Manual de acceso al servicio de máquina virtual alojada en el SCI

En general, las máquinas ofrecidas a través de este servicio se entregan con un sistema operativo correspondiente a alguna distribución de Linux (normalmente CentOS). El acceso que se da a estas máquinas es a su usuario de administración 'root'.

El método de acceso que se establece para el control de este tipo de máquinas es mediante el uso del protocolo SSH en la modalidad de autenticación por clave pública.

Este mecanismo es más seguro que el tradicional (consistente en un nombre usuario y una clave) pero requiere de un esfuerzo adicional de configuración.

Es requisito indispensable para utilizar esta forma de acceso el disponer de una pareja de claves pública/privada y que deben ser generadas por cada usuario que vaya a acceder a la máquina. De esta pareja de claves deben proporcionar al SCI la pública, necesaria para configurarla en la máquina a la que se quiere acceder. La clave privada la debe tener exclusivamente su dueño.

Existen distintos formatos para estas claves. Nosotros el que usamos es openssh.

Asociados a la pareja de claves existe lo que se llama una '*passphrase*' que es el equivalente a la '*password'* de la identificación tradicional y que se establece en el momento de la generación de la pareja de claves. Dicha '*passphrase'* sirve para activar el uso de las claves para, en este caso, poder conectar a la máquina virtualizada.

La elección de esta 'passphrase' es muy importante y se recomienda que no sea almacenada ni apuntada en ninguna parte. Debe ser conocida exclusivamente por el dueño de las claves pública/privada.

La seguridad añadida por este mecanismo de autenticación consiste en que para que alguien pueda usurpar la identidad del propietario de las claves debe tener acceso a dos elementos que son la clave privada y la '*passphrase'*. Otro elemento de seguridad es que la '*passphrase'* nunca se almacena en ningún dispositivo, sólo se proporciona en el momento de la conexión.

Para poder hacer uso de las claves es necesario conocer la '*passphrase'* por lo que aunque alguien obtuviera los ficheros de claves no podría hacer uso de ellos sin conocerla. Además, la obtención de la '*passphrase'* a partir de los ficheros no es viable con la potencia de cálculo de los ordenadores actuales.

Es importante indicar que la pérdida del fichero de la clave privada o el olvido de la '*passphrase'* implica la necesidad de repetir nuevamente el proceso para generar otro par de claves y que suministren al SCI la nueva clave pública generada.

Generación de la pareja de claves pública/privada

Durante el proceso de generación de claves se le pedirá que escriba la '*passphrase*' y como resultado de completar el proceso se obtendrán dos ficheros que contendrán la claves pública y privada.

Según la plataforma que use, la generación de la pareja de claves se hará de una forma u otra.

- **Unix**

La generación de claves se hace mediante el uso del comando **ssh-keygen**. La sintaxis sería

ssh-keygen –f <nombre_fichero> -b 2048

La ejecución de este comando provoca la generación de los dos ficheros de clave con el <nombre_fichero> especificado.

Las claves se generan en formato openssh. Normalmente el fichero que contiene la clave privada no tiene extensión mientras que el de la pública tiene como extensión '.pub'. Las claves se suelen colocar en un directorio oculto llamado '.ssh' que reside en la carpeta correspondiente al usuario dueño las claves. A nivel del sistema operativo, tanto la carpeta como el fichero de la clave privada debe ser propiedad del usuario. La carpeta debe tener como permisos 700 (drwx------) y el fichero de clave privada 600 (-rw-------).

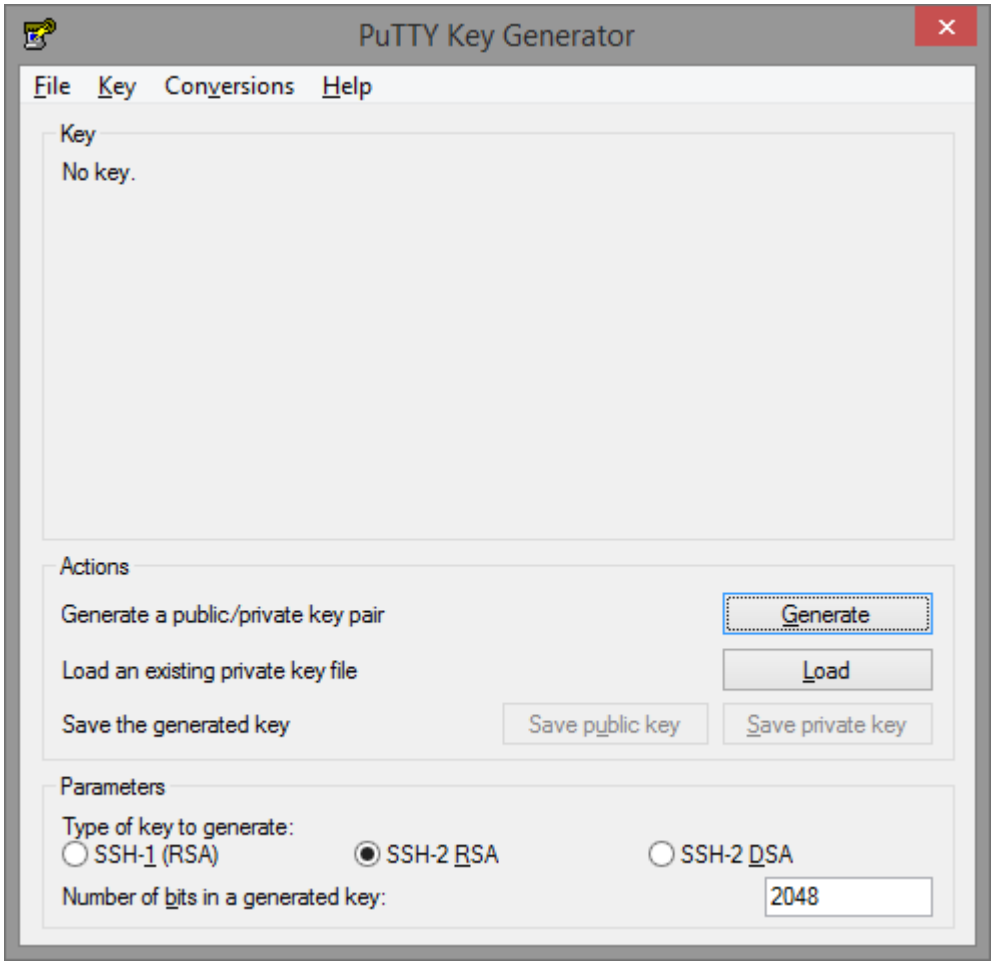
- **Windows**

Para el caso de Windows hay que hacer uso de programas que no vienen con el sistema operativo.

