***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

**Desarrolla un script para bash que realice la gestión de servicios en múltiples servidores GNU/Linux. Para poder llevarlo a cabo, este recibirá como parámetro de entrada el nombre de un fichero de datos con la siguiente estructura:**

*nombreUsuario,ip,servicio,acción*

**Como salida, el usuario obtendrá si cada acción se ha realizado correctamente o no.**

**Como restricción principal, la ejecución deberá ser totalmente desatendida, evitando solicitar cualquier tipo de acción por parte del usuario.**

Además de lo anterior, el servidor deberá cumplir las siguientes condiciones:

* Crearemos un nuevo usuario para ejecutar esta tarea.
* El acceso a la máquina solamente se podrá realizar mediante claves asimétricas, quedando deshabilitado cualquier otro tipo de acceso.
* El acceso remoto como usuario root, vía SSH, debe estar deshabilitado.
* El puerto de acceso no podrá ser el 22.
* La utilización de sudo estará restringido a determinados comandos.
* Solo aceptará peticiones de conexión desde una máquina determinada.

Para realizar la siguiente actividad, comenzaremos instalando openssh-server, lo que nos permitirá arrancar los servicios SSH necesarios para la comunicación entre el servidor controlador y los servidores remotos. Este servicio será configurado para cumplir con las restricciones y requisitos de seguridad que podemos ver en el enunciado

Para instalar este servicio seguiremos los siguientes pasos:

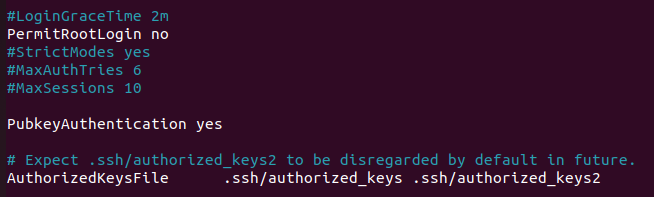
* **sudo apt update →** Este comando sincroniza la lista de paquetes, asegurando que instalemos la versión más reciente del paquete
* **sudo apt install openssh-server -y →** Este comando descarga e instala el paquete openssh-server, que habilita la funcionalidad de SSH en el servidor
* **sudo systemctl enable ssh →** Este comando habilita el servicio instalado.

1. **Configuración Inicial:**

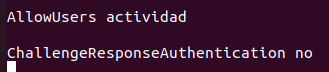
**Editar el archivo de configuración /etc/ssh/sshd\_config:**

1. A continuación, necesitamos ajustar la configuración del servicio para cumplir con las restricciones de seguridad:







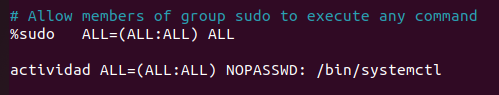


Por último reiniciamos el servicio.

1. **Creación del Usuario y Configuración de Claves Asimétricas:**
2. **Creación de un nuevo Usuario:**

Para esta actividad crearemos un nuevo usuario llamado act4, siguiendo los pasos:

* sudo adduser actividad
* sudo chmod 700 /home/actividad
* sudo chown actividad:actividad /home/actividad
* sudo visudo:

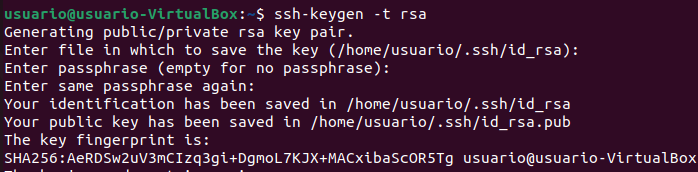


Este usuario será quien ejecute los scripts de gestión de servicios. Durante la creación, se solicitará configurar una contraseña para el usuario

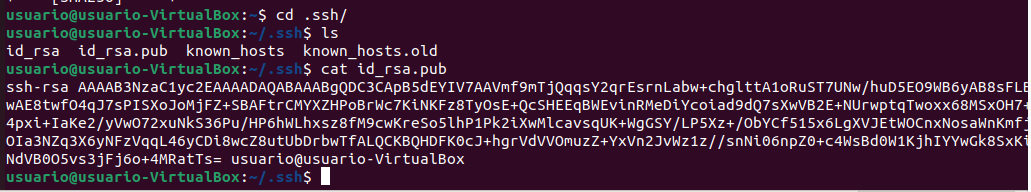
1. **Configurar acceso por claves asimétricas:**

En la máquina desde donde se gestionan los servicios, generamos un par de claves SSH si aún no existe

* Comenzaremos creando las propias claves:



* Comprobaremos la creación de la clave a través de la ruta necesaria, en este caso se encuentra en el directorio .ssh/ . Una vez allí, listamos el contenido y podremos ver el contenido de ese código con cat



1. **Máquina Cliente:**

Una vez tengamos creada la clave en la máquina servidor, accedemos a la máquina cliente para poder copiar su clave e intentar la conexión mediante ssh. Para ello seguiremos los siguientes pasos:

1. **Crear la clave del cliente:**

En la máquina cliente, abrimos una terminal y ejecutamos el siguiente comando para crear un par de claves RSA:

* ssh-keygen -t rsa

1. **Verificar que las claves se han creado:**

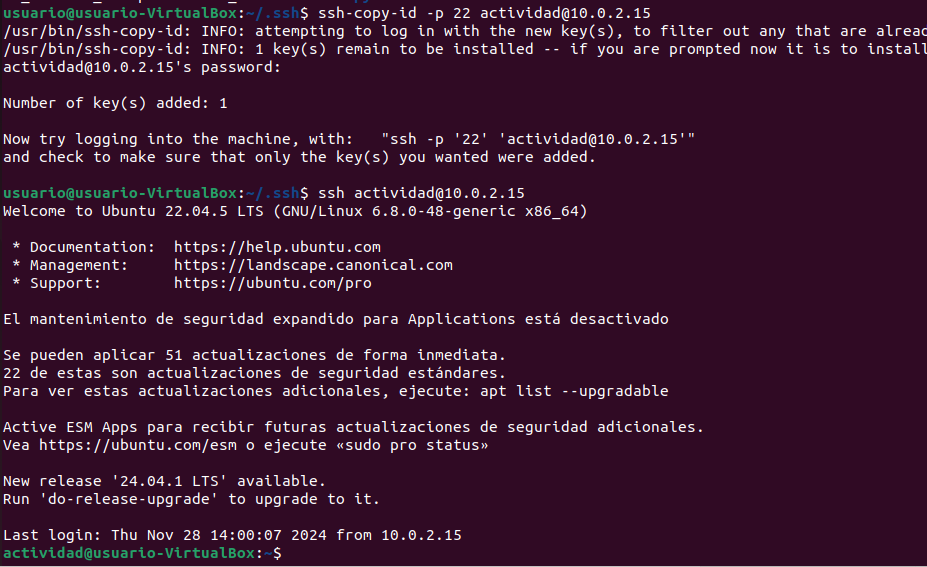
Entraremos en el directorio .ssh y lanzaremos el comando ls para comprobar su información.

Dentro de este directorio nos encontramos con:

* id\_rsa: la clave privada.
* id\_rsa.pub: la clave pública.

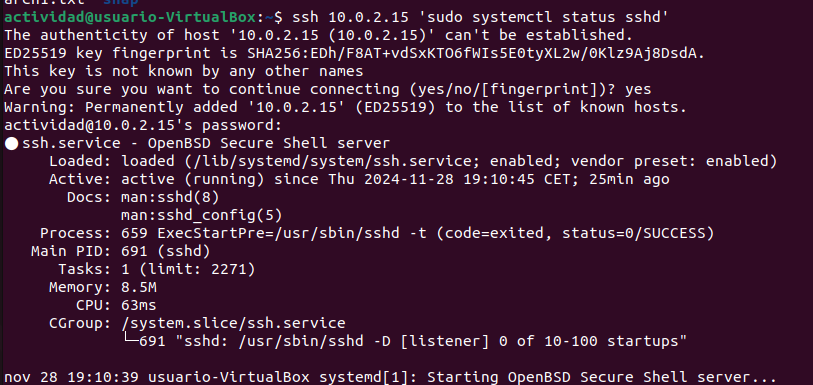
1. **Copiar la clave pública al servidor:**

Ahora que tenemos la clave pública en la máquina cliente, necesitamos copiar al servidor para poder autenticarnos sin usar la contraseña. Además comprobaremos la conexión



1. **Comandos remotos**

Con este comando (o cualquier otro que tenga la opción de ejecutar un servicio) comprobaremos que podemos realizar operaciones desde la máquina cliente a nuestro servidor.

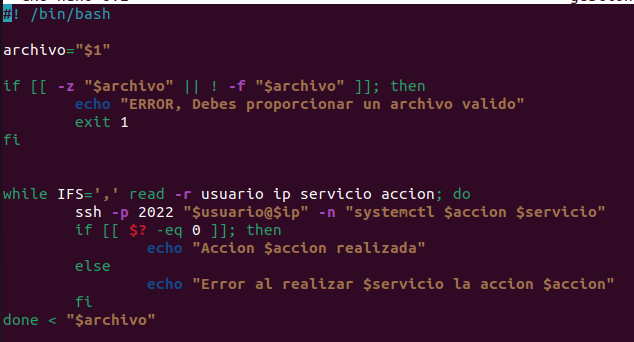


1. **Scripts y ejecución:**

Una vez comprobada la ejecución del proceso, desde la propia máquina del cliente (saliendo de ssh, usando exit) crearemos el script de ejecución y el archivo de datos.

1. **Script gestion.sh y datos.txt**

Este script lo podemos crear en la propia carpeta personal del usuario. El script deberá contener la siguiente información:

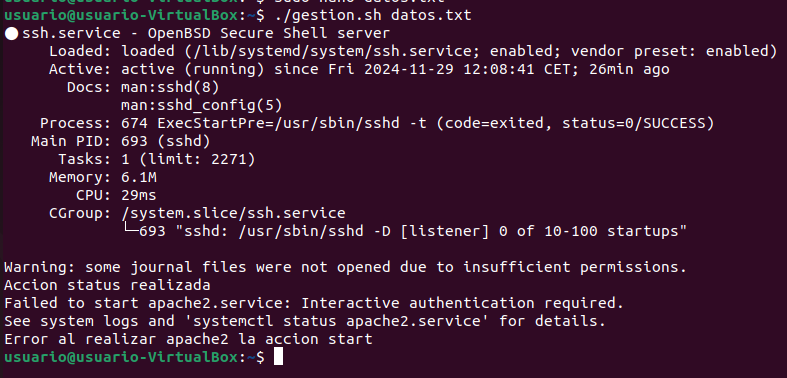


El archivo de datos deberá contener los parámetros elegidos en el script que en este caso son: usuario, ip (del servidor donde queramos ejecutar), servicio (importante comprobar que esté instalado en el sistema) y acción



1. **Ejecución y comprobación del script**

Para ejecutar el script deberemos aplicar los permisos correspondientes con chmod y luego ejecutar:



Como podemos ver, reconoce el servicio ssh y nos muestra el estado, pero al no tener instalado apache2 en el servidor vemos el error.

Si editamos el archivo de datos y aplicamos el servicio cron podremos ver:

