



Seminario 1: Computación en nubes públicas – Modelos IaaS

**Computación de Altas
Prestaciones - Master
Universitario en Ingeniería
Informática**



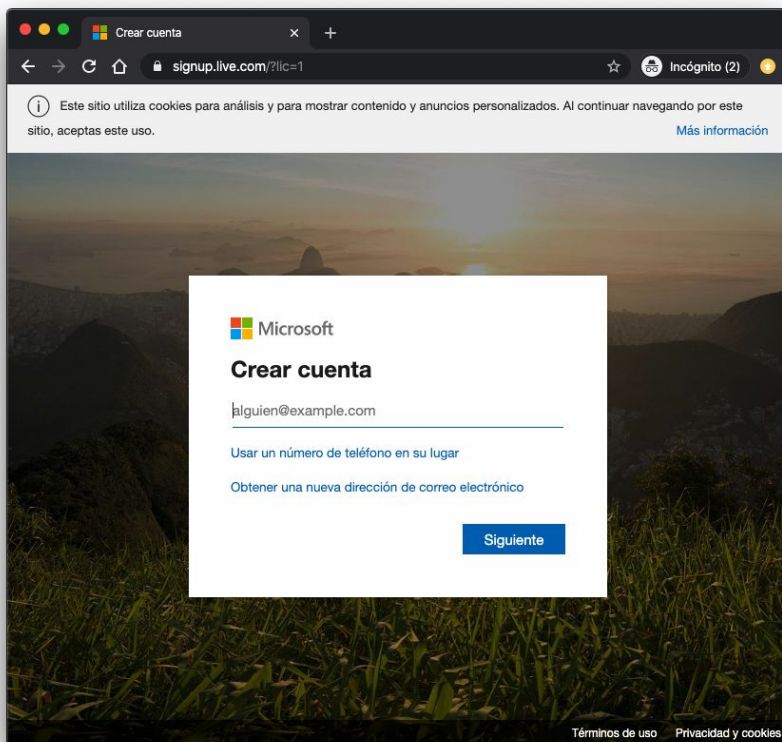
- Presentar una de las plataformas de cloud público más utilizadas y su cobertura internacional.
- Describir los conceptos básicos de las infraestructuras como servicio.
- Describir de forma básica los servicios que gestionan el ciclo de vida en un IaaS.

WINDOWS AZURE

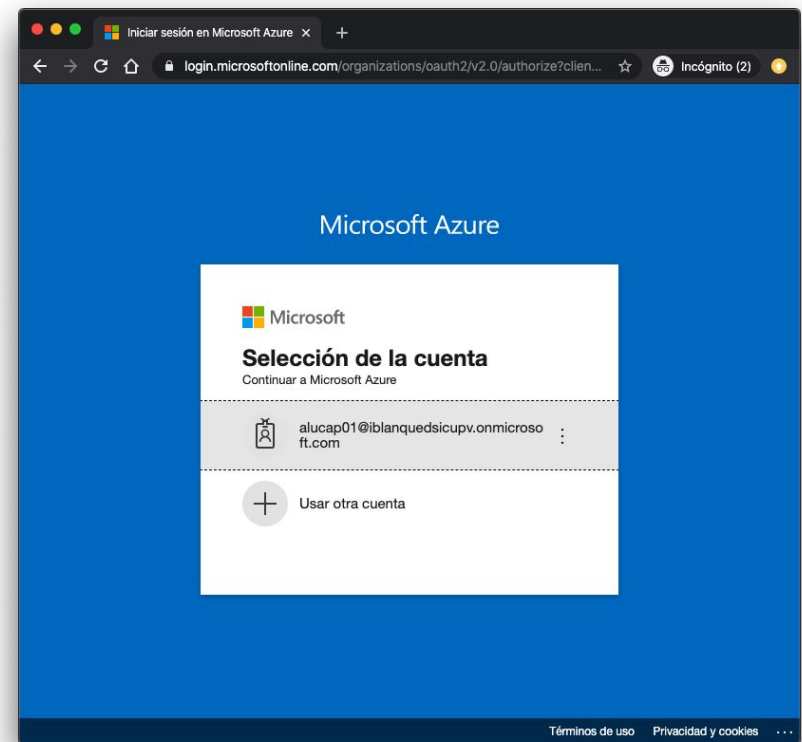
Cuenta Live id

- Para poder acceder a la plataforma de Azure es necesario disponer de una cuenta Live Id

<https://signup.live.com>



<https://portal.azure.com/>



Cuentas precreadas

- A cada alumno se le asignará una cuenta
 - alucpaXX@iblanquedsicupv.onmicrosoft.com
 - Se deberá cambiar la contraseña en el primer acceso.
 - Cada Alumno es responsable del uso de la cuenta.
- Procedemos a entrar en el portal
<https://portal.azure.com/>



Microsoft Azure

Microsoft

alumusit00@iblanquedsicupv.onmicrosoft.com

Actualizar contraseña

Necesita actualizar la contraseña porque se trata de la primera vez que inicia sesión o porque la contraseña expiró.

