I.E.S. Fernando Aguilar Quignon
C/Conil de la Frontera, 3
CP 11010, Cádiz

Administración de Sistemas Operativos - 1ª Evaluación (RA 4 – CE d, e, f) Unidad Didáctica 4. Configuración multiusuario centralizada

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.

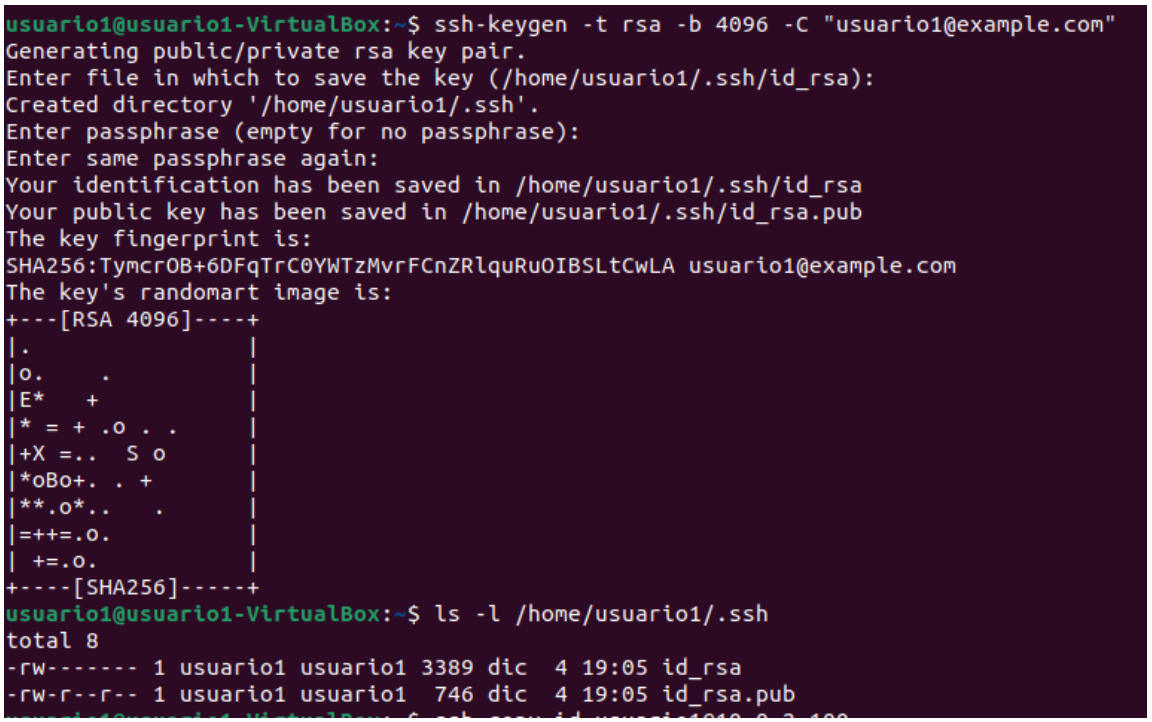
Durante el desarrollo del ejercicio, toda la configuración se realizará sobre los ficheros de configuración globales.

Máquinas y Usuarios

- **Cliente (usuario)**: 10.0.2.10
- **Servidor A (usuario3)**: 10.0.2.50
- **Servidor B (usuario2)**: 10.0.2.100

Paso 1: Crear las claves SSH en la máquina cliente (usuario en 10.0.2.10)

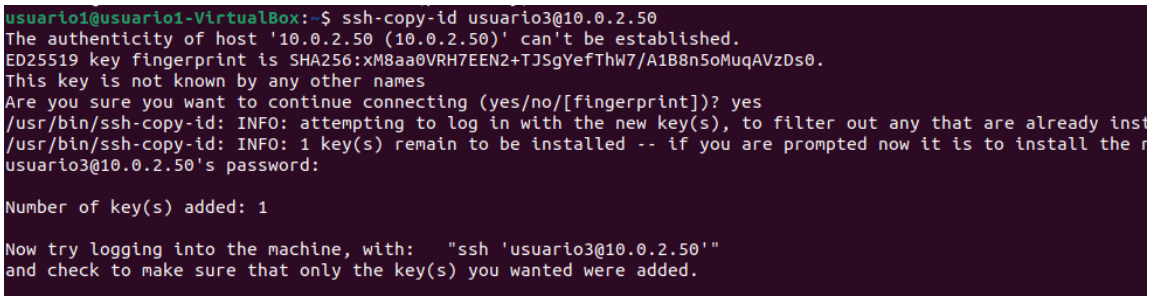
Generar un par de claves SSH con frase de paso: En la máquina cliente (usuario en 10.0.2.10), ejecuta el siguiente comando:



