

64_sshpasspgp

Emilio Cabo Gomis

Sumario

Escenario.....	3
Datos maquinas.....	3
Configuración de sshPass.....	5

Escenario

Implementaremos en nuestro script de copia de seguridad gpg key y sshpass para evitar tener que meter la contraseña en claro cuándo nos conectamos a nuestra máquina mediante el protocolo ssh.

Datos maquinas

Máquina ubuntu:

```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP
group default qlen 1000
    link/ether 08:00:27:49:fc:b7 brd ff:ff:ff:ff:ff:ff
    inet 172.30.2.22/24 brd 172.30.2.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe49:fc7/64 scope link
        valid_lft forever preferred_lft forever
```

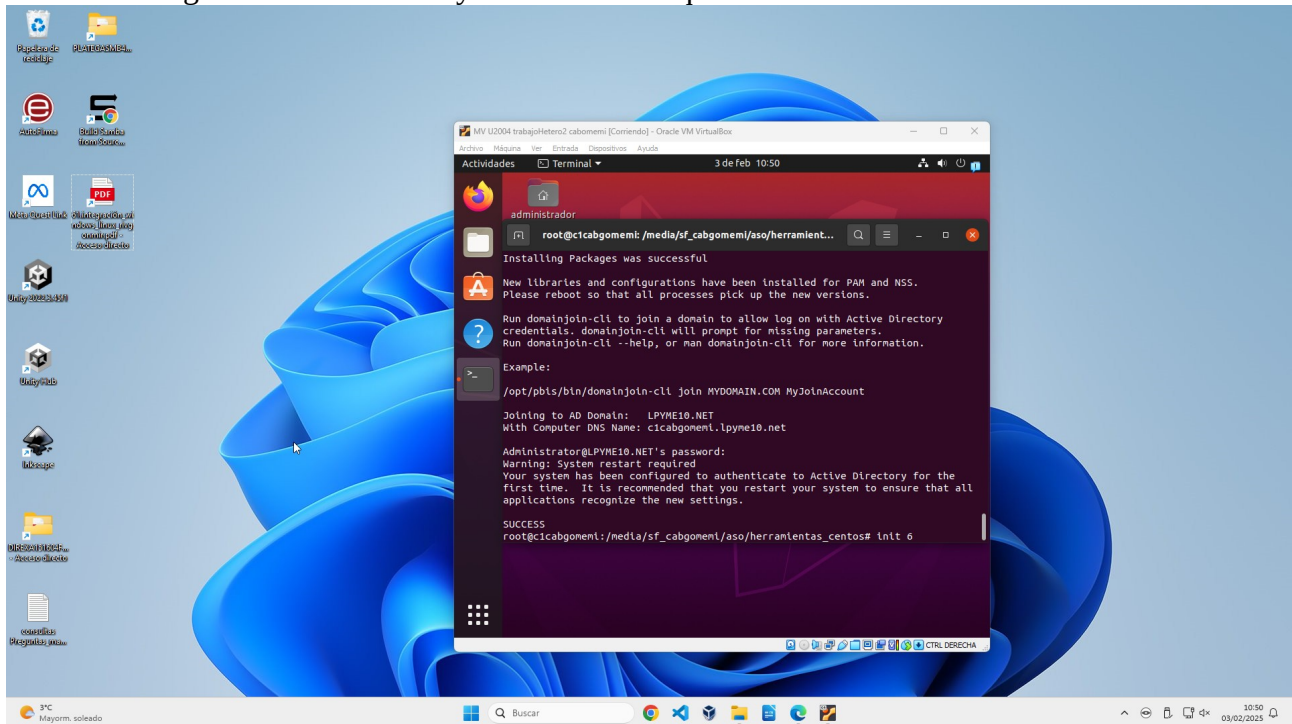
hostname: **c1cabgomemi**

Maquina centos

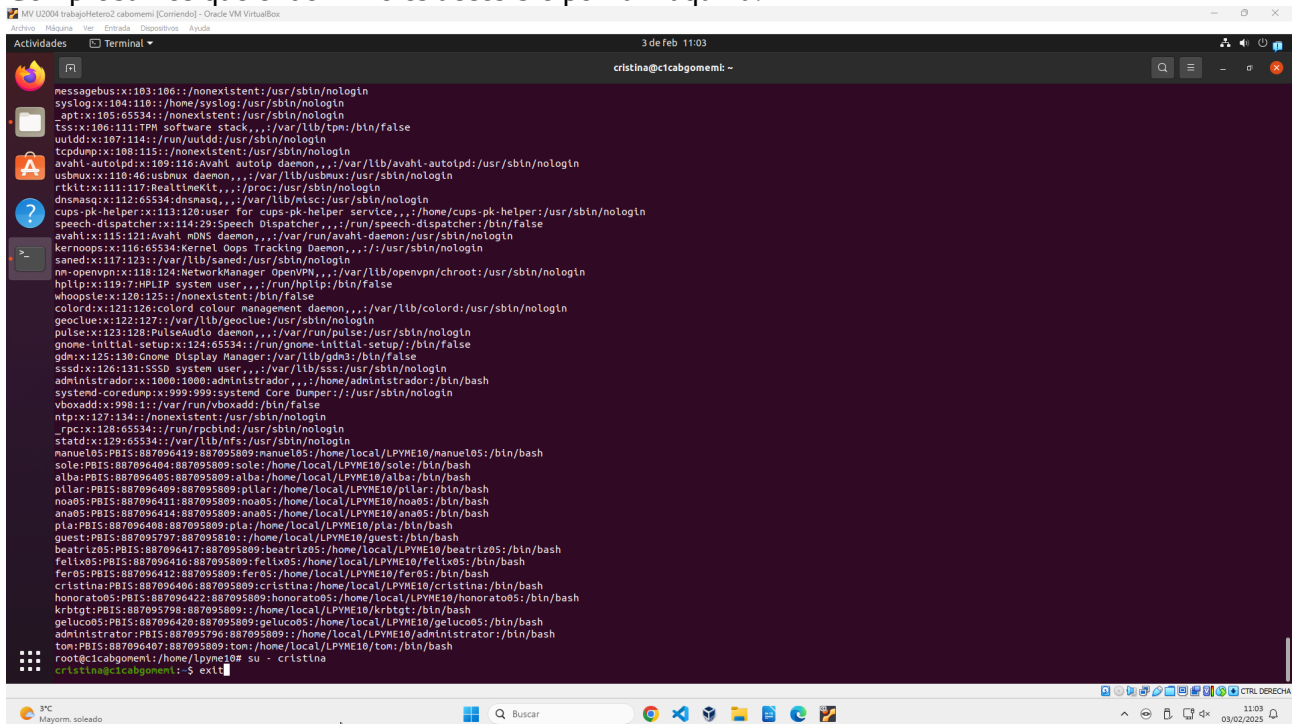
```
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:c9:8e:48 brd ff:ff:ff:ff:ff:ff
    inet 172.30.2.21/24 brd 172.30.2.255 scope global enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fec9:8e48/64 scope link
        valid_lft forever preferred_lft forever
```

hostname: **s1cabgomemi**

Primero configuramos un dominio y uniremos la maquina ubuntu al dominio.

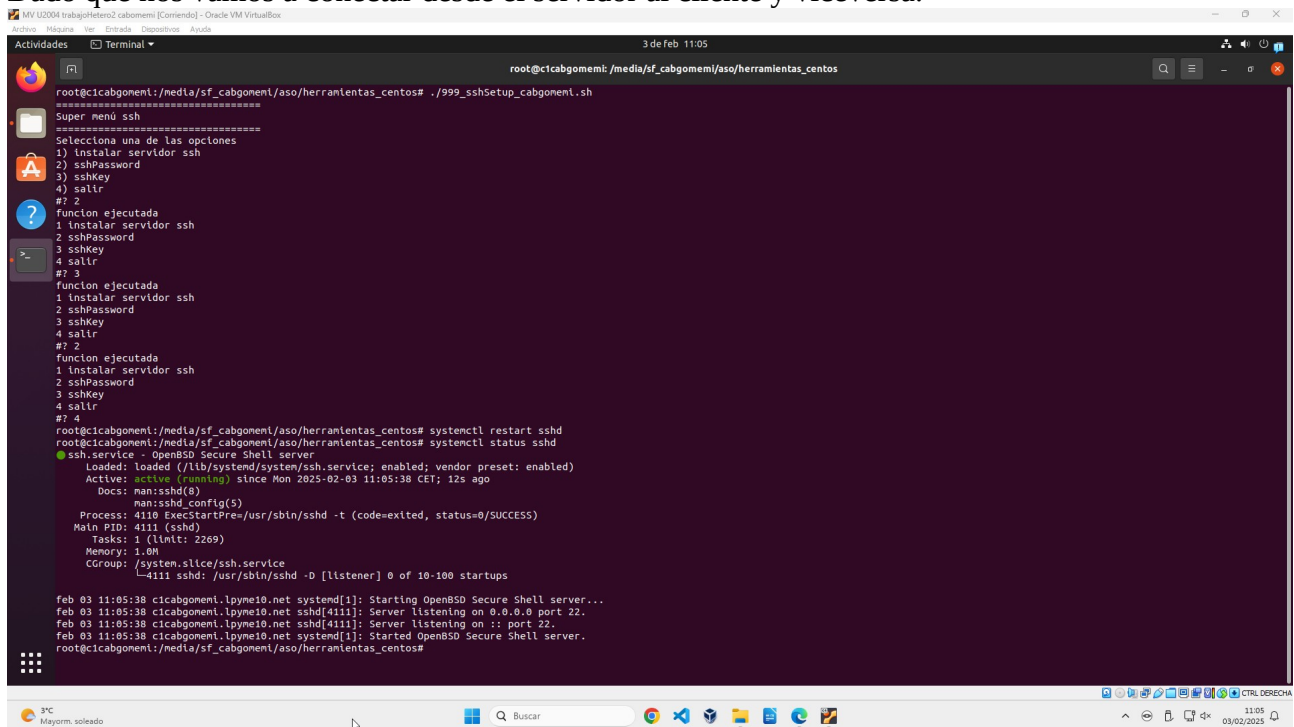


Comprobamos que el dominio es accesible por la máquina.