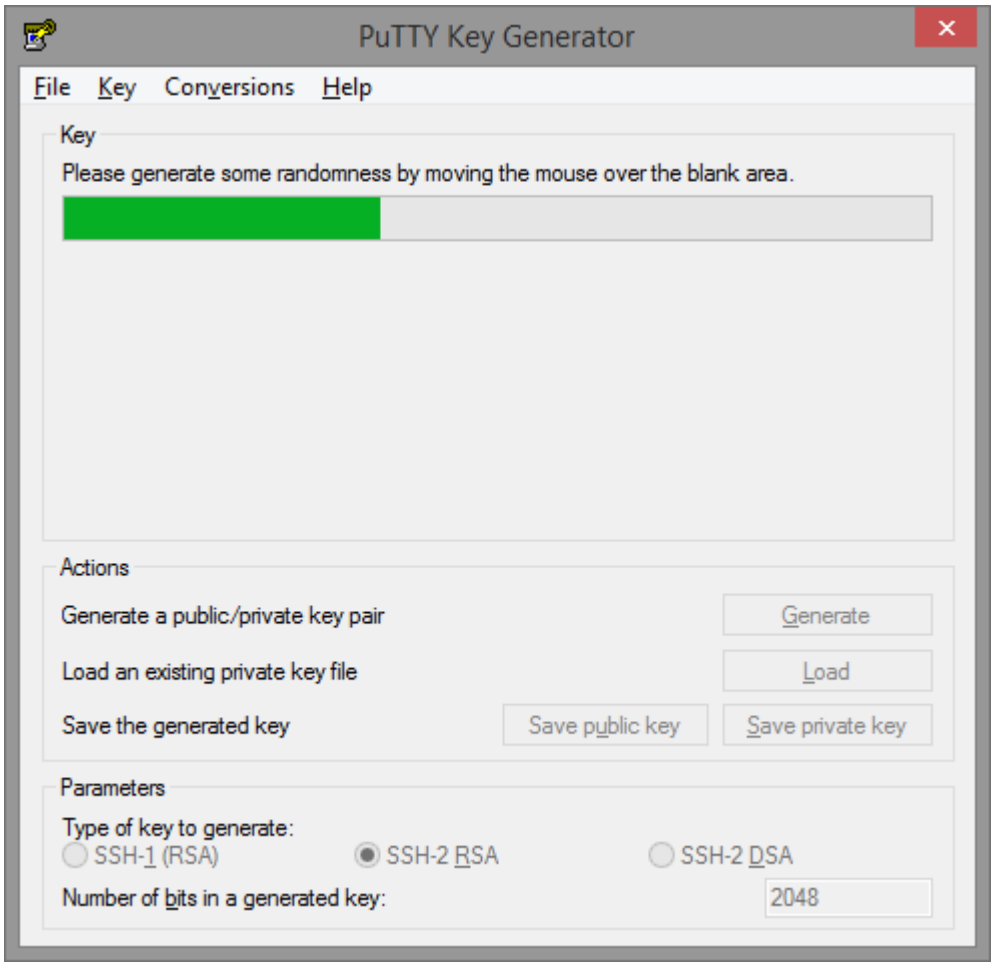
Nosotros recomendamos el uso de **puttygen.exe** para la generación de las claves (puede descargarlo desde http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html).

El proceso a seguir es el siguiente:

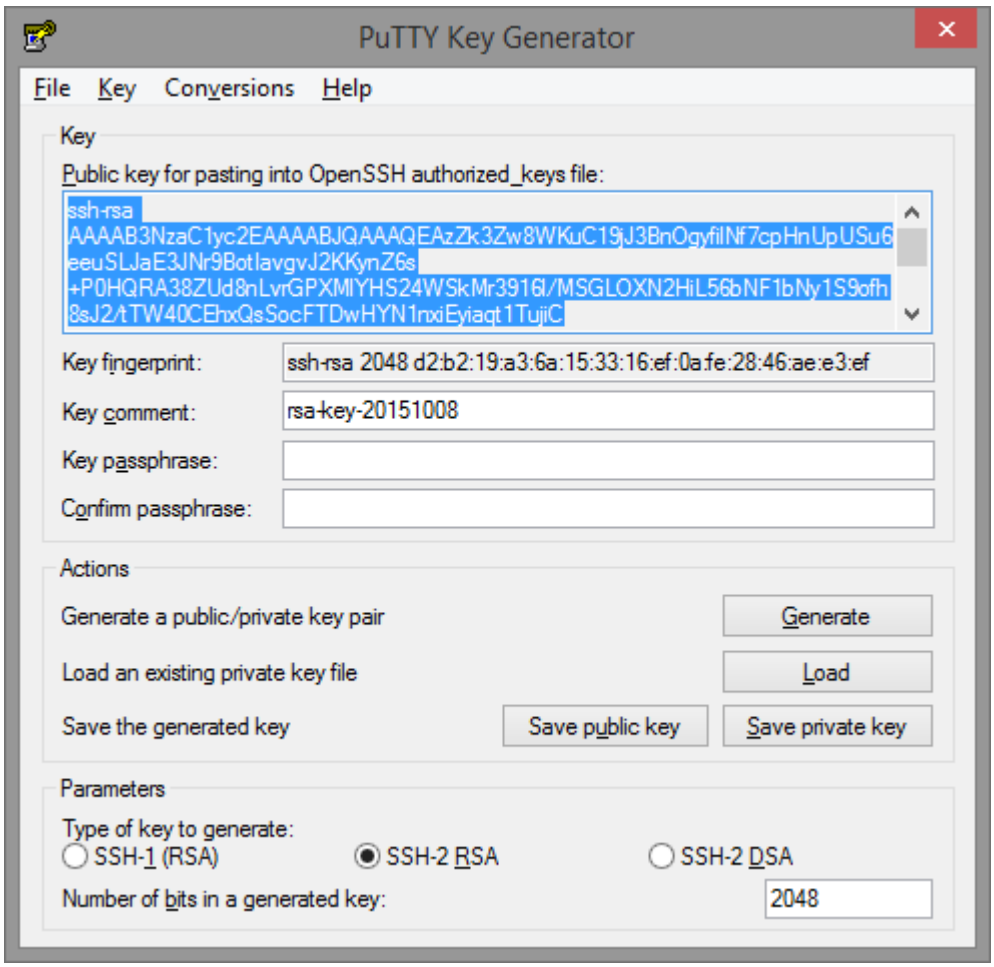
1. Ejecute el programa puttygen.exe y mantenga las opciones que ya vienen seleccionadas por defecto (SSH-2 RSA y 2048 bits)



2. Pulse el botón ‘Generate’. Se le pedirá que mueva el ratón de forma aleatoria por la zona que hay bajo la barra de progreso. Conforme vaya moviendo el ratón se indicará el progreso del proceso.



3. Le aparecerá en un recuadro la clave pública en formato openssh ya seleccionada. Esa es la que nos tiene que enviar al SCI por lo que hay que guardarla. Para ello pulse Ctrl+C o seleccione la opción 'Copiar' pulsando con el botón derecho del ratón sobre la selección (asegúrese que está seleccionado todo el contenido del recuadro) y guarde esa cadena seleccionada en un fichero, por ejemplo, haciendo uso del bloc de notas.