- Esto generará dos archivos en el directorio ~/.ssh/:
  - Clave privada: /home/usuario/.ssh/id_rsa
  - Clave pública: /home/usuario/.ssh/id_rsa.pub

Paso 2: Copiar la clave pública al Servidor A (usuario3 en 10.0.2.50)

Copiar la clave pública al servidor A: En la máquina cliente, usa el siguiente comando para copiar la clave pública a Servidor A (usuario3 en 10.0.2.50):



1. Esto agregará la clave pública al archivo /home/usuario3/.ssh/authorized_keys en **Servidor A**.

Verifica la conexión al Servidor A: Ahora, intenta acceder al **Servidor A**:

```
usuario1@usuario1-VirtualBox:~$ ssh usuario3@10.0.2.50
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-40-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 140 actualizaciones de forma inmediata.
114 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy

usuario3@usuario3-VirtualBox:~$ exit
```

Paso 3: Habilitar el reenvío de agente SSH en la configuración global (Cliente y Servidor A)

1. **En el cliente (10.0.2.10)**:
    - Edita el archivo /etc/ssh/ssh_config para habilitar el reenvío del agente SSH:

sudo nano /etc/ssh/ssh_config

Añade al final del archivo:

```
Host *
   FordwardAgent yes
```

2. Esto permite que el cliente reenvíe la clave privada a **Servidor A** y a otros servidores a los que se conecte.
3. **En el Servidor A (10.0.2.50)**:
    - Edita el archivo /etc/ssh/sshd_config para habilitar el reenvío del agente SSH:

```
AllowAgentForwarding yes
```

Luego, reinicia el servicio SSH:
sudo systemctl restart ssh

Paso 4: Copiar la clave pública desde el Servidor A al Servidor B (usuario2 en 10.0.2.100)

Accede al Servidor A: Desde la máquina **cliente**, accede al **Servidor A**:

```
usuario1@usuario1-VirtualBox:~$ ssh -A usuario3@10.0.2.50
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-40-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 140 actualizaciones de forma inmediata.
114 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Int

Last login: Wed Dec  4 19:50:21 2024 from 10.0.2.10
usuario3@usuario3-VirtualBox:~$
```

Agregar la clave pública al Servidor B: Ahora, en el **Servidor A**, usa ssh-copy-id para copiar la clave pública del **cliente** al **Servidor B** (usuario2 en 10.0.2.100):

```
usuario3@usuario3-VirtualBox:~$ ssh-copy-id usuario2@10.0.2.100
The authenticity of host '10.0.2.100 (10.0.2.100)' can't be established.
ED25519 key fingerprint is SHA256:KQFuTZlFG8KLM+Gsclvvvcef3bAt9s+8LdydOkYQWik.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted n
usuario2@10.0.2.100's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'usuario2@10.0.2.100'"
and check to make sure that only the key(s) you wanted were added.
```

Esto agregará la clave pública a /home/usuario2/.ssh/authorized_keys en **Servidor B**.

Habilitar el reenvío de agente SSH en el Servidor B (10.0.2.100): En **Servidor B**, edita /etc/ssh/sshd_config para habilitar el reenvío de agente SSH:

```
AllowAgentForwarding yes
```

Luego, reinicia el servicio SSH:
sudo systemctl restart ssh

Paso 5: Acceder al Servidor B desde el Servidor A sin ingresar la clave privada

Desde el Servidor A (10.0.2.50), realiza la conexión al **Servidor B (10.0.2.100)** usando el reenvío del agente SSH:

```
usuario3@usuario3-VirtualBox:~$ ssh usuario2@10.0.2.100
usuario2@10.0.2.100's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-49-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 119 actualizaciones de forma inmediata.
94 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet c
```