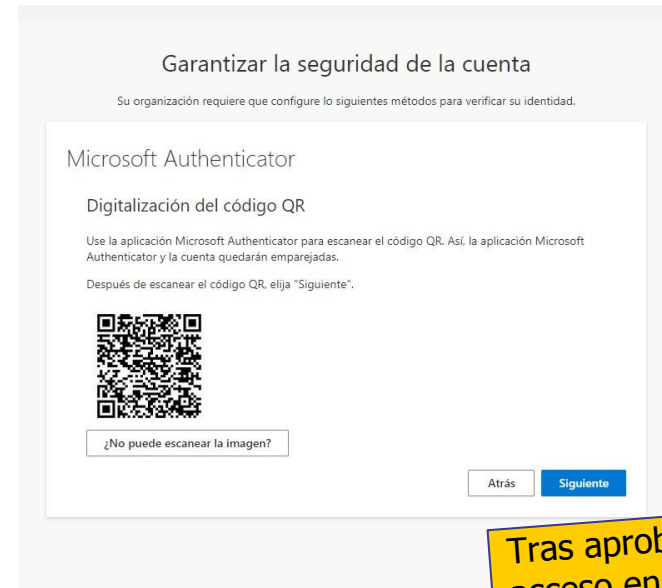
Contraseña actual

Contraseña nueva

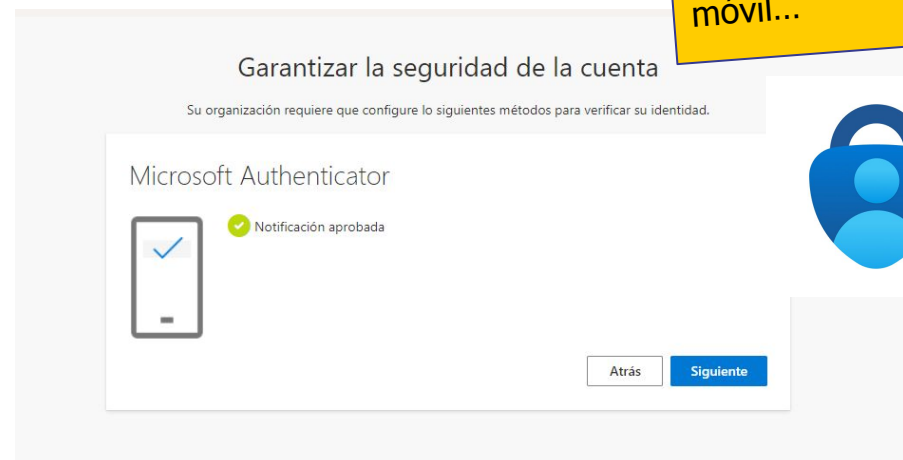
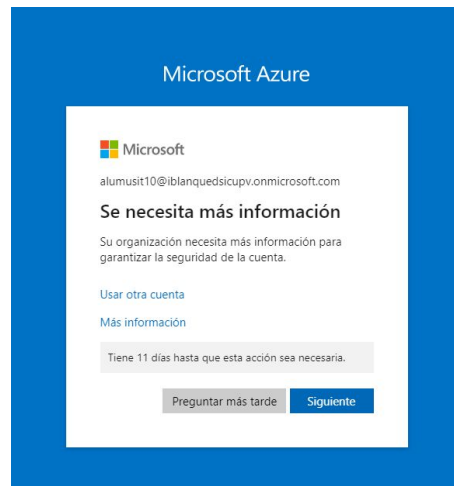
Confirmar contraseña

Iniciar sesión

- Además de actualizar la contraseña, tendrás que aprobar el inicio de sesión con Microsoft Authenticator
 - Es la misma aplicación usada para conectar a la VPN de la UPV.



Tras aprobar el acceso en vuestro móvil...



Portal de Azure

Servicios de Azure

- Crear un recurso
- Usuarios
- Suscripciones
- Azure Active Directory
- Máquinas virtuales
- Identidades administradas
- Acceso condicional d...
- Métodos de autenticació...
- Grupos
- Más servicios

Recursos recientes

Nombre	Tipo	Última consulta
Pago por uso	Suscripción	Hace 1 hora

Navegar

- Suscripciones
- Grupos de recursos
- Todos los recursos
- Panel

Herramientas


- Microsoft Learn**
Aprenda a usar Azure con los cursos en línea gratuitos de Microsoft.
- Azure Monitor**
Supervise las aplicaciones y la infraestructura.
- Security Center**
Proteja sus aplicaciones e infraestructura.
- Administración de costos**
Analice y optimice el gasto en la nube de forma gratuita

Vínculos útiles

- Documentación técnica
- Herramientas de migración de Azure
- Servicios de Azure
- Buscar un experto de Azure
- Actualizaciones recientes de Azure
- Centro de inicio rápido

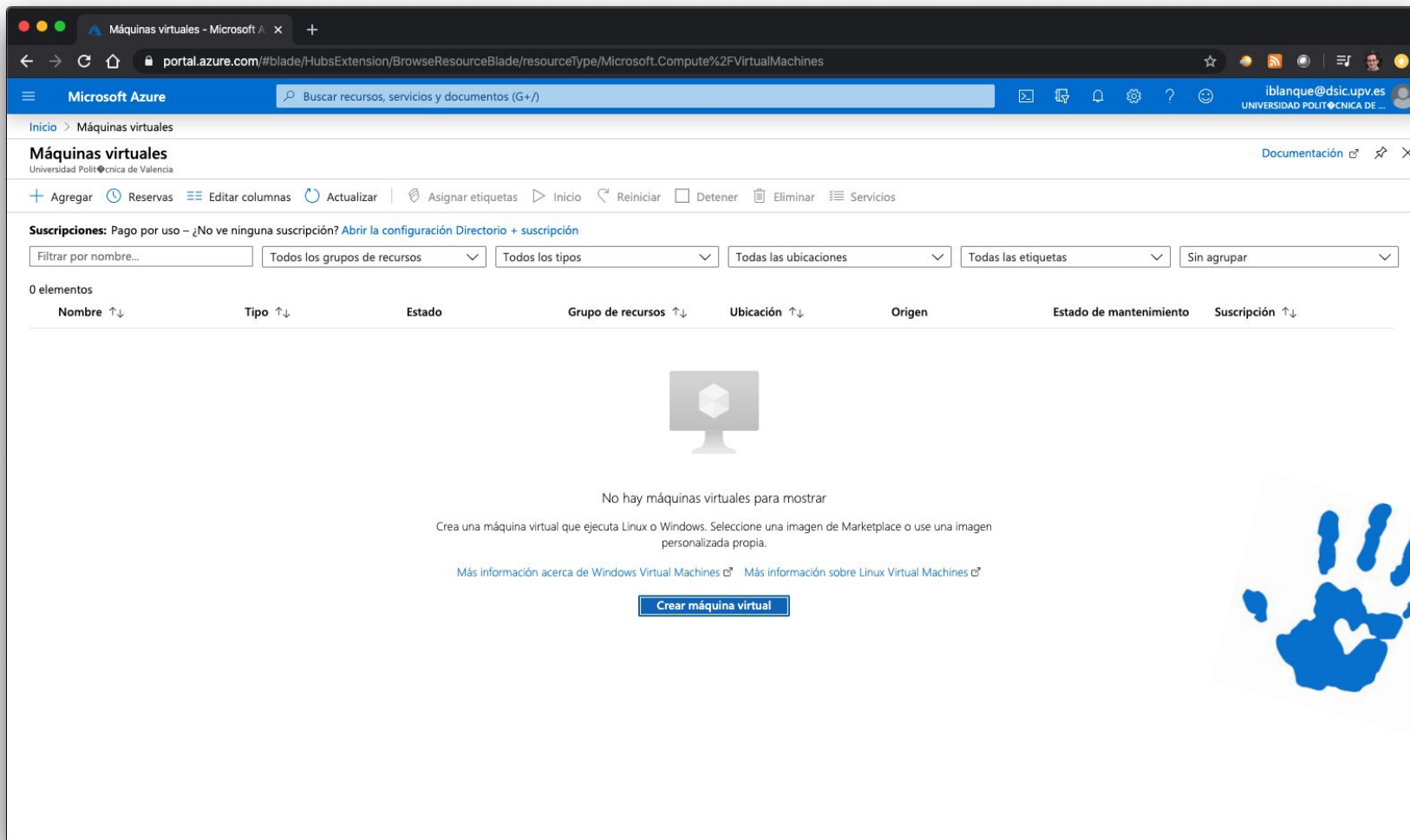
Aplicación móvil de Azure

Download on the App Store | GET IT ON Google Play



Creación de una VM

- Máquinas Virtuales / Crear Máquina Virtual



The screenshot shows the Microsoft Azure portal interface for managing virtual machines. The browser address bar displays the URL: `portal.azure.com/#blade/HubsExtension/BrowseResourceBlade/resourceType/Microsoft.Compute%2FVirtualMachines`. The page title is "Máquinas virtuales" (Virtual Machines) under the "Universidad Politécnica de Valencia" subscription. The interface includes a top navigation bar with the Azure logo and a search bar. Below the navigation bar, there are tabs for "Agregar" (Add), "Reservas" (Reservations), "Editar columnas" (Edit columns), "Actualizar" (Refresh), "Asignar etiquetas" (Assign tags), "Inicio" (Start), "Reiniciar" (Restart), "Detener" (Stop), "Eliminar" (Delete), and "Servicios" (Services). The main content area shows a message: "No hay máquinas virtuales para mostrar" (No virtual machines to show). Below this message, there is a button labeled "Crear máquina virtual" (Create virtual machine). A blue handprint icon is overlaid on the bottom right of the screenshot.

Datos Básicos

- **Subscripción:** La suscripción utilizada para pagar los recursos utilizados en Azure.