Configuración de sshPass.

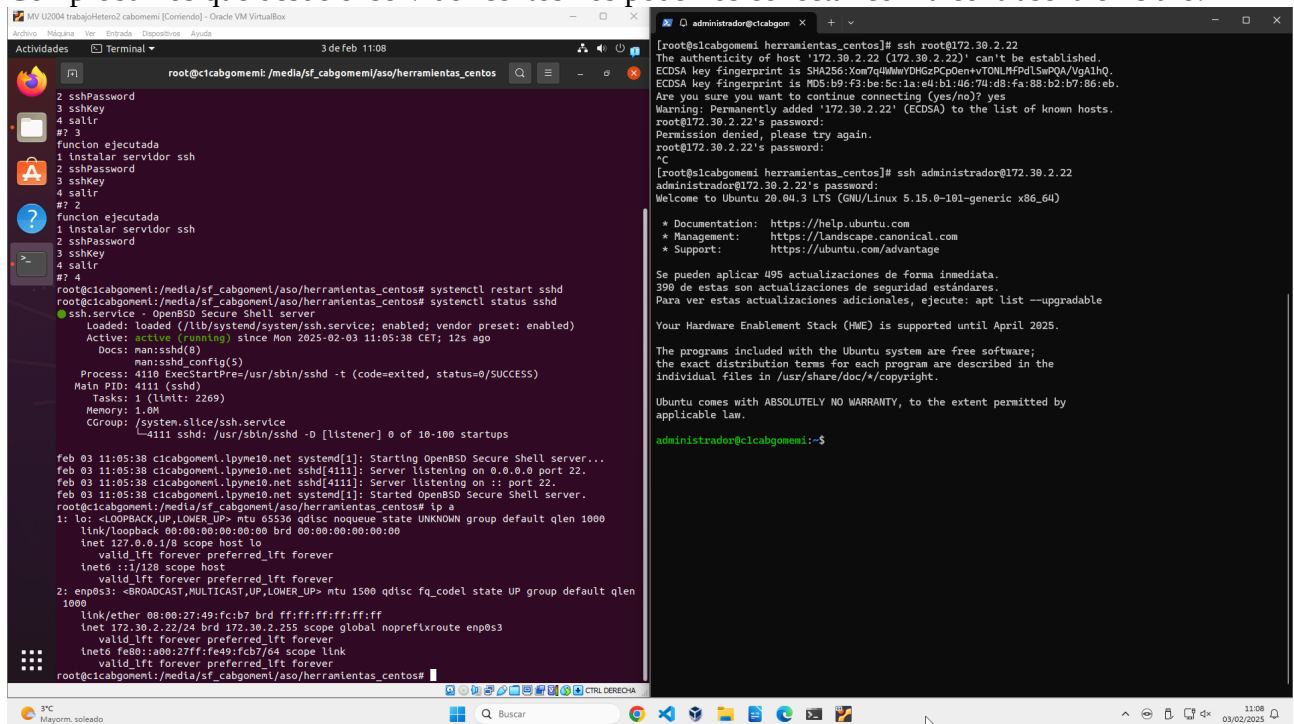
Primero ejecutamos el scripting para la instalación de sshd en el cliente.
Dado que nos vamos a conectar desde el servidor al cliente y viceversa.



```
root@cicabogomem:/media/sf_cabogomem/aso/herramientas_centos# ./999_sshSetup_cabogomem.sh
=====
Super menú ssh
=====
Selecciona una de las opciones
1) Instalar servidor ssh
2) sshPassword
3) sshKey
4) salir
#? 2
funcion ejecutada
1) Instalar servidor ssh
2) sshPassword
3) sshKey
4) salir
#? 3
funcion ejecutada
1) Instalar servidor ssh
2) sshPassword
3) sshKey
4) salir
#? 2
funcion ejecutada
1) Instalar servidor ssh
2) sshPassword
3) sshKey
4) salir
#? 4
root@cicabogomem:/media/sf_cabogomem/aso/herramientas_centos# systemctl restart sshd
root@cicabogomem:/media/sf_cabogomem/aso/herramientas_centos# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2025-02-03 11:05:38 CET; 12s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 4110 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 4111 (sshd)
      Tasks: 1 (limit: 2269)
     Memory: 1.0M
    CGroup: /system.slice/ssh.service
            └─4111 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

feb 03 11:05:38 cicabogomem.lpyne10.net systemd[1]: Starting OpenBSD Secure Shell server...
feb 03 11:05:38 cicabogomem.lpyne10.net sshd[4111]: Server listening on 0.0.0.0 port 22.
feb 03 11:05:38 cicabogomem.lpyne10.net sshd[4111]: Server listening on :: port 22.
feb 03 11:05:38 cicabogomem.lpyne10.net systemd[1]: Started OpenBSD Secure Shell server.
root@cicabogomem:/media/sf_cabogomem/aso/herramientas_centos#
```

Comprobamos que desde el servidor centos nos podemos conectar con la contraseña en claro.



```
root@cicabogomem:/media/sf_cabogomem/aso/herramientas_centos# systemctl restart sshd
root@cicabogomem:/media/sf_cabogomem/aso/herramientas_centos# systemctl status sshd
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2025-02-03 11:05:38 CET; 12s ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 4110 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
    Main PID: 4111 (sshd)
      Tasks: 1 (limit: 2269)
     Memory: 1.0M
    CGroup: /system.slice/ssh.service
            └─4111 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

feb 03 11:05:38 cicabogomem.lpyne10.net systemd[1]: Starting OpenBSD Secure Shell server...
feb 03 11:05:38 cicabogomem.lpyne10.net sshd[4111]: Server listening on 0.0.0.0 port 22.
feb 03 11:05:38 cicabogomem.lpyne10.net sshd[4111]: Server listening on :: port 22.
feb 03 11:05:38 cicabogomem.lpyne10.net systemd[1]: Started OpenBSD Secure Shell server.
root@cicabogomem:/media/sf_cabogomem/aso/herramientas_centos# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:49:fc:b7 brd ff:ff:ff:ff:ff:ff
    inet 172.30.2.22/24 brd 172.30.2.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe49:fc:b7/64 scope link
        valid_lft forever preferred_lft forever
root@cicabogomem:/media/sf_cabogomem/aso/herramientas_centos#
```

```
[root@cicabogomem herramientas_centos]# ssh root@172.30.2.22
The authenticity of host '172.30.2.22 (172.30.2.22)' can't be established.
ECDSA key fingerprint is SHA256:Xow7q4mWVYH8:PCDeH+T0NLYHFDLSnPA/Vgaliq.
ECDSA key fingerprint is MD5:b9:f3:be:5c:1a:ed:b1:86:74:db:fa:88:b2:b7:8e:ab.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '172.30.2.22' (ECDSA) to the list of known hosts.
root@172.30.2.22's password:
Permission denied, please try again.
root@172.30.2.22's password:
^C
[root@cicabogomem herramientas_centos]# ssh administrador@172.30.2.22
administrador@172.30.2.22's password:
Welcome to Ubuntu 20.04.3 LTS (GNU/Linux 5.15.0-101-generic x86_64)

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

Se pueden aplicar 495 actualizaciones de forma inmediata.
390 de estas son actualizaciones de seguridad estándares.
Para ver estas actualizaciones adicionales, ejecute: apt list --upgradable

Your Hardware Enablement Stack (HWE) is supported until April 2025.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

administrador@cicabogomem:~$
```

Ahora comprobaremos que podemos conectarnos de manera automatizada sin que la contraseña esté en el scripting para más seguridad.

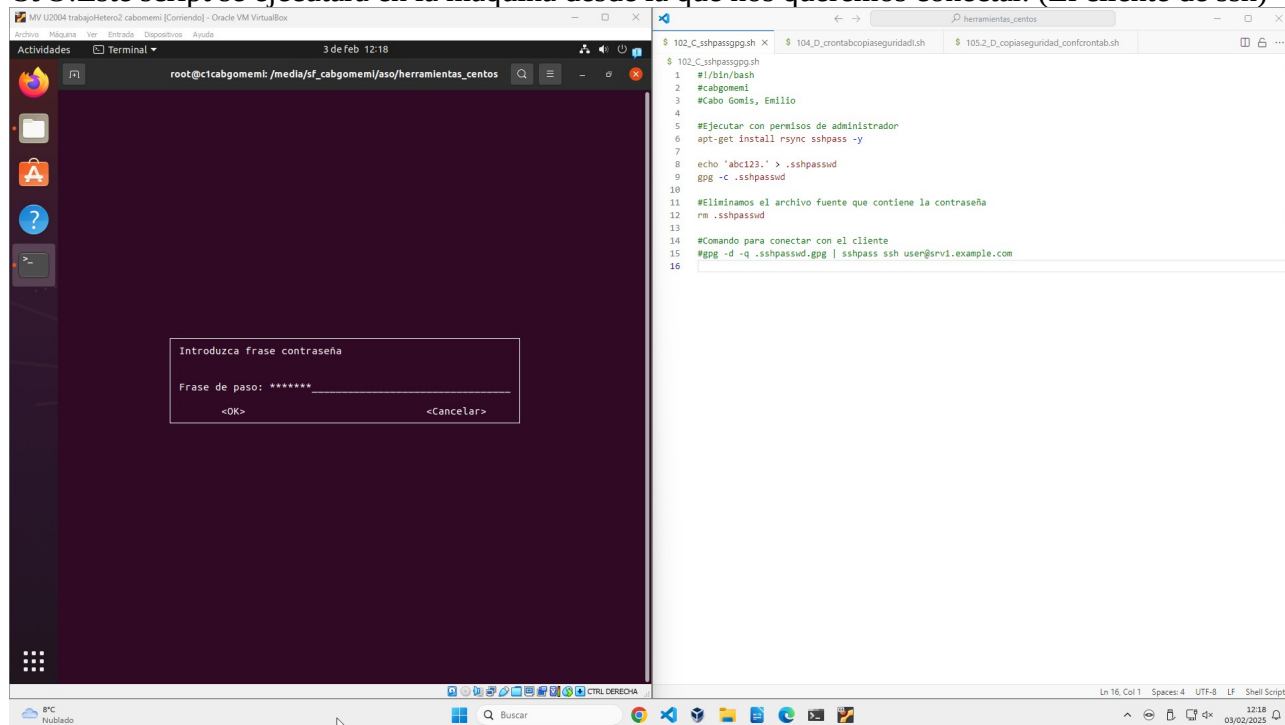
Para ello emplearemos el método sshpass con seguridad aumentada gpg.

En el caso del servidor Centos7 la paquetería viene incluida por defecto; en caso de que estéis empleando otra distribución es probable que tengáis que implementar otra solución.

Contenido del script según documentación RHEL

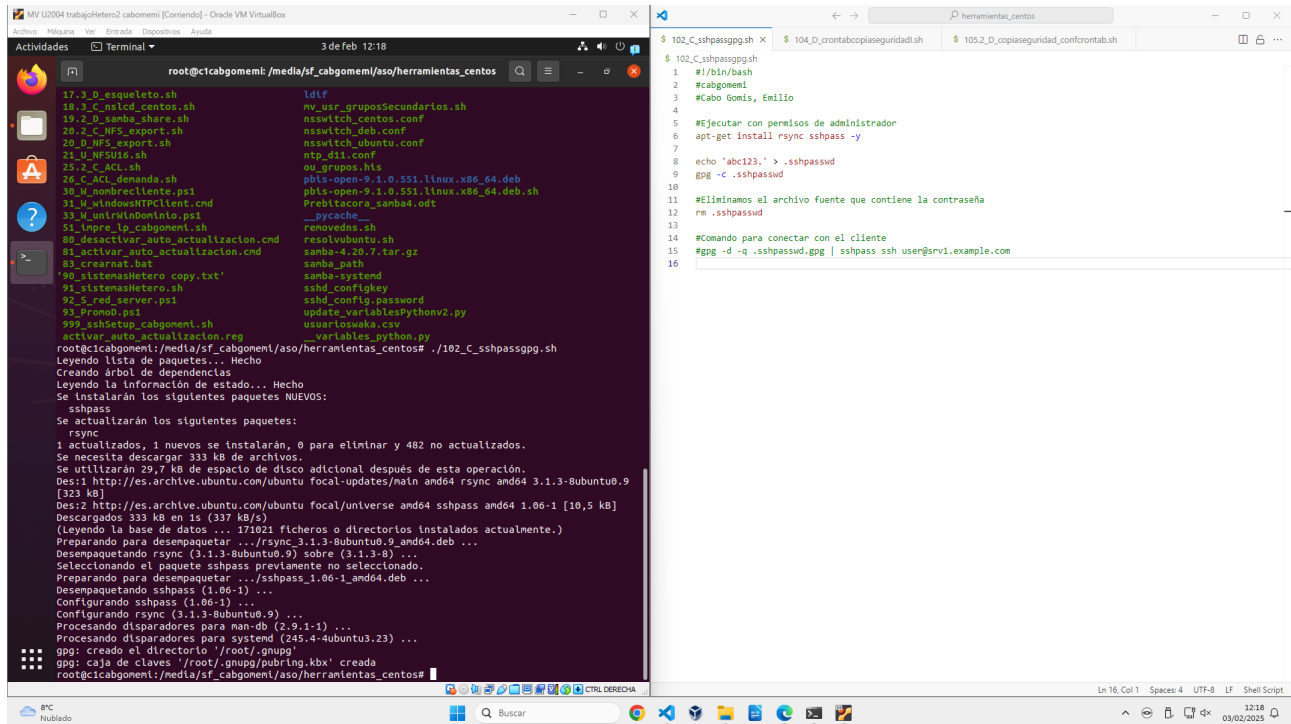
Este es el contenido y la ejecución del script para conectar el equipo mediante una forma segura.