Paso 6: Verificación del flujo completo

Desde la máquina cliente (10.0.2.10), accede al **Servidor A (10.0.2.50)**:

```
usuario1@usuario1-VirtualBox:~$ ssh -A usuario3@10.0.2.50
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-40-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 140 actualizaciones de forma inmediata.
114 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet c

Last login: Wed Dec  4 19:50:21 2024 from 10.0.2.10
usuario3@usuario3-VirtualBox:~$
```

Desde el Servidor A (10.0.2.50), accede al **Servidor B (10.0.2.100)**:

```
usuario3@usuario3-VirtualBox:~$ ssh usuario2@10.0.2.100
usuario2@10.0.2.100's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-49-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 119 actualizaciones de forma inmediata.
94 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet c
```

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

Máquinas y Usuarios

- **Cliente (usuario1)**: 10.0.2.10
- **Servidor A (usuario3)**: 10.0.2.50
- **Servidor B (usuario2)**: 10.0.2.100

Paso 1: Crear las claves SSH en la máquina cliente (usuario1 en 10.0.2.10)

Generar un par de claves SSH con frase de paso: En la máquina **cliente** (usuario1 en 10.0.2.10), ejecuta el siguiente comando:

```
usuario1@usuario1-VirtualBox:~$ ssh-keygen -t rsa -b 4096 -C "usuario1@example.com"
Generating public/private rsa key pair.
Enter file in which to save the key (/home/usuario1/.ssh/id_rsa):
/home/usuario1/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/usuario1/.ssh/id_rsa
Your public key has been saved in /home/usuario1/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:qqACm6xUSxHvATpe87NuGq2hBU/f2EkenYgH0MIbJsg usuario1@example.com
The key's randomart image is:
+---[RSA 4096]----+
|o .+.            |
|.E.==.           |
| oo+++           |
|. o.= + o .      |
| o + = =So       |
|. * + X.o        |
|o+.* =.=         |
|=oo.=o           |
|=. o+.           |
+----[SHA256]-----+
usuario1@usuario1-VirtualBox:~$ ls -l /home/usuario1/.ssh
total 16
-rw------- 1 usuario1 usuario1 3389 dic  4 20:29 id_rsa
-rw-r--r-- 1 usuario1 usuario1  746 dic  4 20:29 id_rsa.pub
-rw------- 1 usuario1 usuario1 1120 dic  4 19:14 known_hosts
-rw-r--r-- 1 usuario1 usuario1  284 dic  4 19:14 known_hosts.old
```

- Esto generará dos archivos en el directorio ~/.ssh/ de **usuario1**:
  - Clave privada: /home/usuario1/.ssh/id_rsa
  - Clave pública: /home/usuario1/.ssh/id_rsa.pub

Paso 2: Copiar la clave pública al Servidor A (usuario3 en 10.0.2.50)

Copiar la clave pública al servidor A: En la máquina cliente, usa el siguiente comando para copiar la clave pública al Servidor A (usuario3 en 10.0.2.50):

```
usuario1@usuario1-VirtualBox:~$ ssh-copy-id usuario3@10.0.2.50
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed

/usr/bin/ssh-copy-id: WARNING: All keys were skipped because they already exist on the remote system.
              (if you think this is a mistake, you may want to use -f option)
```

1. Esto agregará la clave pública a /home/usuario3/.ssh/authorized_keys en **Servidor A**.

Verifica la conexión al Servidor A: Ahora, intenta acceder al **Servidor A**:

```
usuario1@usuario1-VirtualBox:~$ ssh usuario3@10.0.2.50
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-40-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 140 actualizaciones de forma inmediata.
114 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet conne

Last login: Wed Dec  4 20:15:48 2024 from 10.0.2.10
```

- Se te pedirá la frase de paso solo la primera vez. Luego no se te pedirá más en la misma sesión.

Paso 3: Habilitar el reenvío de agente SSH en la configuración dentro del ámbito del usuario (Cliente y Servidor A)

1. **En el cliente (10.0.2.10)**:
   - Crea o edita el archivo ~/.ssh/config de **usuario1** para habilitar el reenvío del agente SSH:

```
  GNU nano 6.2                                /home/usuario1/.ssh/config
Host *
   ForwardAgent yes
```

2. Esto permite que el cliente reenvíe la clave privada a **Servidor A** y a otros servidores a los que se conecte.

3. **En el Servidor A (10.0.2.50)**:
    - Crea o edita el archivo ~/.ssh/config de **usuario3** para habilitar el reenvío del agente SSH:

4. **Reiniciar el servicio SSH en el Servidor A**: Como estás trabajando dentro del ámbito del usuario, no necesitas modificar la configuración global de SSH en el servidor. En este caso, el archivo ~/.ssh/config es suficiente. Sin embargo, es importante asegurarse de que el reenvío de agente esté habilitado correctamente. Si fuera necesario, también puedes verificar que en el servidor **AllowAgentForwarding yes** esté habilitado.

Paso 4: Copiar la clave pública desde el Servidor A al Servidor B (usuario2 en 10.0.2.100)

Accede al Servidor A: Desde la máquina **cliente**, accede al **Servidor A**:

Agregar la clave pública al Servidor B: Ahora, en el **Servidor A**, usa ssh-copy-id para copiar la clave pública del **cliente** al **Servidor B** (usuario2 en 10.0.2.100):

```
usuario3@usuario3-VirtualBox:~$ ssh-copy-id -f usuario2@10.0.2.100

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'usuario2@10.0.2.100'"
and check to make sure that only the key(s) you wanted were added.
```

1. Esto agrega la clave pública a /home/usuario2/.ssh/authorized_keys en **Servidor B**.

Habilitar el reenvío de agente SSH en el Servidor B (10.0.2.100): En **Servidor B**, edita ~/.ssh/config para habilitar el reenvío de agente SSH para el **usuario2**:

```
  GNU nano 6.2                                  /home/usuario1/.ssh/config
Host *
   ForwardAgent yes
```

Paso 5: Acceder al Servidor B desde el Servidor A sin ingresar la clave privada

Desde el Servidor A (10.0.2.50), realiza la conexión al **Servidor B (10.0.2.100)** usando el reenvío del agente SSH:

```
usuario1@usuario1-VirtualBox:~$ ssh usuario3@10.0.2.50
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-40-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 140 actualizaciones de forma inmediata.
114 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet conne

Last login: Wed Dec  4 20:15:48 2024 from 10.0.2.10
```

Paso 6: Verificación del flujo completo

Desde la máquina cliente (10.0.2.10), accede al **Servidor A (10.0.2.50)**:

```
usuario1@usuario1-VirtualBox:~$ ssh usuario3@10.0.2.50
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-40-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 140 actualizaciones de forma inmediata.
114 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settir

Last login: Wed Dec  4 20:36:22 2024 from 10.0.2.10
```

1. **Desde el Servidor A (10.0.2.50)**, accede al **Servidor B (10.0.2.100)**:

```
usuario3@usuario3-VirtualBox:~$ ssh usuario2@10.0.2.100
usuario2@10.0.2.100's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-49-generic x86_64)

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

El mantenimiento de seguridad expandido para Applications está desactivado

Se pueden aplicar 119 actualizaciones de forma inmediata.
94 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Active ESM Apps para recibir futuras actualizaciones de seguridad adicionales.
Vea https://ubuntu.com/esm o ejecute «sudo pro status»

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settir

Last login: Wed Dec  4 19:52:34 2024 from 10.0.2.50
usuario2@usuario2-VirtualBox:~$
```

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.

```
usuario1@usuario1-VirtualBox:~$ sudo apt install xorg
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
xorg ya está en su versión más reciente (1:7.7+23ubuntu2).
fijado xorg como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 120 no actualizados.
usuario1@usuario1-VirtualBox:~$ nano ~/.ssh/config
```

Habilitación del reenvío de X11 en la configuración de SSH: Editamos el archivo de configuración de SSH global en el cliente:
sudo nano /etc/ssh/ssh_config

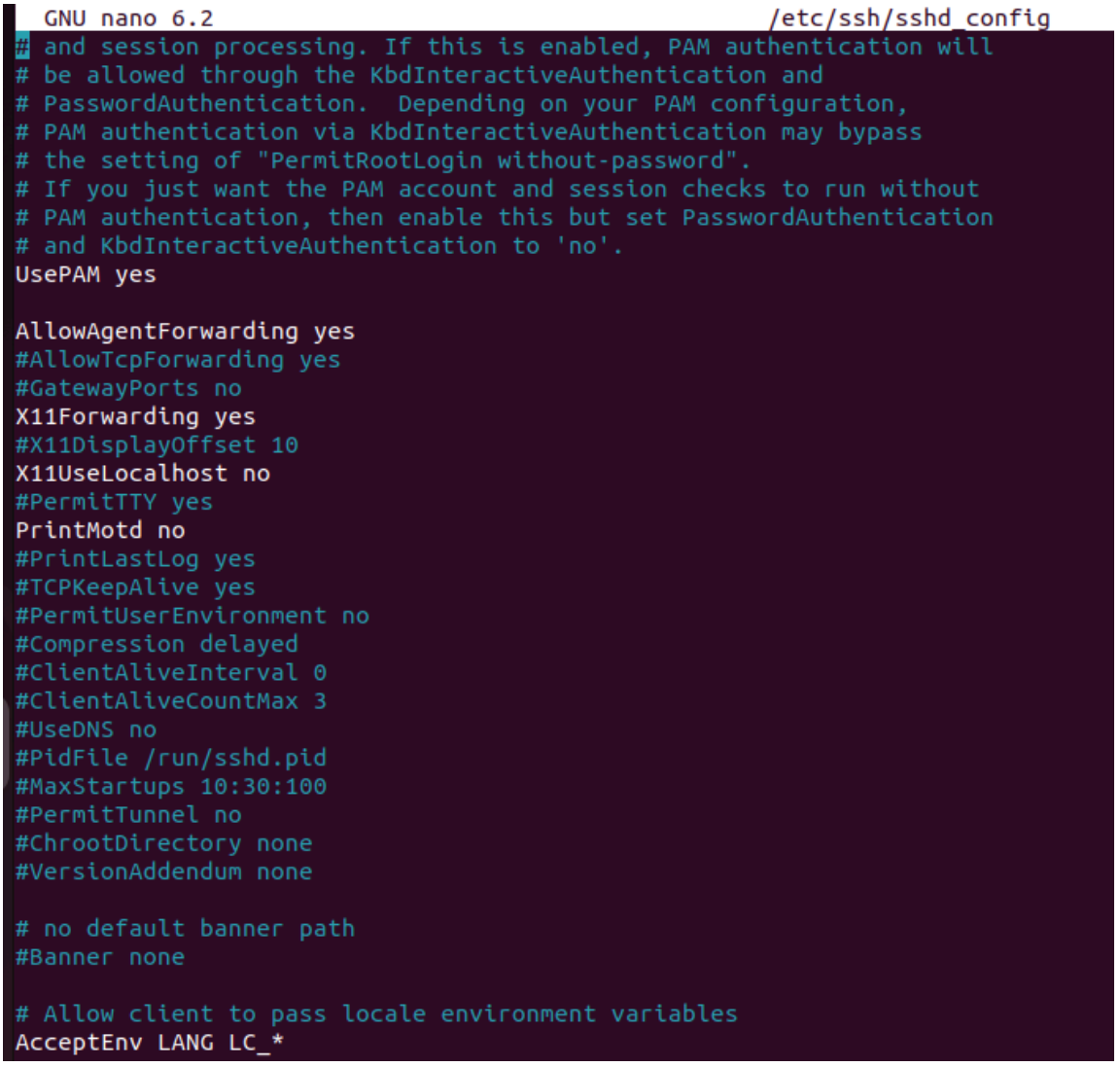
Se descomentaron las siguientes líneas:

```
  GNU nano 6.2                                    /etc/ssh/ssh_config
# This is the ssh client system-wide configuration file.  See
# ssh_config(5) for more information.  This file provides defaults for
# users, and the values can be changed in per-user configuration files
# or on the command line.

# Configuration data is parsed as follows:
#  1. command line options
#  2. user-specific file
#  3. system-wide file
# Any configuration value is only changed the first time it is set.
# Thus, host-specific definitions should be at the beginning of the
# configuration file, and defaults at the end.

# Site-wide defaults for some commonly used options.  For a comprehensive
# list of available options, their meanings and defaults, please see the
# ssh_config(5) man page.

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

Host *
#   ForwardAgent no
   ForwardX11 yes
   ForwardX11Trusted yes
#   PasswordAuthentication yes
#   HostbasedAuthentication no
#   GSSAPIAuthentication no
#   GSSAPIDelegateCredentials no
#   GSSAPIKeyExchange no
#   GSSAPITrustDNS no
#   BatchMode no
#   CheckHostIP yes
#   AddressFamily any
#   ConnectTimeout 0
#   StrictHostKeyChecking ask
#   IdentityFile ~/.ssh/id_rsa
```

Configuración adicional: No se realizaron modificaciones en el archivo ~/.ssh/config ya que las configuraciones globales son suficientes.

2. Configuración en el Servidor A (usuario3 en 10.0.2.50) y Servidor B (usuario2 en 10.0.2.100)

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:



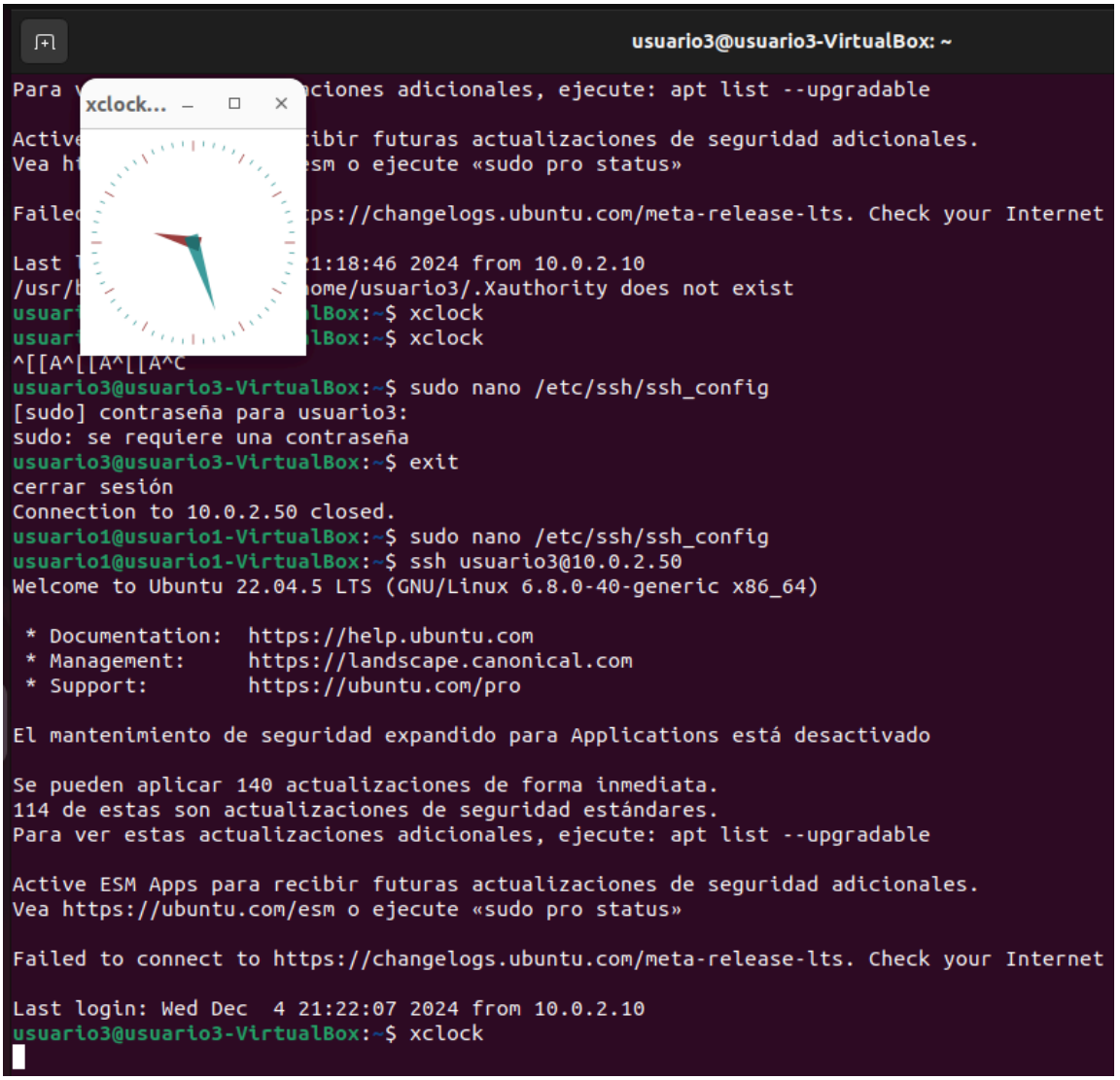
- **UsePAM yes**: Habilita la autenticación PAM, necesaria para algunas configuraciones de seguridad.
- **AllowAgentForwarding yes**: Permite el reenvío del agente SSH.
- **X11Forwarding yes**: Habilita el reenvío de X11, lo que permite ejecutar aplicaciones gráficas.
- **PrintMotd no**: Desactiva la impresión del mensaje del día, optimizando las conexiones SSH.