- **Grupo de Recursos:** Sirve para gestionar los recursos virtuales creados en Azure y crear máquinas con reglas comunes. Se recomienda crear uno la 1ª vez y siempre utilizar el mismo. (ej. grCAP**iblanque**).

Detalles del proyecto

Seleccione la suscripción para administrar recursos implementados y los costes. Use los grupos de recursos como carpetas para organizar y administrar todos los recursos.

Suscripción * ⓘ

Pago por uso

Grupo de recursos * ⓘ

Seleccionar existentes...

[Crear nuevo](#)

Detalles de instancia

Nombre de máquina virtual * ⓘ

Región * ⓘ

(ESTADOS UNIDOS) Este de EE. UU.

Opciones de disponibilidad ⓘ

No se requiere redundancia de la infraestructura

Imagen * ⓘ

Ubuntu Server 18.04 LTS

[Examinar todas las imágenes públicas y privadas](#)

Instancia de Azure Spot ⓘ

☐ Sí ☒ No

Tamaño * ⓘ

Standard D2s v3

2 vcpu, 8 GiB de memoria (\$9,10 €/mes)

[Cambiar el tamaño](#)

Cuenta de administrador

Tipo de autenticación ⓘ

☐ Contraseña ☒ Clave pública SSH

Nombre de usuario * ⓘ

Clave pública SSH * ⓘ

[Más información sobre la creación y](#)

Reglas de puerto de entrada

Seleccione los puertos de red de máquina virtual que son accesibles desde la red Internet, o red más limitado o granular en la pestaña Red.

Puertos de entrada públicos * ⓘ

☐ Ninguno ☒ Permitir los puertos seleccionados

Seleccionar puertos de entrada *

SSH (22)



cceso de

Datos Básicos

- **Nombre de máquina Virtual:** Nombre único de la MV (p.e. mvCAP**iblanque**LINUX).
- **Región:** Corresponde la ubicación física del datacenter donde se ubicará la MV a crear. (Ej. *Norte de Europa*)
- **Opciones de disponibilidad:** Opciones para administrar la disponibilidad y la tolerancia de las aplicaciones. (No se requiere redundancia de la infraestructura).
- **Imagen:** Imagen predefinida con la aplicación o el sistema operativo base de la máquina virtual (Ej. Ubuntu server 20,04 LTS).

Detalles del proyecto

Seleccione la suscripción para administrar recursos implementados y los costes. Use los grupos de recursos como carpetas para organizar y administrar todos los recursos.

Suscripción * ⓘ

Grupo de recursos * ⓘ

[Crear nuevo](#)

Detalles de instancia

Nombre de máquina virtual * ⓘ

Región * ