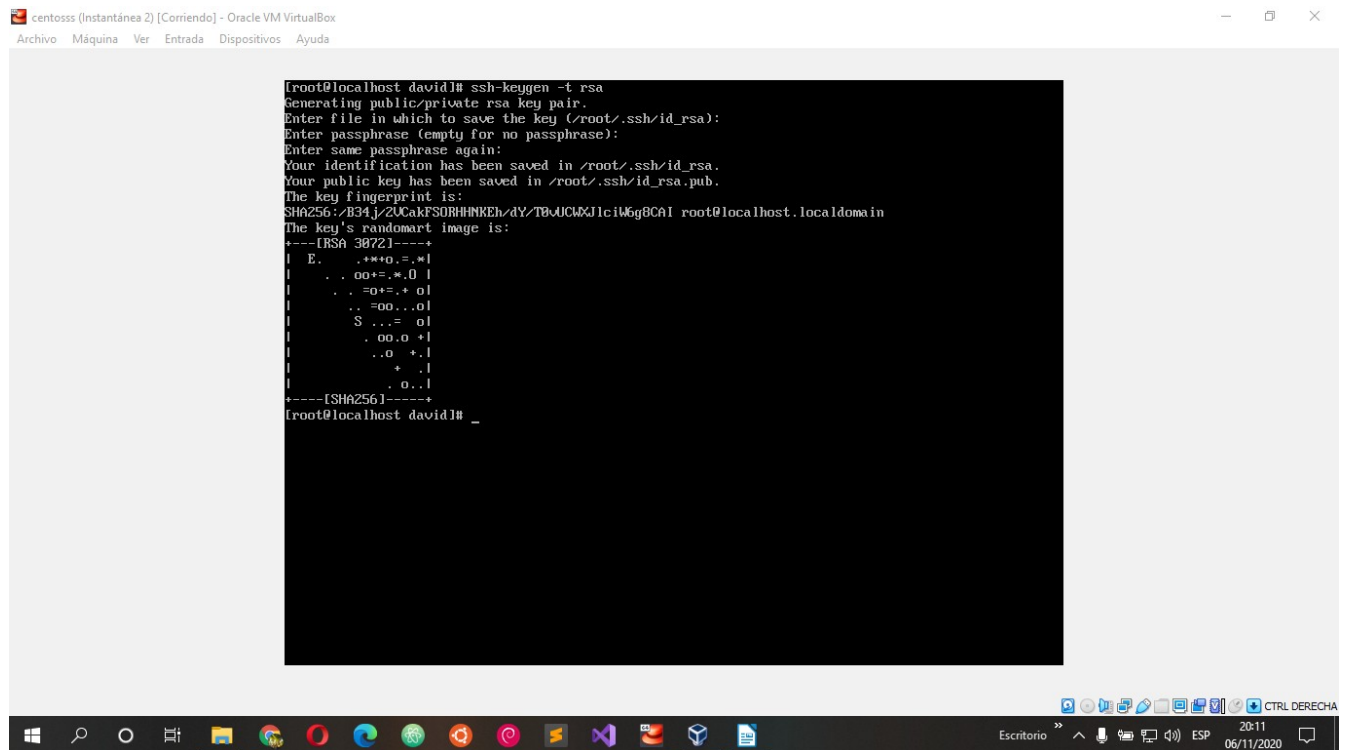


1. Generación de claves en el servidor de Centos.

En la máquina servidor vamos a generar la clave pública y privada. Para ello usamos el siguiente comando:

```
[root@localhost ~]# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:11nM68WlnJUJaHpalqkpq84FEsh7yusJ8U1M1e4UjGg root@localhost.localdomain
The key's randomart image is:
+---[RSA 3072]-----+
|  . . . o o      . . |
| o. E o o o  o .oo|
| ooo .      .o o .o=|
| o... . . . B + =o|
| ..oo o .S 0 o +.o|
| ..o . o. =      . .|
| .o      .o      . |
| . o . . .      |
| .+ .+.      |
+-----[SHA256]-----+
[root@localhost ~]# cd /root/.ssh/
[root@localhost .ssh]# ls
id_rsa  id_rsa.pub
[root@localhost .ssh]#
```

Como Podemos ver se ha generado en /root/.ssh la contraseña publica: id_rsa.pub y la privada id_rsa



```
centos8s (Instantánea 2) [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda

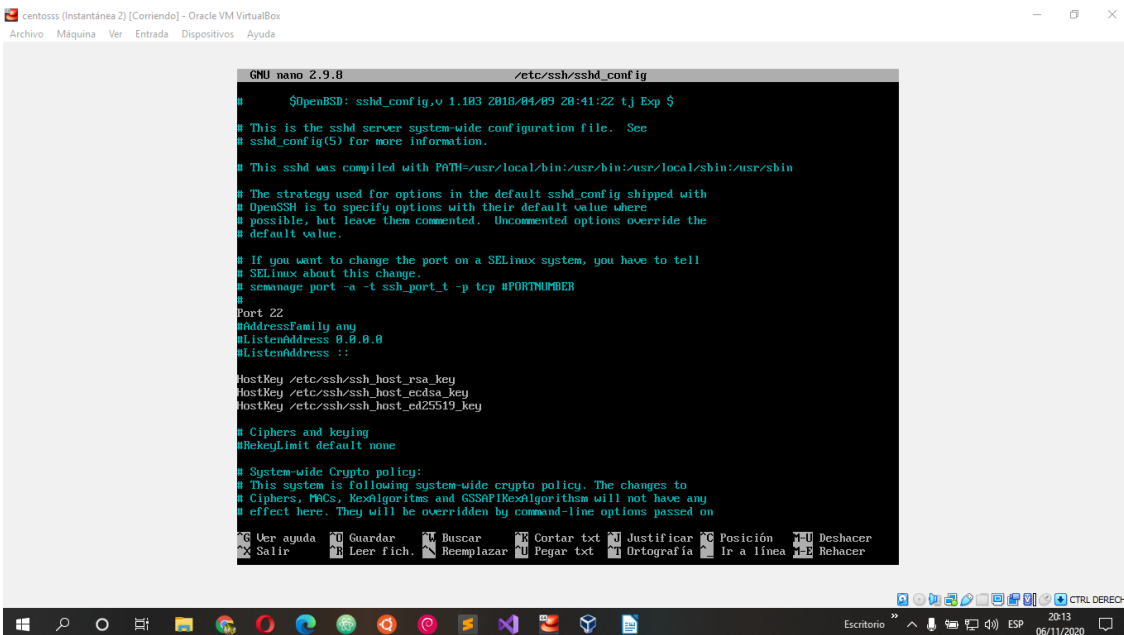
root@localhost davidl# ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:/B34j/2UCakFSORHhNKEh/4Y/TB4JCWdJlciW6g8CAI root@localhost.localdomain
The key's randomart image is:
+--[RSA 3072]-----+
| E..+*+o.=.*+|
|..+oo+*.o.l|
|..+o+*.+o.l|
|..+oo...o.l|
|S...= o.l|
|.oo.o +l|
|..o +.l|
|..+ .l|
|..o..l|
+-----[SHA256]-----+
root@localhost davidl#
```

2. Cambio en la configuración de SSH

Editamos el fichero: `/etc/ssh/sshd_config` y vamos a habilitar que solo se puedan logar usando un certificado para ello ponemos el parámetro:

PasswordAuthentication no

Reiniciamos el servicio.



```
GNU nano 2.9.0 /etc/ssh/sshd_config
# OpenSSH: sshd_config.v 1.103 2018/04/09 20:41:22 t.j Exp $
# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.
# This sshd was compiled with PATH=/usr/local/bin:/usr/bin:/usr/local/sbin:/usr/sbin
# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.
# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
# Ciphers and keying
#RekeyLimit default none
# System-wide Crypto policy:
# This system is following system-wide crypto policy. The changes to
# Ciphers, MACs, KexAlgorithms and GSSAPIKexAlgorithm will not have any
# effect here. They will be overridden by command-line options passed on
Ver ayuda Guardar Buscar Cortar txt Justificar Posición Deshacer
Salir Leer fich. Reemplazar Pegar txt Ortografía Ir a línea Rehacer
```

centos8 (Instantánea 2) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 2.9.8 /etc/ssh/sshd_config

# the server start up.
# To opt out, uncomment a line with redefinition of CRYPTO_POLICY=
# variable in /etc/sysconfig/ssh to override the policy.
# For more information, see manual page for update-crypto-policies(8).

# Logging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for

Uer ayuda Guardar Buscar Cortar txt Justificar Posición Deshacer
Salir Leer fich. Reemplazar Pegar txt Ortografía Ir a línea Rehacer
```

Escritorio 20:13 06/11/2020

centos8 (Instantánea 2) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
GNU nano 2.9.8 /etc/ssh/sshd_config

#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

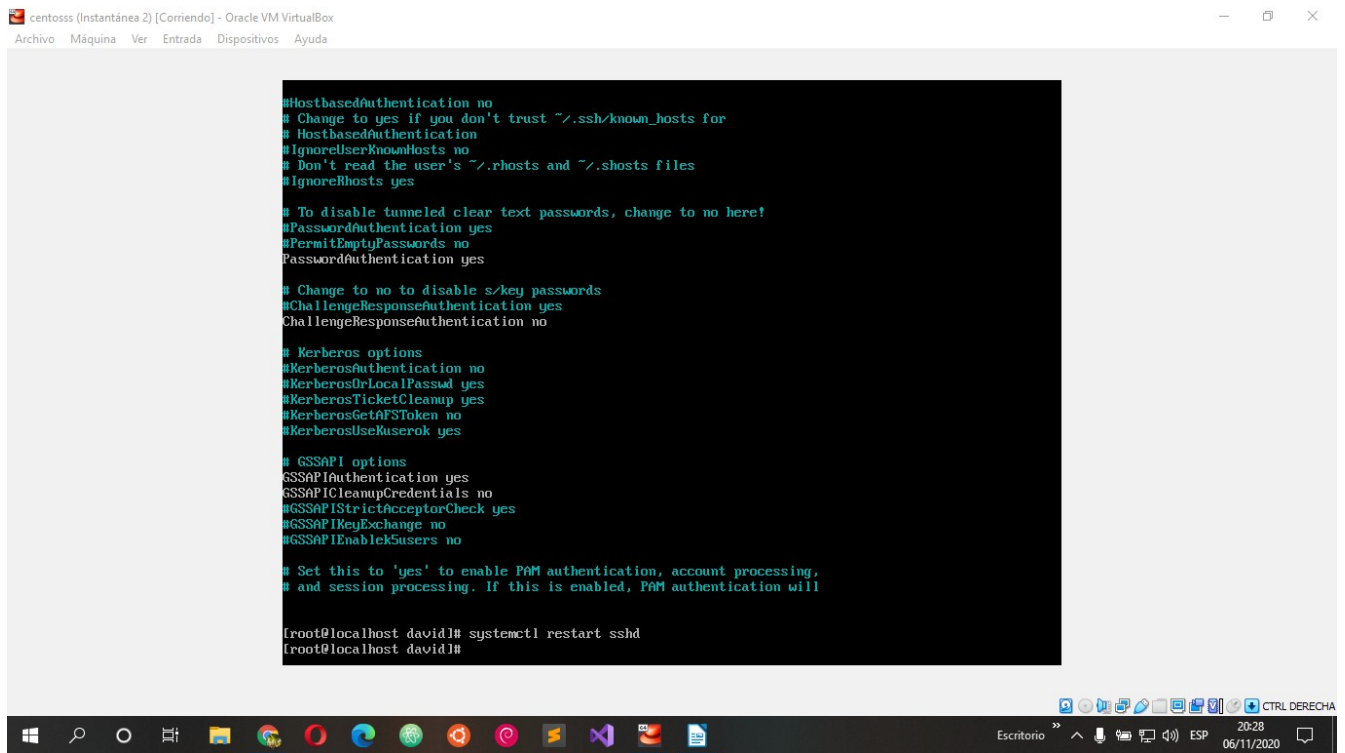
# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
#GSSAPIEnableK5users no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will

Uer ayuda Guardar Buscar Cortar txt Justificar Posición Deshacer
Salir Leer fich. Reemplazar Pegar txt Ortografía Ir a línea Rehacer
```

Escritorio 20:28 06/11/2020



centosss (Instantánea 2) [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

```
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

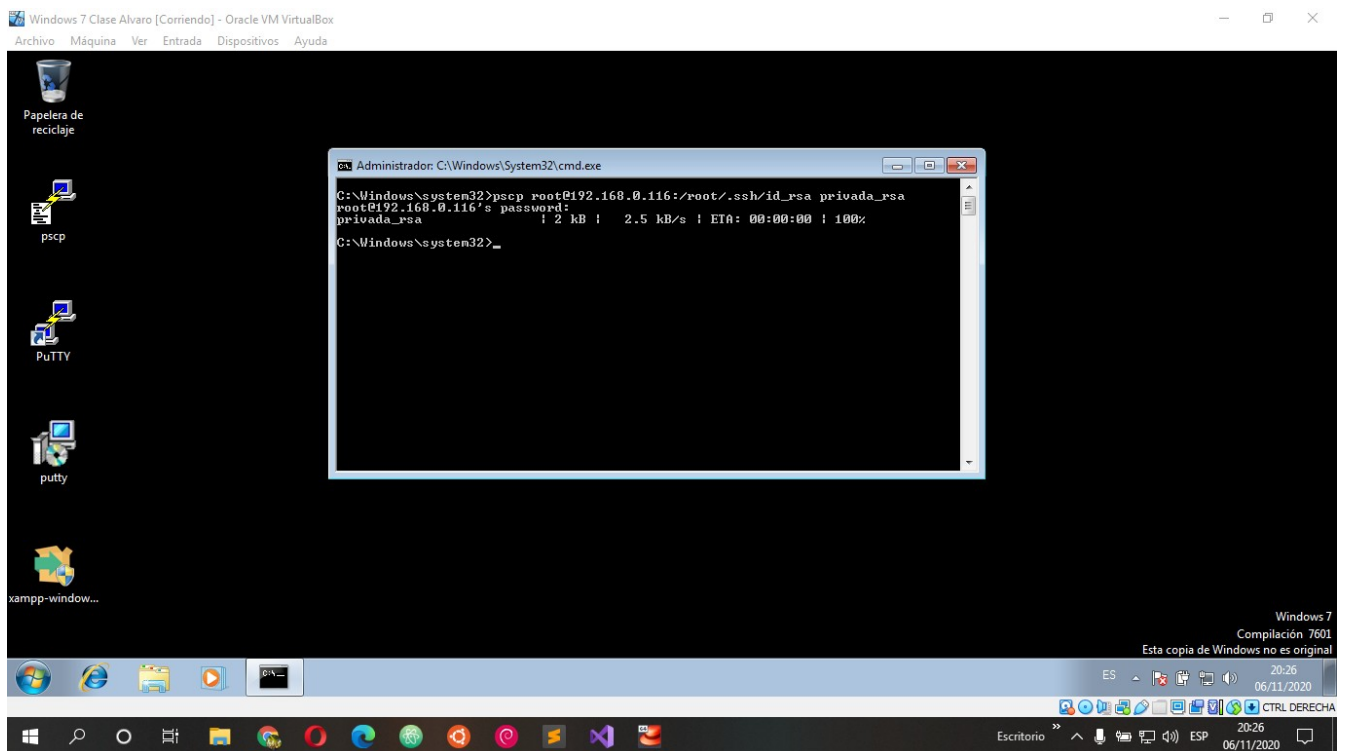
# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
#GSSAPIEnableK5users no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will

[root@localhost david]# systemctl restart sshd
[root@localhost david]#
```

Escritorio 20:28 06/11/2020

3. Ahora vamos a copiar la contraseña privada al cliente en Windows usando el comando pscp



Windows 7 Clase Alvaro [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Papelera de reciclaje

pscp

PuTTY

putty

xampp-window...

```
C:\Windows\system32>pscp root@192.168.0.116:/root/.ssh/id_rsa privada_rsa
root@192.168.0.116's password:
privada_rsa      1 2 kB | 2.5 kB/s | ETA: 00:00:00 | 100%

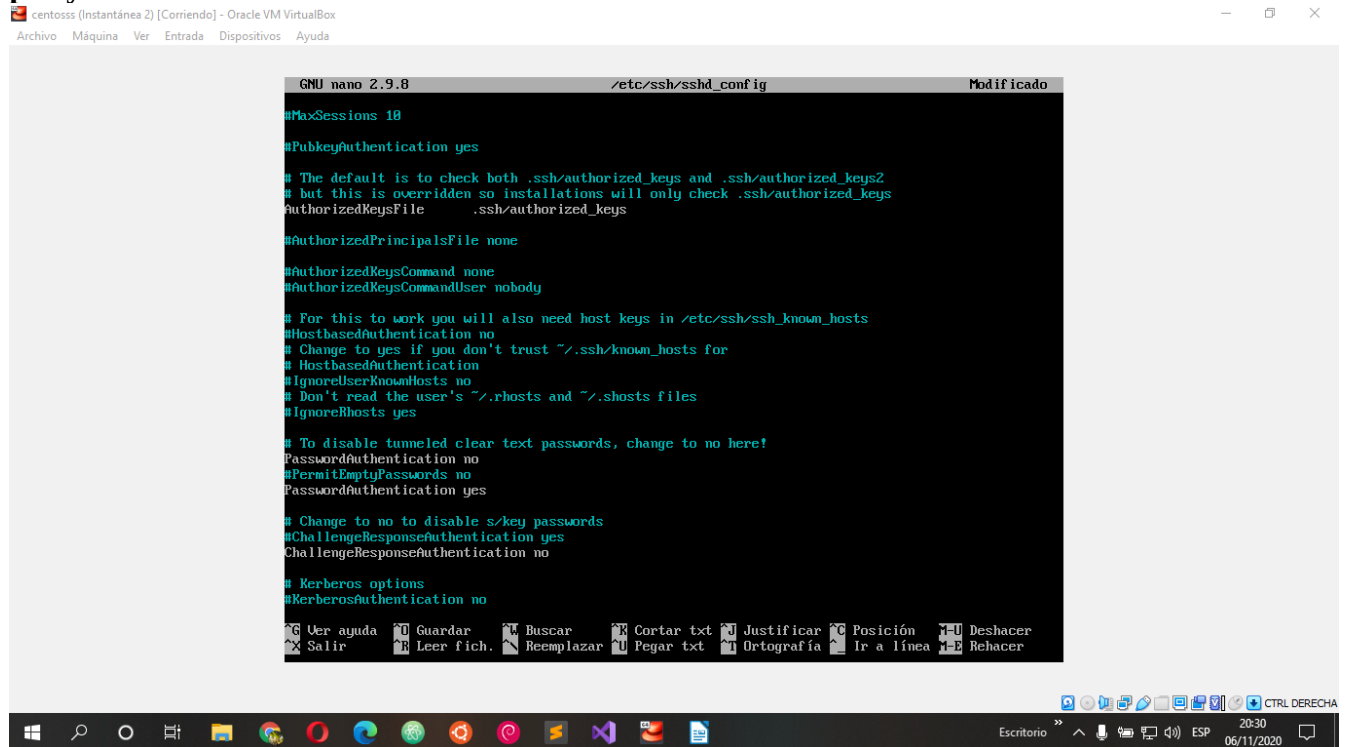
C:\Windows\system32>_
```

Windows 7
Compilación 7601
Esta copia de Windows no es original

ES 20:26 06/11/2020

Escritorio 20:26 06/11/2020

4. Convertimos el certificado usando el puTTYGen a un certificado en formato válido para putty.



The screenshot shows a terminal window titled "centosss (Instantánea 2) [Corriendo] - Oracle VM VirtualBox". The terminal is running the GNU nano 2.9.8 editor, editing the file /etc/ssh/sshd_config. The configuration file content is as follows:

```
GNU nano 2.9.8 /etc/ssh/sshd_config Modificado

#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

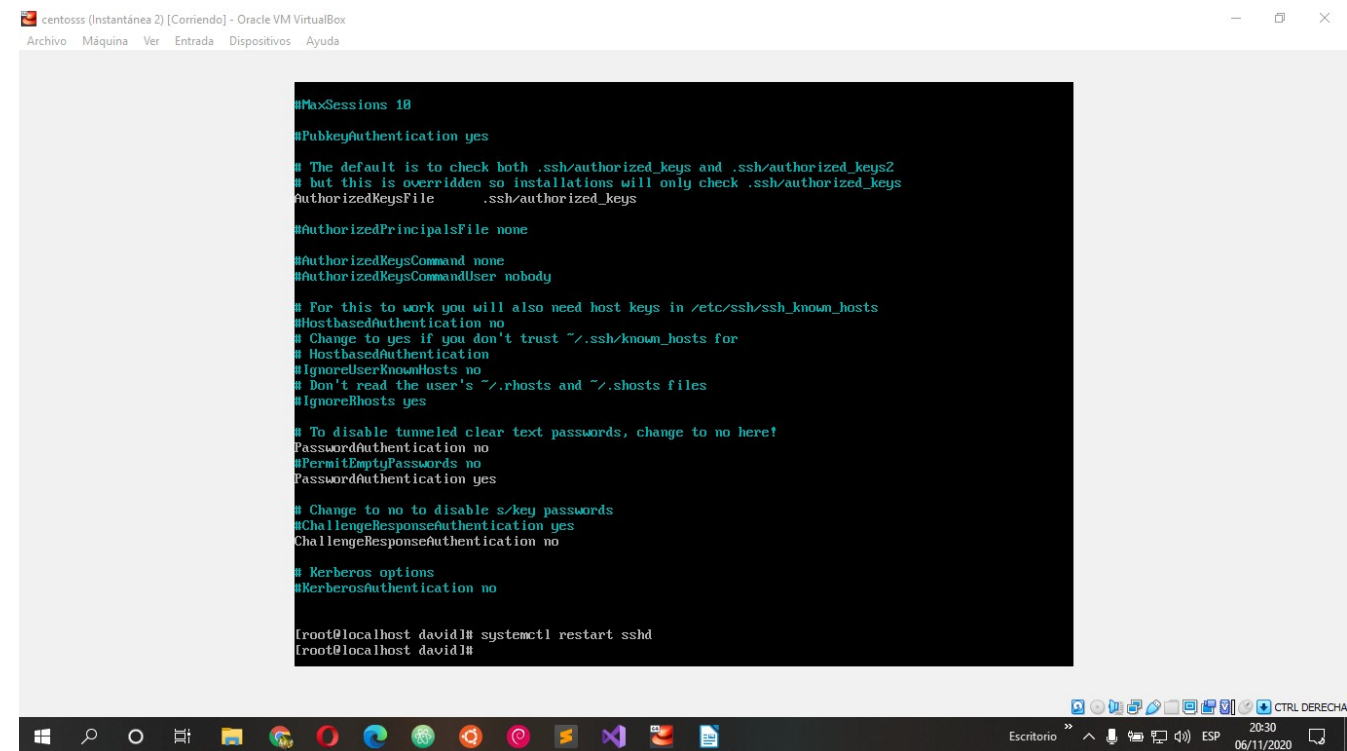
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no

Uer ayuda Guardar Buscar Cortar txt Justificar Posición Deshacer
Salir Leer fich. Reemplazar Pegar txt Ortografia Ir a línea Rehacer
```



The screenshot shows the same terminal window as above, but now the configuration file has been saved and the sshd service is being restarted. The terminal output is as follows:

```
GNU nano 2.9.8 /etc/ssh/sshd_config Modificado

#MaxSessions 10

#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile .ssh/authorized_keys

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

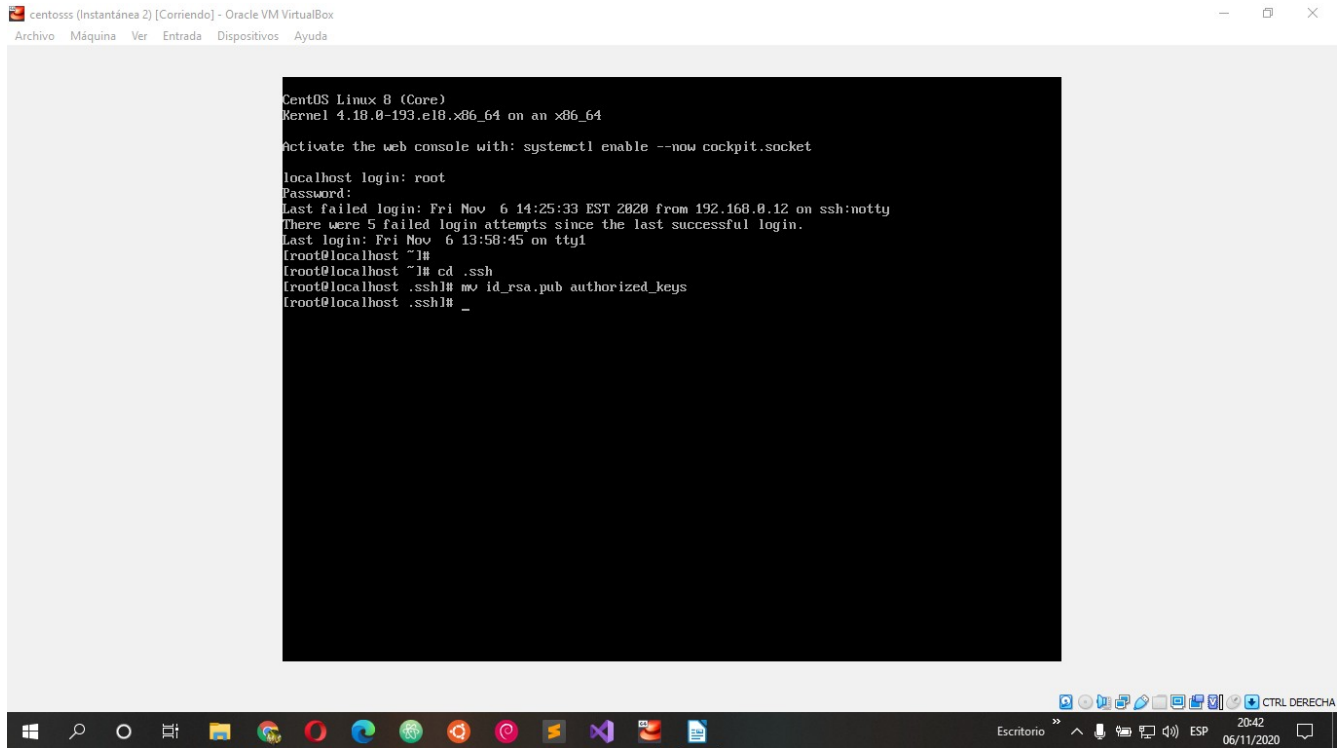
# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
PasswordAuthentication no
#PermitEmptyPasswords no
PasswordAuthentication yes

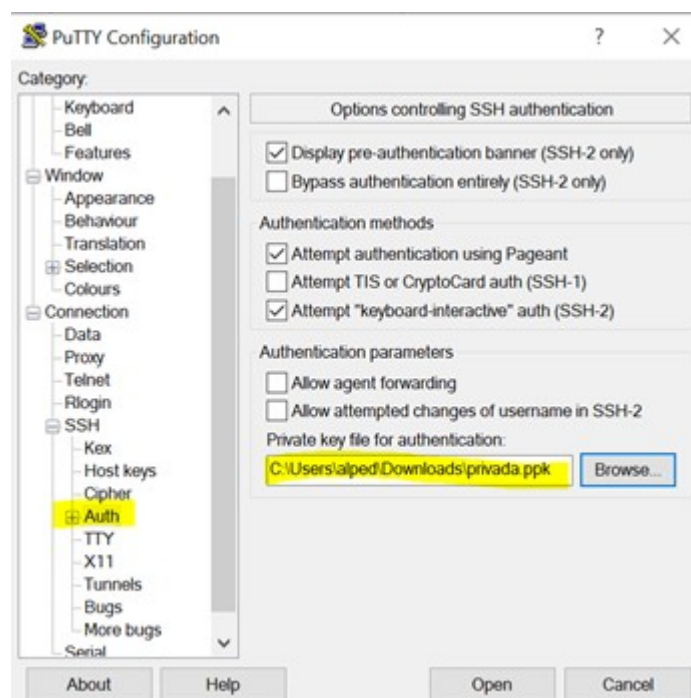
# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

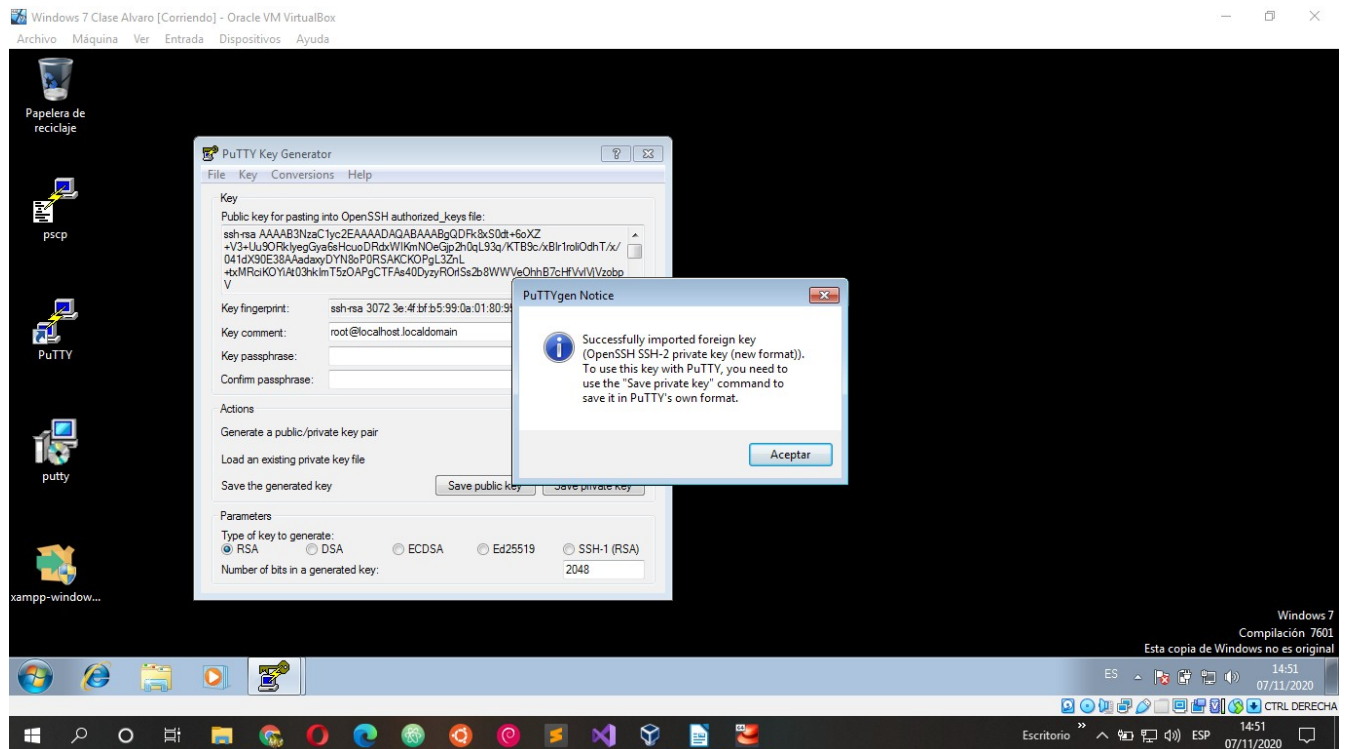
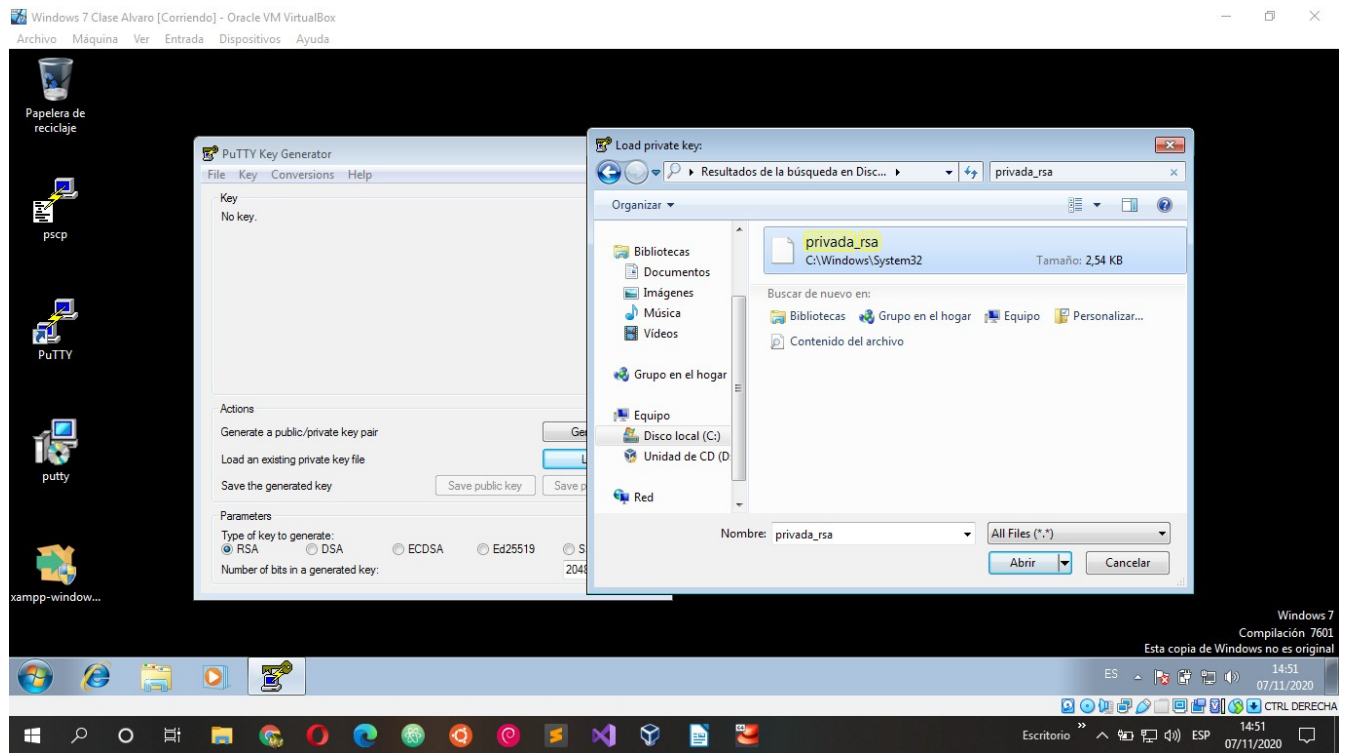
# Kerberos options
#KerberosAuthentication no

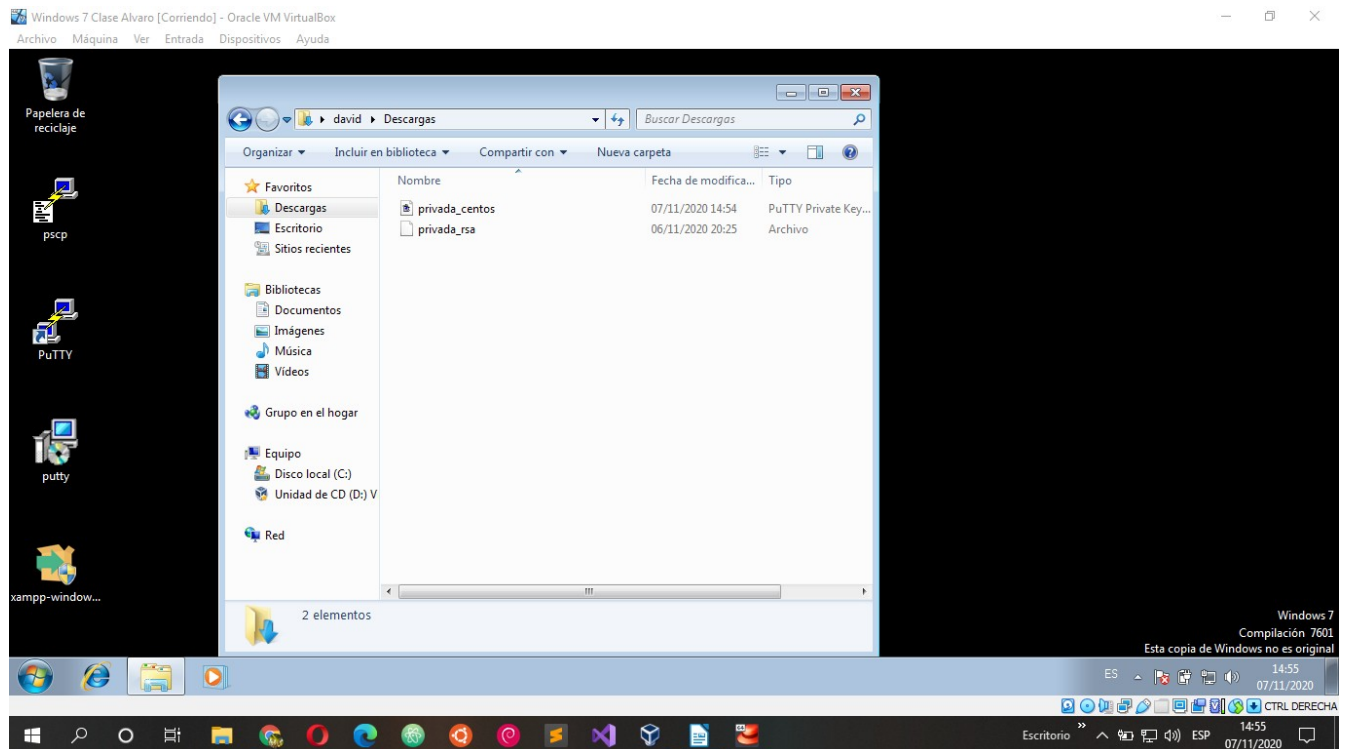
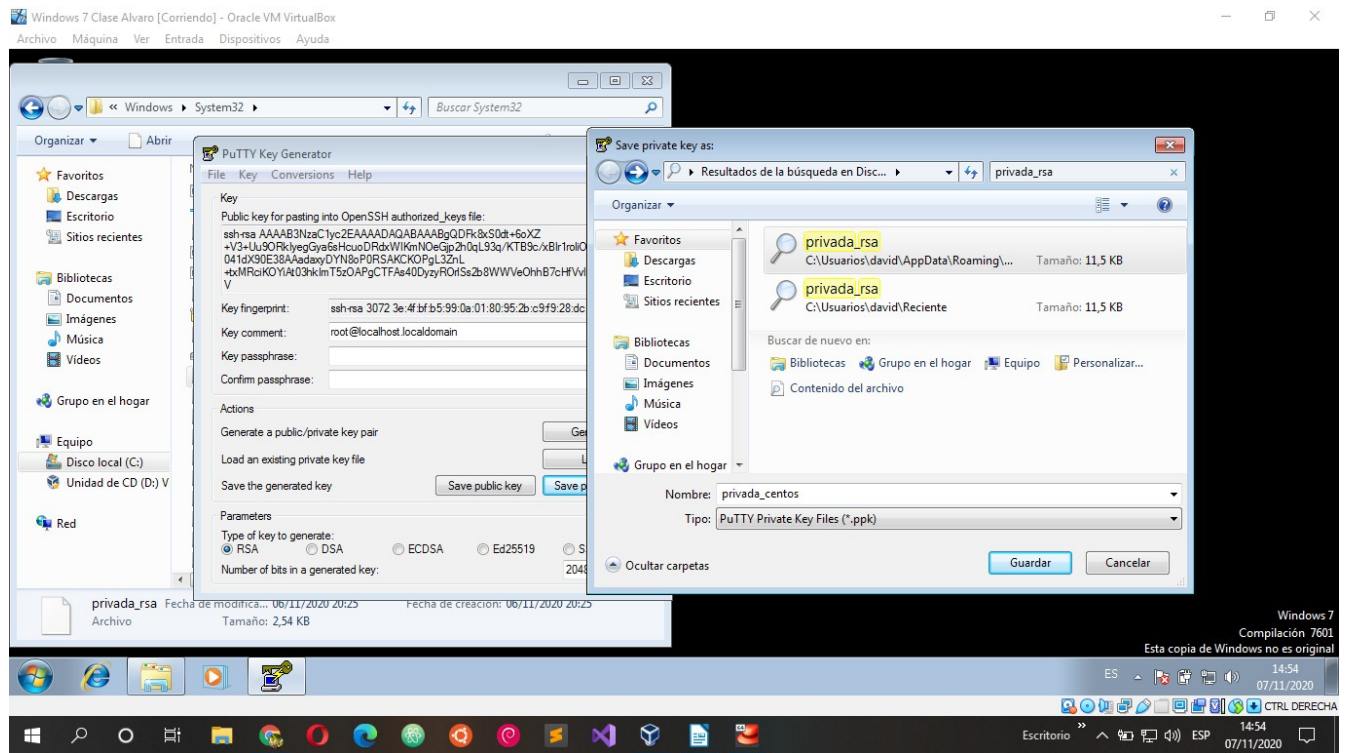
[root@localhost david]# systemctl restart sshd
[root@localhost david]#
```



5. Arrancamos el putty y ponemos los datos del cliente. Además especificamos donde está el certificado privado.







6. Probamos que accedemos al servidor SSH sin necesidad de contraseña.