Reinicio del servicio SSH para aplicar los cambios: Después de realizar los

cambios, reiniciamos el servicio SSH en ambos servidores:
sudo systemctl restart ssh

Prueba del flujo de trabajo

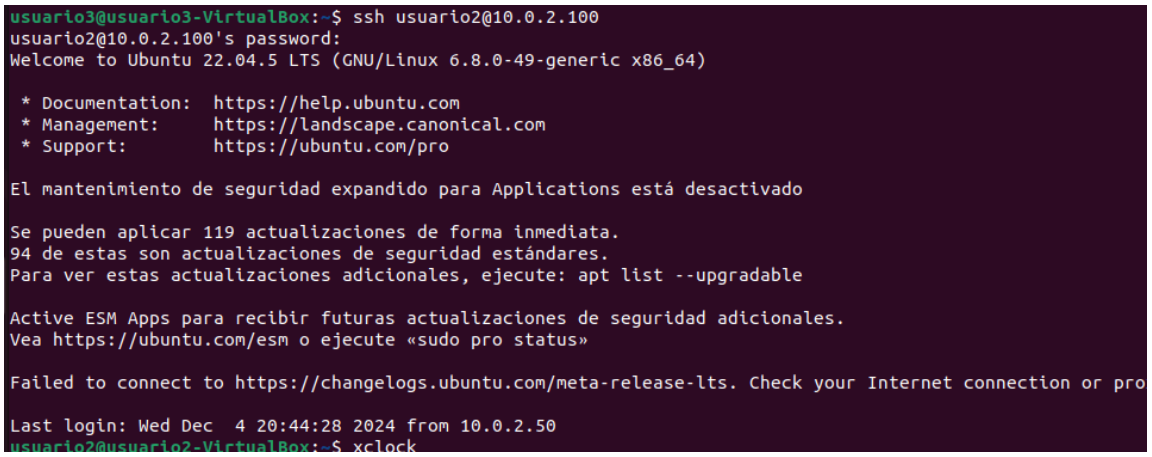
Desde el cliente (usuario1 en 10.0.2.10), nos conectamos al **Servidor A**:
Verificamos que el reenvío de X11 está funcionando correctamente ejecutando una aplicación gráfica en el servidor remoto:



Esto debería abrir la aplicación gráfica xclock en el cliente, indicando que la configuración ha sido exitosa.

Desde el **Servidor A**, también verificamos el acceso al **Servidor B** (si es necesario):
ssh usuario2@10.0.2.100

1. Nuevamente, probamos ejecutar aplicaciones gráficas desde el **Servidor B**.



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

- **SendEnv.**
- **HashKnownHosts.**
- **EscapeChar.**
- **GlobalKnownHostsFile.**
- **NumberOfPasswordPrompts.**
- **StrictHostKeyChecking.**

1. SendEnv

- **Descripción:**
  - Permite enviar variables de entorno del cliente al servidor SSH. Esto es útil si el servidor necesita utilizar ciertas configuraciones del cliente, como idioma (LANG) o configuración regional.

Configuración en ssh_config:
- SendEnv LANG LC_*

- Esto envía las variables relacionadas con el idioma y localización al servidor.
- **Requisitos:**
  - El servidor debe estar configurado para aceptar estas variables, configurando AcceptEnv en sshd_config.

Ejemplo práctico: Supongamos que tu cliente usa el idioma español. Puedes enviar esta configuración al servidor:
- SendEnv LANG

2. HashKnownHosts

- **Descripción:**

    - Determina si las direcciones IP y nombres de host se deben almacenar en formato hash en el archivo ~/.ssh/known_hosts.
    - Usar hashes mejora la seguridad, ya que protege la información de servidores en caso de que alguien obtenga acceso al archivo known_hosts.

Configuración en ssh_config:
- HashKnownHosts yes

- Con esta configuración, las entradas en known_hosts estarán en formato cifrado.
- **Ventajas:**
    - Evita la exposición de los nombres o direcciones IP de los servidores SSH en texto plano.
- **Nota:**
    - Si activas esta opción, no podrás buscar manualmente nombres de host en known_hosts.

---

3. EscapeChar

- **Descripción:**
    - Define un carácter especial que permite realizar comandos en la sesión SSH activa, como suspender la conexión o ejecutar comandos locales.

Configuración en ssh_config:
- EscapeChar ~

- Por defecto, el carácter de escape es ~.
- **Comandos útiles con el carácter de escape:**
    - ~.: Cierra la conexión SSH inmediatamente.
    - ~C: Abre un modo de comando especial.
    - ~?: Muestra una lista de comandos disponibles.
- **Nota:**

Si prefieres no usar un carácter de escape, puedes deshabilitar esta opción configurándola como:
- EscapeChar none

    -

---

4. GlobalKnownHostsFile

- **Descripción:**
    - Especifica la ubicación del archivo global que contiene las claves públicas conocidas de los servidores SSH.
    - Por defecto, es /etc/ssh/ssh_known_hosts.

Configuración en ssh_config:
- GlobalKnownHostsFile /etc/ssh/ssh_known_hosts

- Puedes usar esta opción para apuntar a un archivo alternativo.
- **Uso combinado con UserKnownHostsFile:**
    - GlobalKnownHostsFile define el archivo global (compartido por todos los usuarios).
    - UserKnownHostsFile define el archivo de claves específicas del usuario (como ~/.ssh/known_hosts).

---

5. NumberOfPasswordPrompts

- **Descripción:**
    - Establece el número máximo de veces que el cliente SSH solicitará la contraseña al usuario si la autenticación inicial falla.

Configuración en ssh_config:
- NumberOfPasswordPrompts 2

- En este ejemplo, el cliente solicitará la contraseña dos veces antes de abandonar la conexión.
- **Uso:**
    - Es útil para evitar intentos infinitos de autenticación, especialmente si usas scripts automáticos o servicios que no deberían interactuar con el usuario repetidamente.

---

6. StrictHostKeyChecking

- **Descripción:**
    - Controla cómo el cliente SSH maneja las claves de host desconocidas.
- **Opciones disponibles:**
    - yes: El cliente rechazará cualquier conexión si la clave del servidor no coincide con la clave en known_hosts.
    - no: El cliente conectará automáticamente y añadirá la clave del servidor al archivo known_hosts.
    - ask: El cliente pedirá al usuario confirmar si se debe aceptar la clave del servidor. Esta es la configuración predeterminada en muchas distribuciones.

Configuración en ssh_config:
- StrictHostKeyChecking ask

-

Ejemplo práctico: Si prefieres evitar confirmaciones interactivas en un entorno automatizado:
- StrictHostKeyChecking no

- Sin embargo, esto puede ser un riesgo de seguridad si un servidor malintencionado suplanta al legítimo.

RESUMEN:

Opción	Descripción	Ejemplo
SendEnv	**Envía variables de entorno del cliente al servidor.**	**SendEnv LANG LC_***
HashKnownHosts	**Guarda los nombres/IP de los hosts en formato hash.**	**HashKnownHosts yes**
EscapeChar	**Define un carácter para realizar comandos especiales en la sesión SSH.**	**EscapeChar ~**
GlobalKnownHostsFile	**Especifica el archivo global de claves públicas de hosts.**	**GlobalKnownHostsFile /path/file**
NumberOfPasswordPrompts	**Define cuántas veces se solicitará la contraseña al usuario antes de abandonar la conexión.**	**NumberOfPasswordPrompts 2**
StrictHostKeyChecking	**Controla cómo manejar claves de host desconocidas.**	**StrictHostKeyChecking ask**