OJO: Este script se ejecutará en la máquina desde la que nos queremos conectar. (El cliente de ssh)



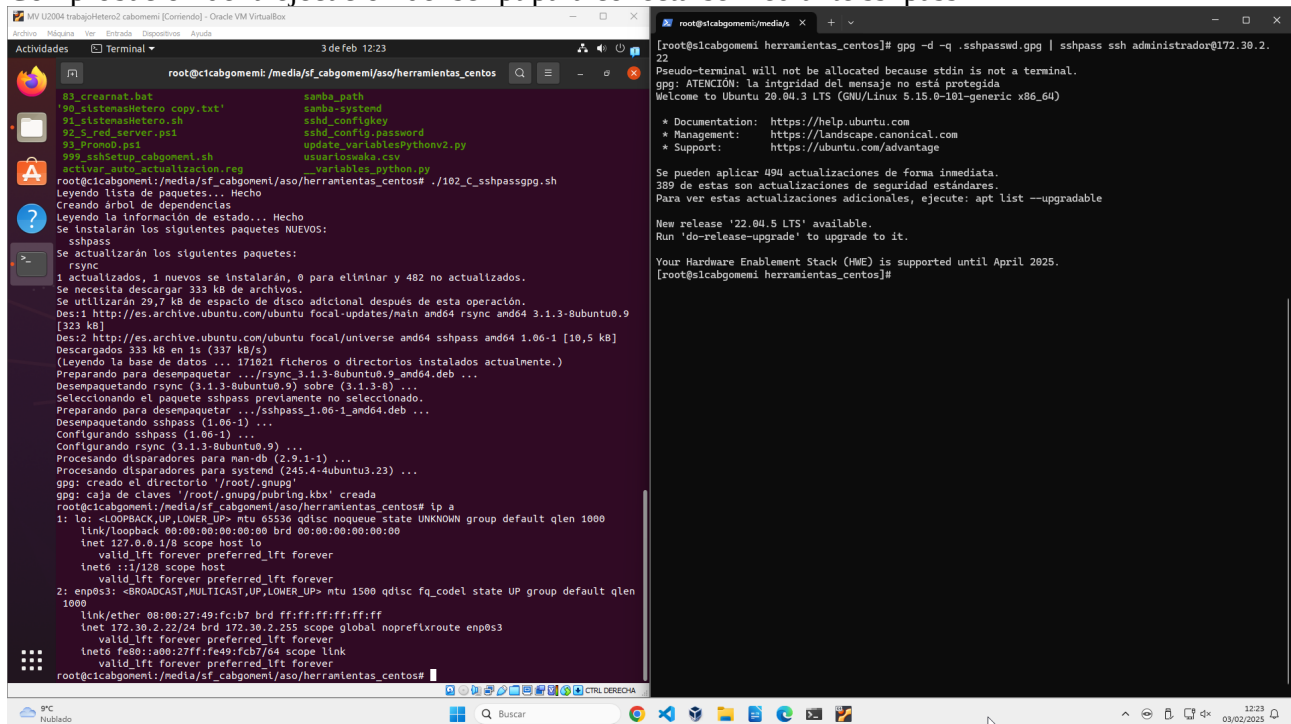
Cómo en mi caso me conectaré desde las dos máquinas en el examen implementaré este script tanto en la máquina centos cómo ubuntu.

Pantalla 2



```
root@icabgonemi:/media/sf_cabgonemi/aso/herramientas_centos# ./102_C_sshpasspgg.sh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  sshpass
Se actualizarán los siguientes paquetes:
  rsync
1 actualizados, 1 nuevos se instalarán, 0 para eliminar y 482 no actualizados.
Se necesita descargar 333 kB de archivos.
Se utilizarán 29,7 kB de espacio de disco adicional después de esta operación.
Des1: http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 rsync amd64 3.1.3-8ubuntu0.9 [323 kB]
Des2: http://es.archive.ubuntu.com/ubuntu focal/universe amd64 sshpass amd64 1.06-1 [10,5 kB]
Descargados 333 kB en 1s (337 kB/s)
(Leyendo la base de datos ... 171021 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../rsync.3.1.3-8ubuntu0.9.amd64.deb ...
Desempaquetando rsync (3.1.3-8ubuntu0.9) sobre (3.1.3-8) ...
Seleccionando el paquete sshpass previamente no seleccionado.
Preparando para desempaquetar .../sshpass.1.06-1.amd64.deb ...
Desempaquetando sshpass (1.06-1) ...
Configurando sshpass (1.06-1) ...
Configurando rsync (3.1.3-8ubuntu0.9) ...
Procesando disparadores para man-db (2.9.1-1) ...
Procesando disparadores para systemd (245.4-4ubuntu3.23) ...
gpg: creado el directorio '/root/.gnupg'
gpg: caja de claves '/root/.gnupg/pubring.kbx' creada
root@icabgonemi:/media/sf_cabgonemi/aso/herramientas_centos#
```

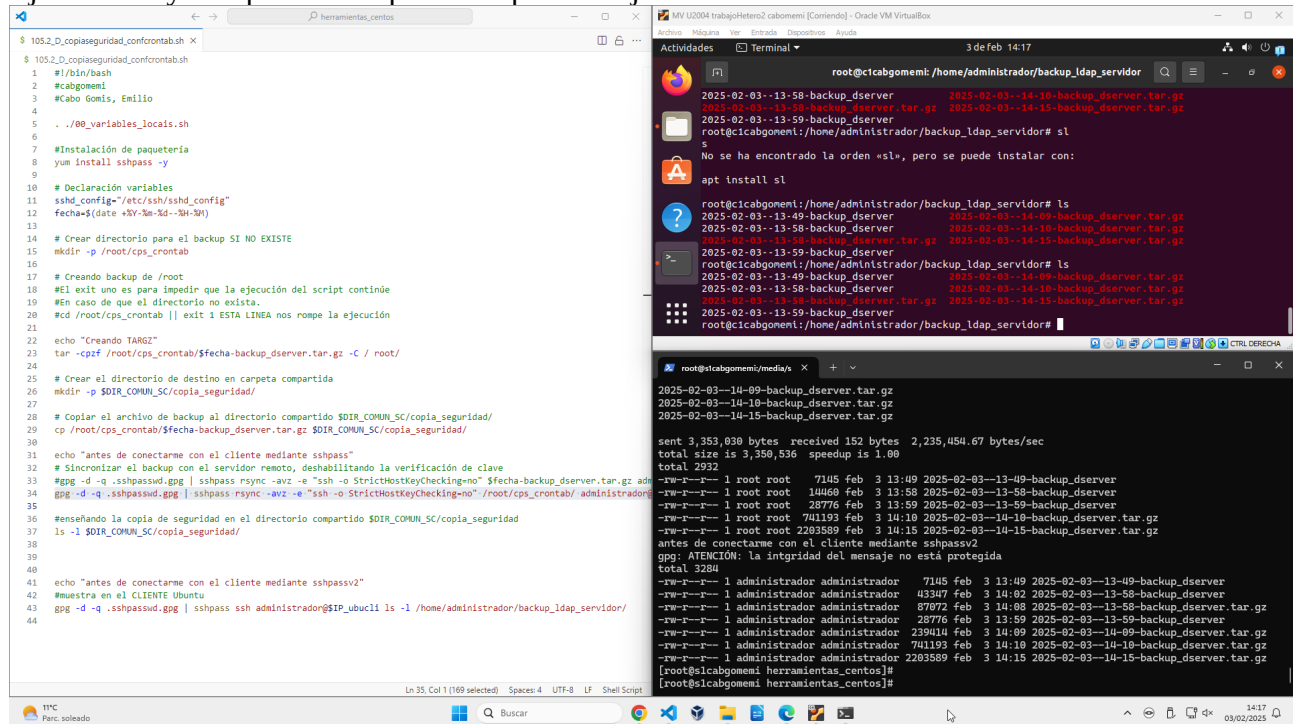
Comprobación de la ejecución del script para conectarse mediante sshpass



```
root@icabgonemi:/media/sf_cabgonemi/aso/herramientas_centos# ./102_C_sshpasspgg.sh
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  sshpass
Se actualizarán los siguientes paquetes:
  rsync
1 actualizados, 1 nuevos se instalarán, 0 para eliminar y 482 no actualizados.
Se necesita descargar 333 kB de archivos.
Se utilizarán 29,7 kB de espacio de disco adicional después de esta operación.
Des1: http://es.archive.ubuntu.com/ubuntu focal-updates/main amd64 rsync amd64 3.1.3-8ubuntu0.9 [323 kB]
Des2: http://es.archive.ubuntu.com/ubuntu focal/universe amd64 sshpass amd64 1.06-1 [10,5 kB]
Descargados 333 kB en 1s (337 kB/s)
(Leyendo la base de datos ... 171021 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../rsync.3.1.3-8ubuntu0.9.amd64.deb ...
Desempaquetando rsync (3.1.3-8ubuntu0.9) sobre (3.1.3-8) ...
Seleccionando el paquete sshpass previamente no seleccionado.
Preparando para desempaquetar .../sshpass.1.06-1.amd64.deb ...
Desempaquetando sshpass (1.06-1) ...
Configurando sshpass (1.06-1) ...
Configurando rsync (3.1.3-8ubuntu0.9) ...
Procesando disparadores para man-db (2.9.1-1) ...
Procesando disparadores para systemd (245.4-4ubuntu3.23) ...
gpg: creado el directorio '/root/.gnupg'
gpg: caja de claves '/root/.gnupg/pubring.kbx' creada
root@icabgonemi:/media/sf_cabgonemi/aso/herramientas_centos# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:49:fc:b7 brd ff:ff:ff:ff:ff:ff
    inet 172.30.2.22/24 brd 172.30.2.255 scope global noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe49:fc:b7/64 scope link
        valid_lft forever preferred_lft forever
root@icabgonemi:/media/sf_cabgonemi/aso/herramientas_centos#
```

Implementación en el scripting de rysnc

Ejecutamos y comprobamos que el script se ha ejecutado correctamente



```
$ 105.2_D_copiaseguridad_confrontab.sh
1 #!/bin/bash
2 #cabgomem
3 #Cabo Gomis, Emilio
4
5 # Configuración de variables
6
7 # Instalación de paquetería
8 yum install sshpass -y
9
10 # Declaración variables
11 sshd_config="/etc/ssh/sshd_config"
12 fecha=$(date +%Y-%m-%d-%H-%M)
13
14 # Crear directorio para el backup SI NO EXISTE
15 mkdir -p /root/cps_crontab
16
17 # Creando backup de /root
18 # El exit uno es para impedir que la ejecución del script continúe
19 # En caso de que el directorio no exista.
20 # cd /root/cps_crontab || exit 1 ESTA LINEA nos rompe la ejecución
21
22 echo "Creando TAR.GZ"
23 tar -cpzf /root/cps_crontab/$fecha-backup_dserver.tar.gz -C / root/
24
25 # Crear el directorio de destino en carpeta compartida
26 mkdir -p $DIR_COMUN_SC/copia_seguridad/
27
28 # Copiar el archivo de backup al directorio compartido $DIR_COMUN_SC/copia_seguridad/
29 cp /root/cps_crontab/$fecha-backup_dserver.tar.gz $DIR_COMUN_SC/copia_seguridad/
30
31 echo "antes de conectarme con el cliente mediante sshpass"
32 # Sincronizar el backup con el servidor remoto, deshabilitando la verificación de clave
33 # gpg -d -q .sshpasswd.gpg | sshpass rsync -avz -e "ssh -o StrictHostKeyChecking=no" $fecha-backup_dserver.tar.gz admin@192.168.1.100
34 # gpg -d -q .sshpasswd.gpg | sshpass rsync -avz -e "ssh -o StrictHostKeyChecking=no" /root/cps_crontab/ administrador@192.168.1.100
35
36 # Enseñando la copia de seguridad en el directorio compartido $DIR_COMUN_SC/copia_seguridad
37 ls -l $DIR_COMUN_SC/copia_seguridad/
38
39
40
41 echo "antes de conectarme con el cliente mediante sshpassv2"
42 # muestra en el CLIENTE Ubuntu
43 gpg -d -q .sshpassv2.gpg | sshpass ssh administrador@192.168.1.100 ls -l /home/administrador/backup_ldap_servidor/
44
```

```
root@icabgomem:/home/administrador/backup_ldap_servidor# ls
2025-02-03-13-58-backup_dserver 2025-02-03-14-10-backup_dserver.tar.gz
2025-02-03-13-58-backup_dserver 2025-02-03-14-15-backup_dserver.tar.gz
root@icabgomem:/home/administrador/backup_ldap_servidor# ls
2025-02-03-13-58-backup_dserver 2025-02-03-14-10-backup_dserver.tar.gz
2025-02-03-13-58-backup_dserver 2025-02-03-14-15-backup_dserver.tar.gz
root@icabgomem:/home/administrador/backup_ldap_servidor# ls
2025-02-03-13-58-backup_dserver 2025-02-03-14-10-backup_dserver.tar.gz
2025-02-03-13-58-backup_dserver 2025-02-03-14-15-backup_dserver.tar.gz
root@icabgomem:/home/administrador/backup_ldap_servidor#
```

```
sent 3,353,030 bytes received 152 bytes 2,235,454.67 bytes/sec
total size is 3,350,536 speedup is 1.00
total 2932
-rw-r--r-- 1 root root 7145 feb 3 13:49 2025-02-03-13-49-backup_dserver
-rw-r--r-- 1 root root 14469 feb 3 13:58 2025-02-03-13-58-backup_dserver
-rw-r--r-- 1 root root 28776 feb 3 13:59 2025-02-03-13-59-backup_dserver
-rw-r--r-- 1 root root 741193 feb 3 14:10 2025-02-03-14-10-backup_dserver.tar.gz
-rw-r--r-- 1 root root 2283589 feb 3 14:15 2025-02-03-14-15-backup_dserver.tar.gz
antes de conectarme con el cliente mediante sshpassv2
gpg: ATENCIÓN: la integridad del mensaje no está protegida
total 3284
-rw-r--r-- 1 administrador administrador 7145 feb 3 13:49 2025-02-03-13-49-backup_dserver
-rw-r--r-- 1 administrador administrador 43347 feb 3 14:02 2025-02-03-13-58-backup_dserver
-rw-r--r-- 1 administrador administrador 87072 feb 3 14:08 2025-02-03-13-58-backup_dserver.tar.gz
-rw-r--r-- 1 administrador administrador 28776 feb 3 13:59 2025-02-03-13-59-backup_dserver
-rw-r--r-- 1 administrador administrador 239414 feb 3 14:09 2025-02-03-14-09-backup_dserver.tar.gz
-rw-r--r-- 1 administrador administrador 741193 feb 3 14:10 2025-02-03-14-10-backup_dserver.tar.gz
-rw-r--r-- 1 administrador administrador 2283589 feb 3 14:15 2025-02-03-14-15-backup_dserver.tar.gz
[root@icabgomem herramientas_centos]#
[root@icabgomem herramientas_centos]#
```

PRACTICA FINALIZADA