4. A continuación vuelva a la ventana de puttygen del punto anterior y pulse sobre el botón ‘Save public key’ y posteriormente sobre el botón ‘Save private key’ y recuerde dónde ha guardado estos ficheros pues contienen sus claves pública y privada en formato ‘putty’ y que tendrá que usar para configurar el acceso desde un cliente Windows hacia la máquina virtual.
   Puttygen pone la extensión ‘.ppk’ al fichero de clave privada y ‘.pub’ al de la pública, aunque esto es opcional y puede poner el nombre y extensión que quiera en el momento de guardarlas

Configuración de acceso a la máquina virtual

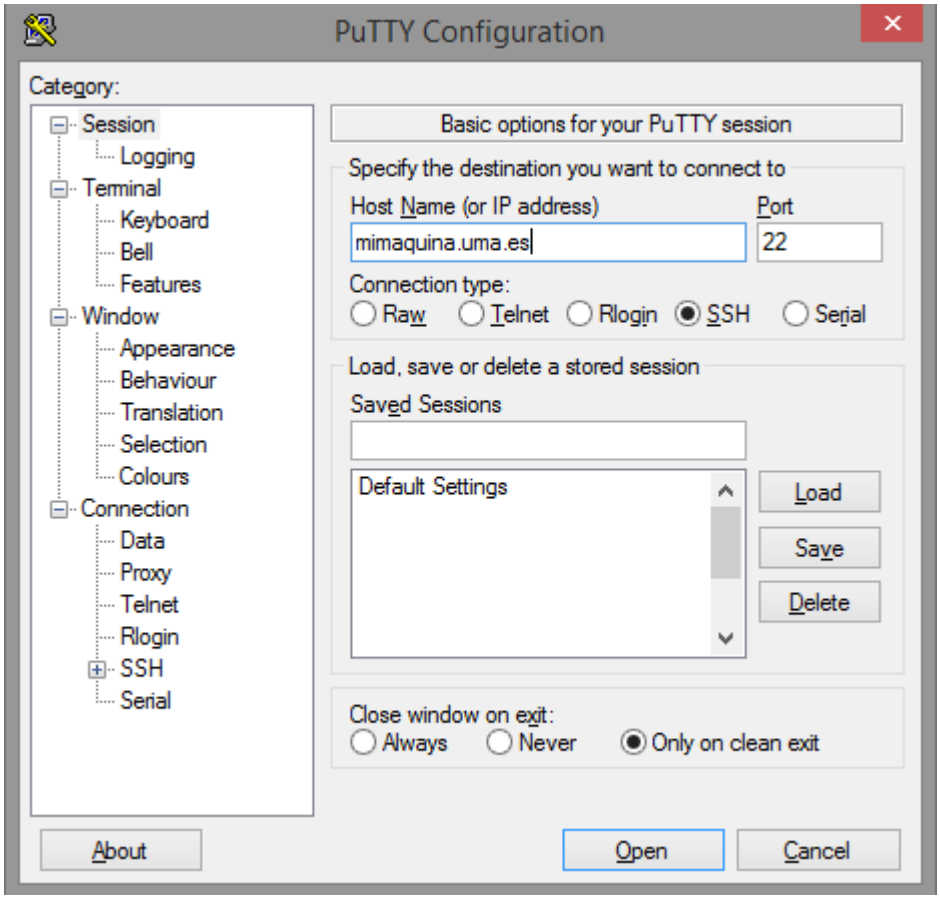
Para poder establecer una conexión ssh con la máquina virtual desde Windows es necesario hacer uso de programas que no vienen con el sistema operativo.

Nosotros recomendamos el uso de **putty.exe** (puede descargarlo desde http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html). Este programa no requiere instalación y lo puede usar incluso desde una sesión de Windows de un usuario sin privilegios.

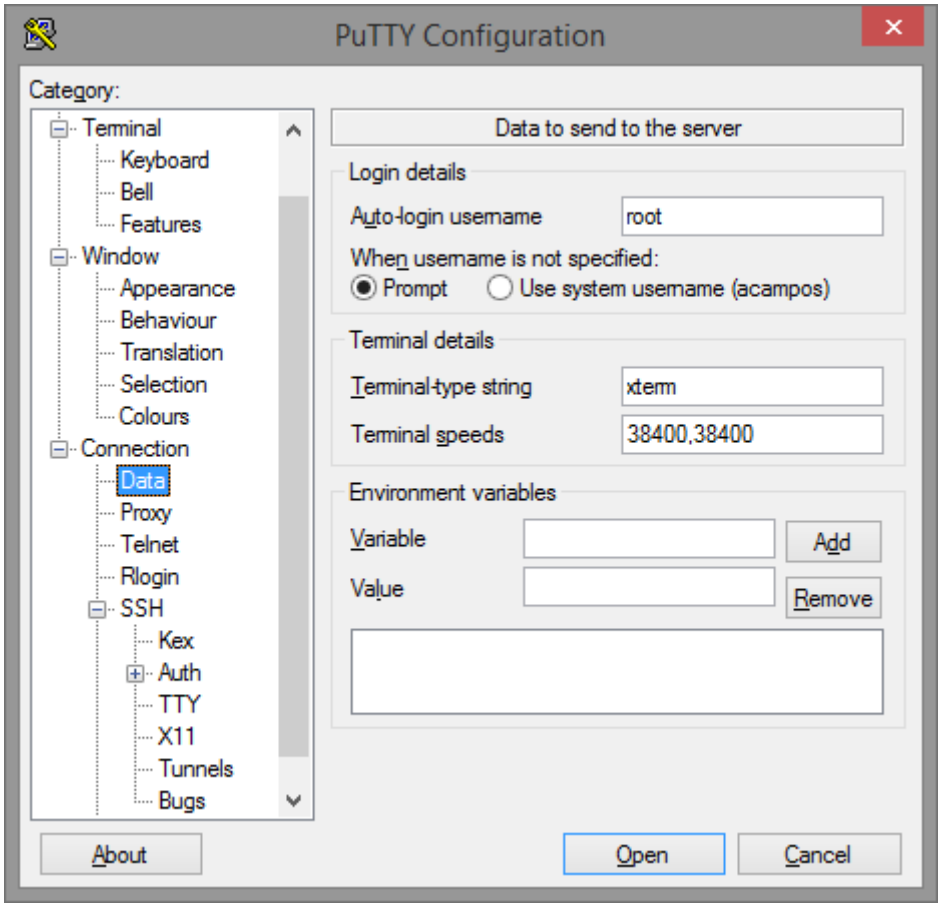
Para establecer una conexión con la máquina virtualizada es necesario configurar un '*perfil de conexión*'

A continuación se detallan los pasos de configuración de un perfil de conexión en el supuesto de que la máquina a la que queremos acceder se llama '*mimaquina.uma.es*' y vamos a establecer una sesión como usuario '*root*' de esa máquina.

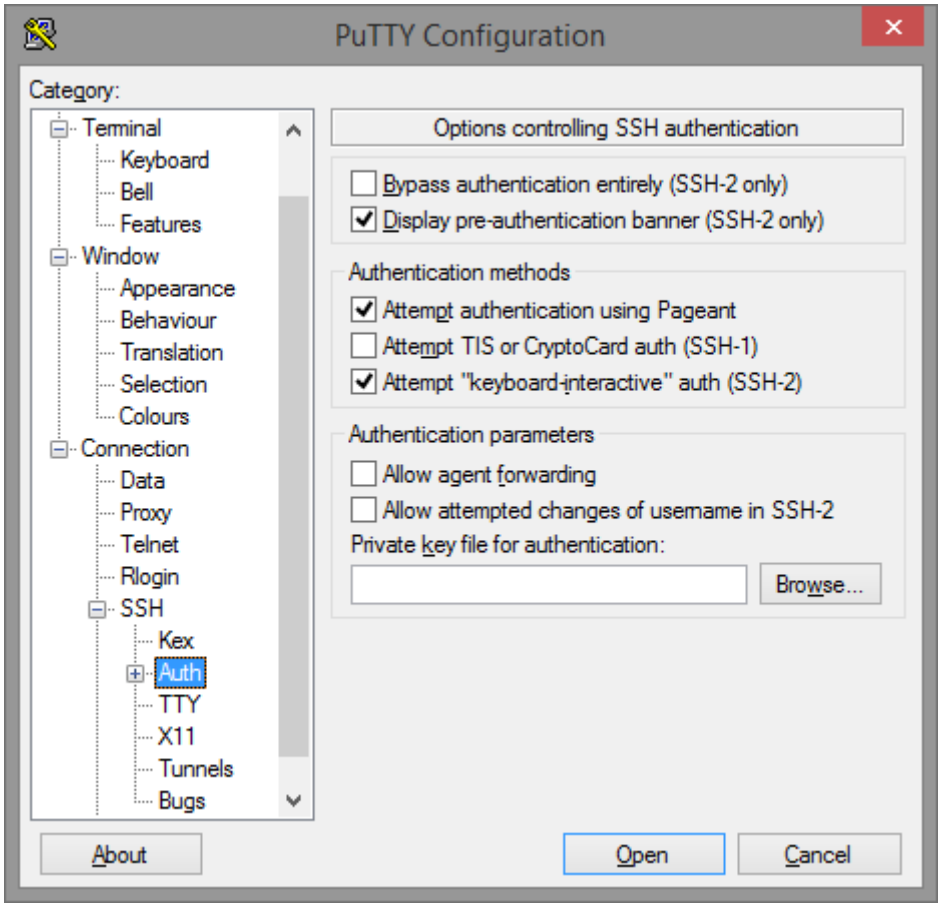
1. Una vez arrancado putty.exe aparecemos en el panel 'Session'. En él debemos introducir en el campo 'Host Name (or IP address)' el nombre de la máquina a la que queremos conectarnos y en el campo 'Port' el puerto que nos hayan indicado (en caso de no conocer el nº de puerto dejamos el valor por defecto 22). El resto de opciones se dejan con los valores prestablecidos.



