile**. → Especifica la ubicación global del archivo de hosts conocidos.

*Uso práctico:* GlobalKnownHostsFile /etc/ssh/ssh\_known\_hosts

* **NumberOfPasswordPrompts**. → Define el número máximo de intentos de contraseña.

*Uso práctico:* NumberOfPasswordPrompts 3

* **StrictHostKeyChecking**. → Controla cómo se manejan los hosts desconocidos

*Uso práctico:* StrictHostKeyChecking ask