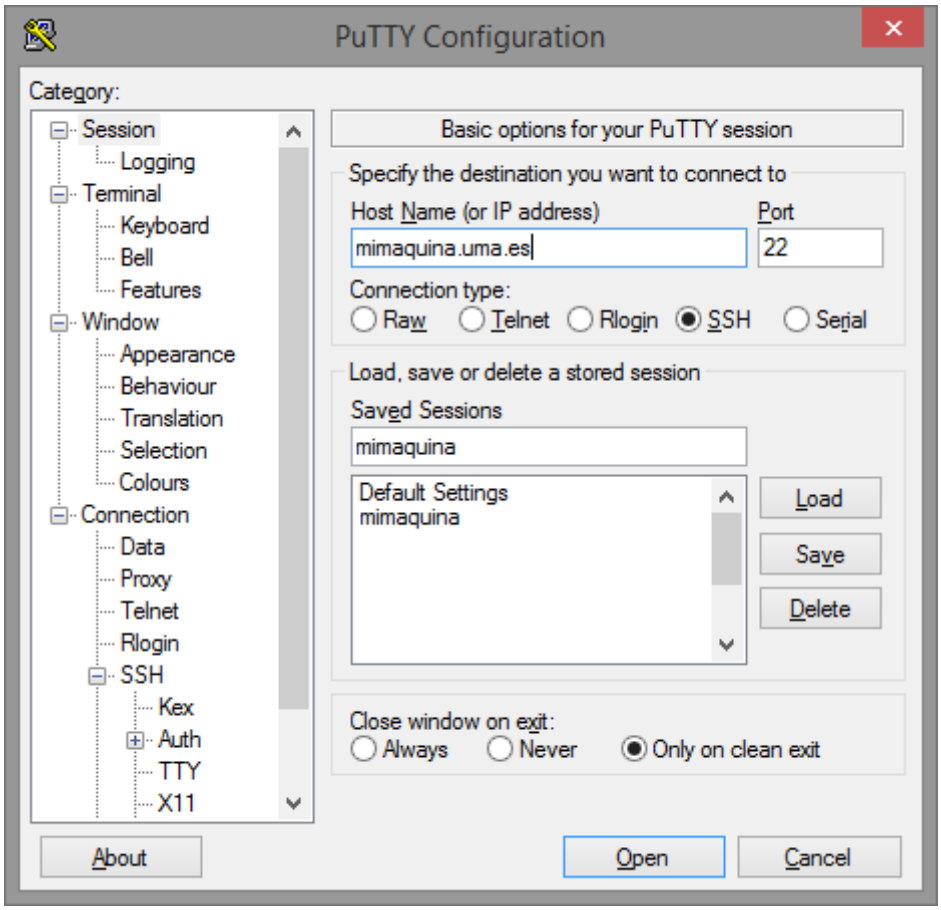
2. En segundo lugar pulsamos en la opción ‘Connection’ -> ‘Data’, donde rellenamos el campo ‘Auto-login username’ con el nombre de usuario con el que queremos iniciar sesión en ‘mimaquina.uma.es’, que en nuestro caso es ‘root’



3. En tercer lugar pulsamos en la opción ‘Connection’ -> ‘SSH’ -> ‘Auth’. En este panel tenemos que indicar en el campo ‘Private keyfile for authentication’ la ubicación del fichero de la clave privada a usar para esta conexión y que debe ser el asociado a la clave pública que suministró al SCI para esta máquina. Este fichero es el que se generó en el apartado anterior y para el que dijimos que puttygen.exe le asignaba por defecto la extensión ‘.ppk’.



4. Por último, volvemos al panel por el que empezamos, el de la categoría ‘Session’ y damos un nombre a este perfil de conexión, rellenando el campo ‘Saved Sessions’ con un nombre que no esté listado en el recuadro inferior. Una vez escrito el nombre pulsamos sobre el botón ‘Save’ y el nombre se añadirá automáticamente a la lista de perfiles que tenemos configurados.



Configuración de un túnel SSH

Aunque es algo más complejo, podemos simplificar la idea de un túnel ssh como un mecanismo por el que se persiguen dos beneficios

1. Cifrar parte del camino por el que fluyen las comunicaciones entre máquinas.
2. Poder llegar a un servicio ofrecido por una máquina y para el que existe un firewall intermedio que no permite la comunicación directa.

El escenario que nos interesa en este manual es el que corresponde al nº 2 pues el servicio de máquina virtual se ofrece de forma que a la máquina en cuestión sólo se puede acceder por ssh para su administración. El resto de servicios que son accesibles son aquellos que se han solicitado y para los que se ha creado la máquina. Esto no quita que en la máquina haya más servicios necesarios para el funcionamiento de lo que se pretende ofrecer.

Por política de seguridad, las máquinas tienen cerrados todos los puertos salvo aquellos por los que se prestan los servicios solicitados, dejando siempre el puerto ssh para administración.

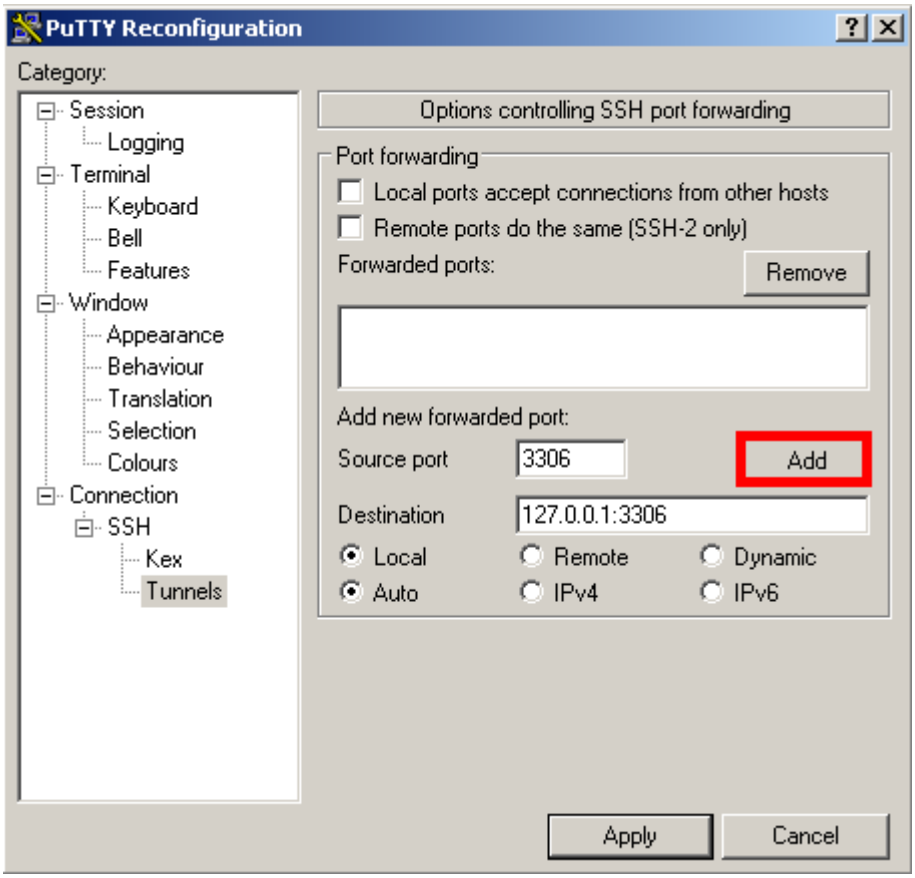
El ejemplo habitual es el de una máquina solicitada para albergar un web. En este caso los únicos puertos accesibles de esa máquina son aquellos necesarios para el servidor de páginas web (normalmente el puerto 80 y el 443). Pero, normalmente, junto al servidor de páginas web suele haber un servidor de bases de datos para hacer que el web sea dinámico y que atiende en su propio puerto, el cual no es accesible directamente desde otras máquinas.

En este escenario es cómodo para el administrador poder gestionar directamente el servidor de bases de datos mediante algún programa gráfico que conecte directamente con el servidor en lugar de instalar una aplicación web que sirva para administrar la base de datos.

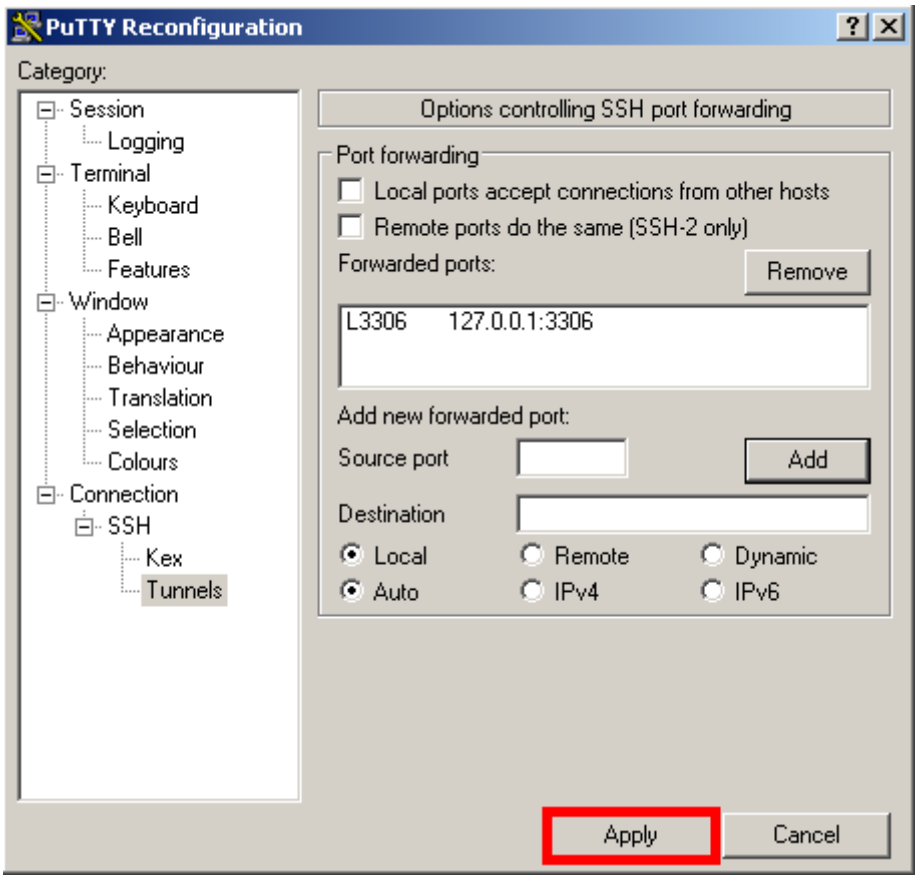
La solución es establecer un túnel ssh entre la máquina local y la máquina virtual. El túnel se establece entre el programa putty.exe, que representa el extremo ssh de la máquina local, y el servicio ssh levantado en la máquina virtual.

El programa gráfico de gestión de la base de datos hay que configurarlo para que en lugar de conectar directamente con el servidor de base de datos, conecte con la *entrada del túnel* que proporciona putty.exe. En la configuración del túnel en putty.exe lo que se indica es dónde hay que dirigirse al *salir del túnel* por el otro extremo. En realidad, lo que ocurre en ambos extremos del túnel es una traslación de puertos además de la operación de cifrado/descifrado, siempre presente en las conversaciones ssh.

La configuración de un túnel en putty.exe consistiría en todo lo mencionado anteriormente en el apartado de *Configuración de acceso a la máquina virtual* y, adicionalmente, configurar la opción ‘Connection’ -> ‘SSH’ -> ‘tunnel’. Poniendo como ejemplo la configuración de establecimiento de un túnel hacia un servidor de bases de datos MySQL que responde en el puerto 3306, lo que hay que rellenar quedaría de la siguiente manera:



y tras pulsar el botón ‘Add’ obtendríamos:

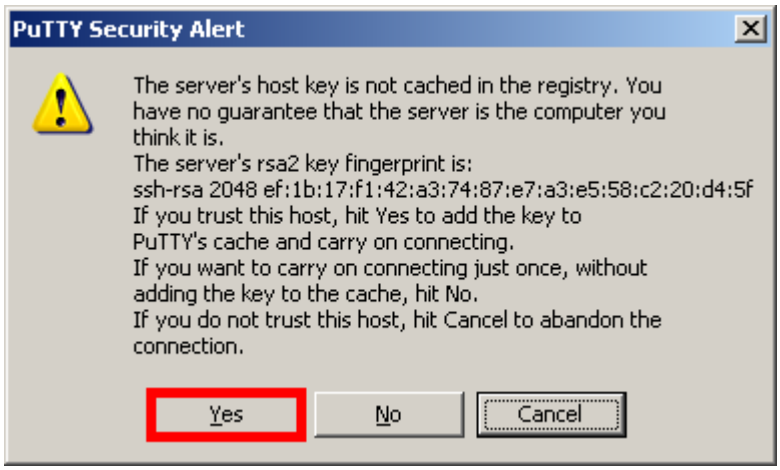


Cuando abrimos una sesión de putty.exe con un túnel configurado obtendremos la ventana de terminal en la que podremos trabajar normalmente y, mientras esté abierta, el túnel está establecido, permitiendo que otros programas hagan uso de él. Hay que tener en cuenta que si se cierra esta ventana (sesión), también estamos eliminando el túnel. También ocurre que si intentamos cerrar esta ventana de terminal cuando ya hay algún programa usando el túnel, ésta no se cierra. Se cerrará automáticamente cuando se deje de usar el túnel.

Conexión con la máquina virtual

Para conectar con la máquina virtual sólo hay que iniciar el programa putty.exe y hacer doble clic sobre el perfil de conexión que hemos configurado para esta máquina

La primera vez que putty.exe establezca una conexión con mimaquina.uma.es le aparecerá un aviso de la siguiente forma y al que responderemos pulsando 'Yes':



A partir de ahí las siguientes conexiones que haga no pasarán por este aviso salvo que se hayan producido cambios en la configuración de claves del servidor.

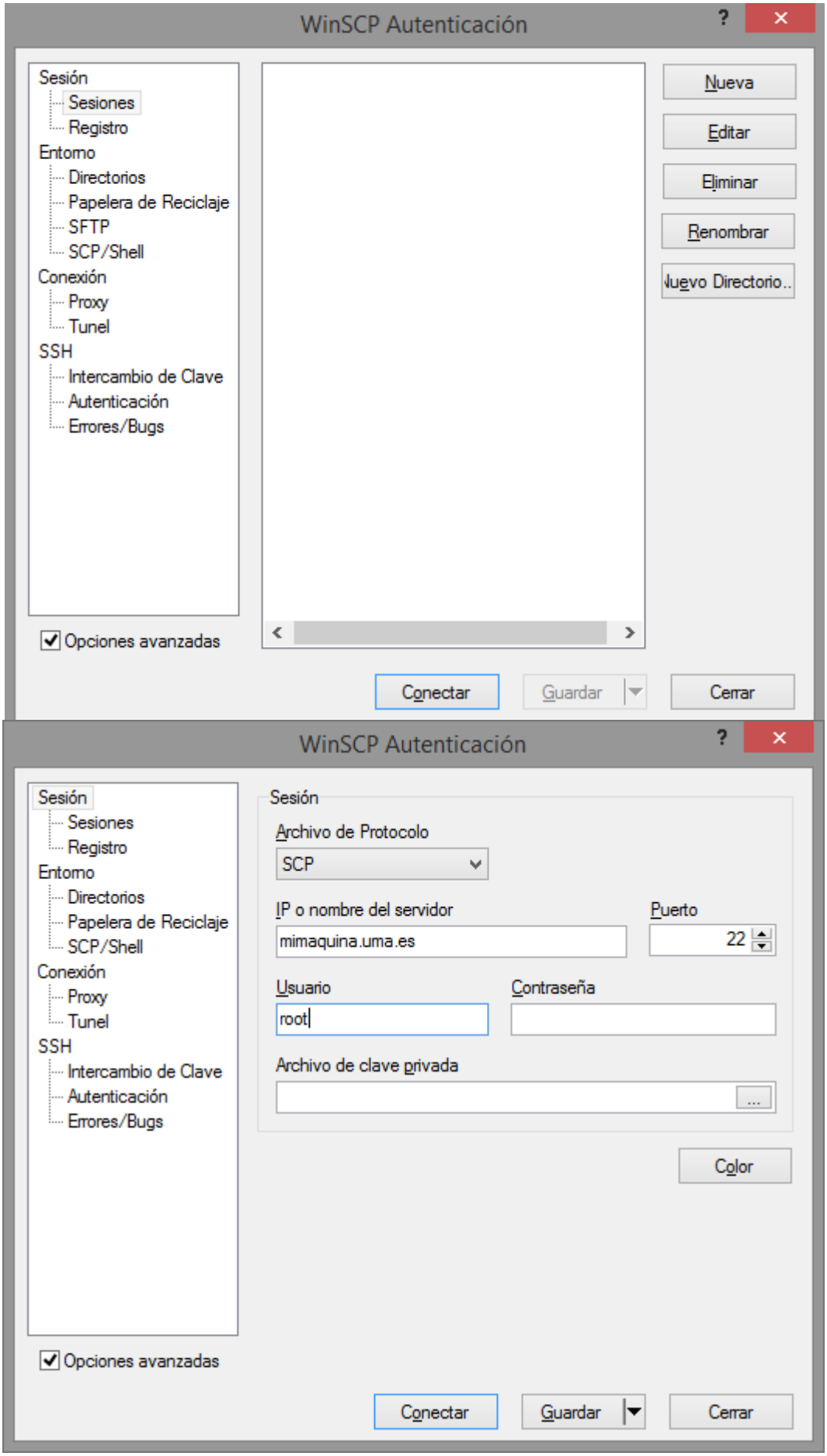
Intercambio de ficheros con la máquina virtual

El intercambio de ficheros entre nuestra máquina personal y la máquina virtual lo haremos mediante SCP. Recomendamos el uso del programa Winscp que puede descargar desde https://winscp.net/eng/download.php.

Para la configuración de este programa tenemos que seguir los siguientes pasos (usamos los mismos datos de conexión que se utilizaron en el ejemplo para conectar mediante putty.exe)

Si aún no estamos en el panel de configuración entramos en el menú 'Sesión' -> 'Nueva sesión' y pulsamos el botón 'Nueva'. Seleccionamos en el campo 'Archivo de protocolo' el valor 'SCP'. En el campo 'IP o nombre del servidor' ponemos mimaquina.uma.es. En el campo 'Usuario' ponemos 'root' y en el campo 'Archivo de clave privada' indicamos la ubicación del fichero que contiene nuestra clave privada (el de la extensión .ppk).

Finalmente pulsamos en el botón 'Guardar' y se añadirá una nueva sesión en la lista de sesiones con el nombre root@mimaquina.uma.es



Cuando conectamos con este perfil obtendremos una ventana en la que la parte izquierda

corresponde a nuestro ordenador local y la parte derecha será lo que hay en la máquina virtualizada. En esta situación se pueden intercambiar ficheros en ambas direcciones.

Uso de un agente de usuario SSH

Normalmente, para las tareas administrativas, sólo tendremos que establecer conexiones SSH esporádicas entre nuestra máquina y la máquina virtual administrada.

Cada vez que conectamos por SSH se nos pedirá que introduzcamos la '*passphrase*' que establecimos.

Si necesitamos conectarnos con frecuencia, ya sea para abrir un terminal, ya sea para transferir ficheros por SCP, existe la posibilidad de tener instalado lo que se llama un agente de usuario ssh, que no es más que un programa cuya misión es mantener cargadas en memoria todas claves que vayamos a usar y para las que habrá solicitado previamente cada una de las passphrases asociadas.

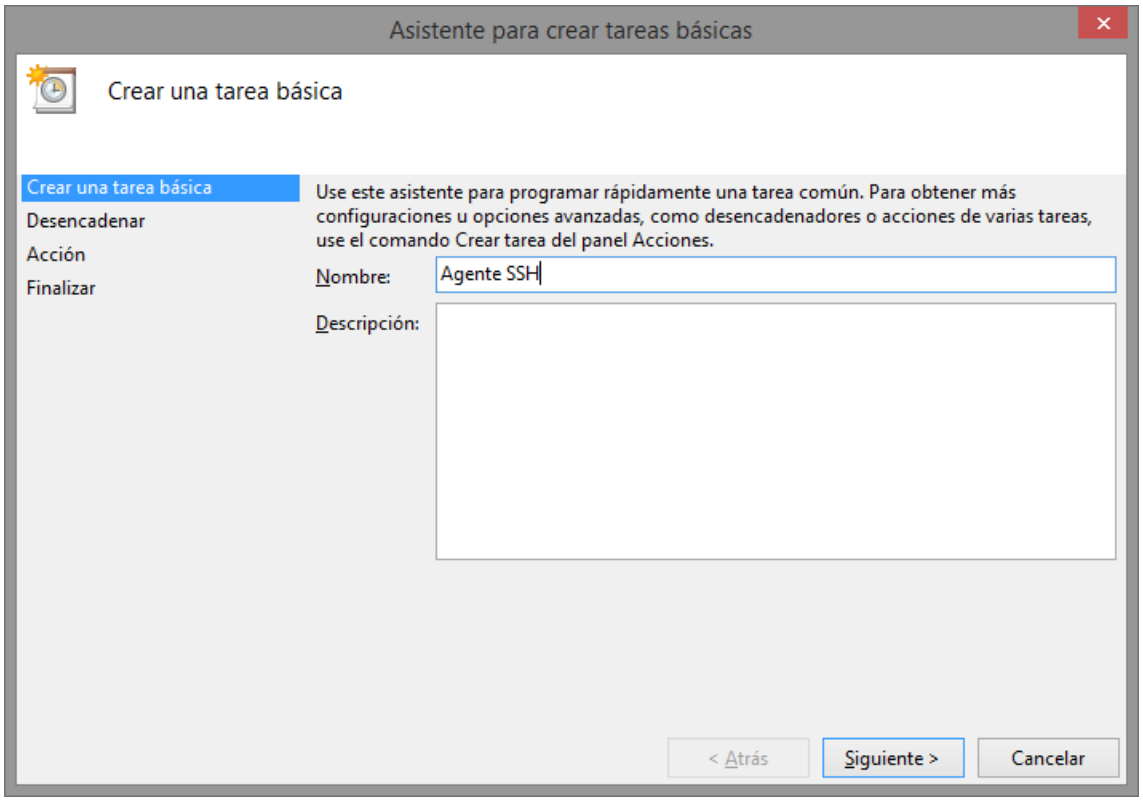
Para el caso de Windows existe el programa **pageant.exe** (puede descargarlo desde http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html). Este programa se suele configurar para que arranque en el inicio de sesión de Windows. En ese momento, solicita las '*passphrases*' de cada una de las claves privadas que se quieran cargar en memoria**.** A partir de ese momento el agente ya tiene autorizado el uso de las claves cargadas y los programas como putty.exe o winscp.exe, cuando realizan una conexión para la que tienen configurada el uso de una clave privada, hablan directamente con el agente para ver si ya tiene cargada esa clave. Si es así, no vuelven a solicitar la '*passphrase*'.

Tanto si ejecuta el programa pageant.exe manualmente como si lo configura para que se ejecute en el inicio de sesión, podrá ver que está en ejecución observando el icono que debe haber en el área de notificaciones situada en la barra de tareas de Windows.

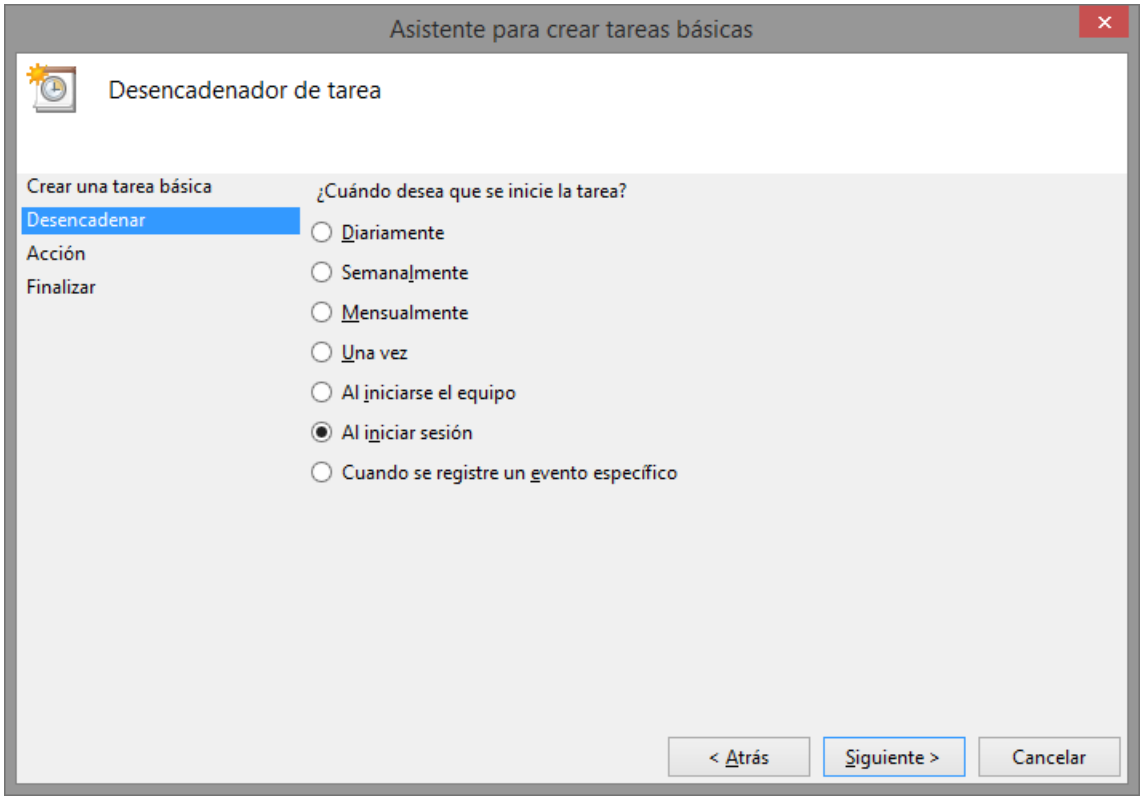
Haciendo clic con el botón derecho del ratón sobre este icono tiene opciones para gestionar las claves, pudiendo agregar nuevas claves o eliminar claves cargadas.

Si queremos automatizar el uso de las claves cargándolas en el inicio de sesión tendríamos que crear una tarea programada para el usuario que deseemos. Para ello iniciamos sesión de Windows con el usuario en cuestión. Entramos en el programador de tareas de Windows (suponemos Windows 7 o superior), agregamos una '*Tarea básica*' y seguimos los pasos del asistente:

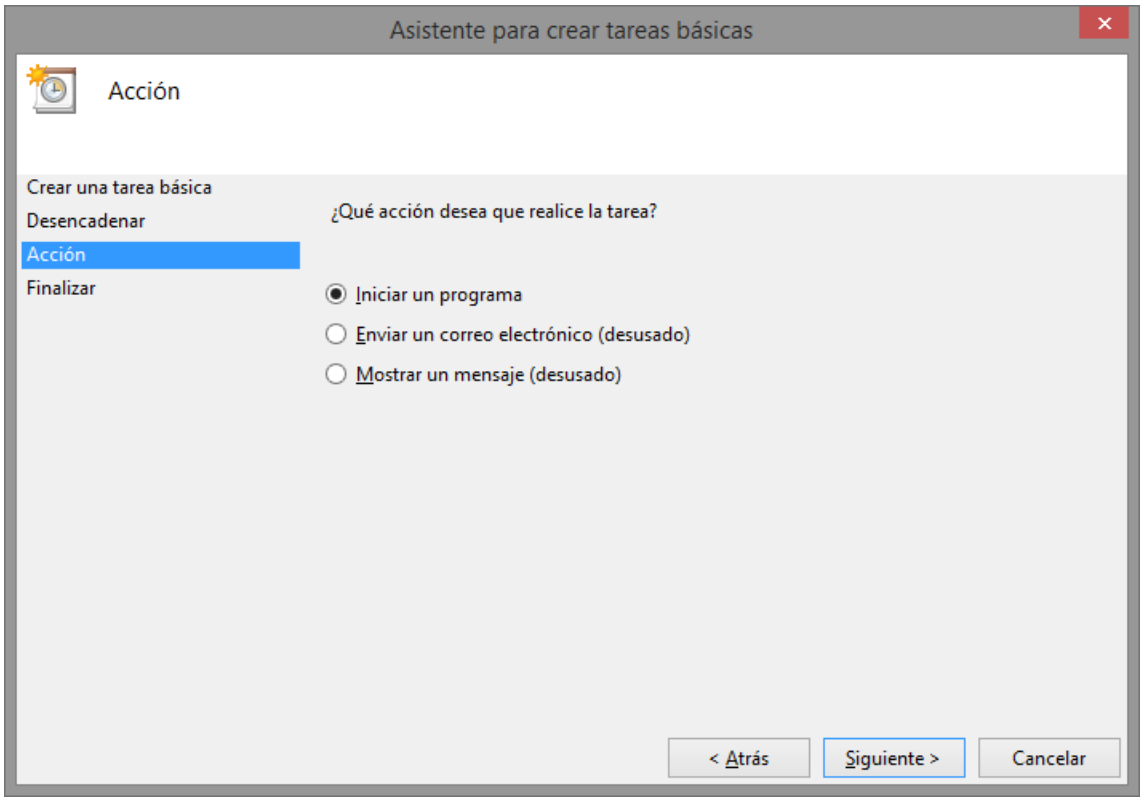
Le asignamos un nombre.



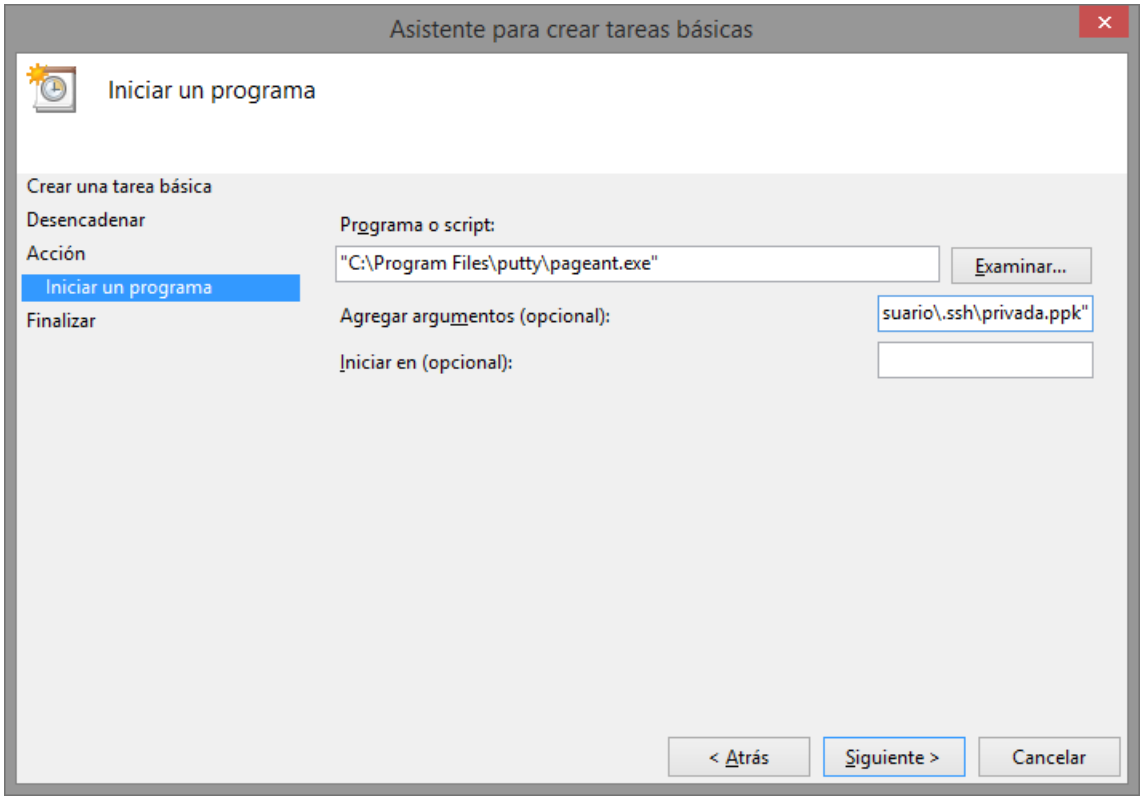
En el desencadenador establecemos ‘Al iniciar sesión’



En acción seleccionamos ‘Iniciar un programa’

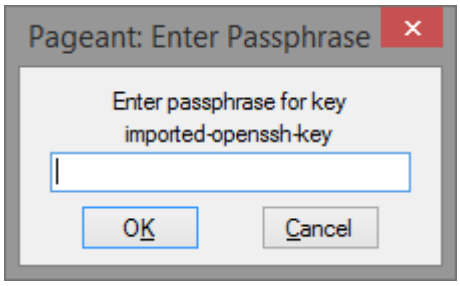


A continuación indicamos que el programa es pageant.exe y le indicamos como argumentos la lista de ubicaciones de las claves privadas que queremos que cargue.



Y pulsamos ‘Finalizar’ para terminar el asistente

Con esta configuración, cada vez que este usuario inicie una sesión, se le pedirá la 'passphrase' de cada clave privada que se haya pasado como argumento.



Notas adicionales sobre el servicio

Debido al sistema de virtualización es posible que haya operaciones que no pueda hacer aun siendo usuario 'root'. Si necesitara alguna operación concreta que no pueda realizar, debe consultarla con el SCI.

- Las máquinas virtuales disponen de un único interfaz de red que exclusivamente tiene direccionamiento IPv6. En el entorno del sistema están definidas las variables $http_proxy y $https_proxy con valor 'http://jano8.sci.uma.es:3128/'. Cualquier aplicación instalada que necesite comunicarse mediante los protocolos http o https y que no haga uso de esta configuración, debe usar estos valores para configurarla.
- Las máquinas virtuales traen una configuración prestablecida cuyo comportamiento no debe modificar. Concretamente:
    - Trae una serie de reglas de firewall configuradas. Aunque puede añadir nuevas reglas no debe eliminar ninguna de las que hay.
    - Puede agregar claves públicas para que otros usuarios entren como 'root' pero no debe eliminar ninguna de las que están configuradas inicialmente.
    - Trae configuradas algunas resoluciones de nombres. Aunque puede añadir nuevas no debe eliminar ninguna de las que hay.
- El envío de correos electrónicos desde estas máquinas se tiene que hacer a través de conexión autenticada con el servidor correo.uma.es usando TLS y mediante el empleo de una identificación válida en DUMA. La siguiente configuración sería la que habría que poner en la aplicación o producto desde el que se quiera enviar correos:
    - Servidor de correo: correo.uma.es
    - Puerto: 587
    - Usuario y clave: Se le proporcionará una identificación válida asociada a la máquina. También puede usarse cualquier identificación válida en DUMA pero tenga en cuenta que en la configuración tendrá que quedar guardada la clave. El cambio la clave asociada a la identificación que se le proporciona lo debe solicitar a través del CAU.
- Si van a hacer uso de SSL en algo que instalen, por ejemplo, para ofrecer contenidos web por una vía segura (https), pueden solicitar un certificado de servidor a través del CAU en lugar de usar un certificado autofirmado.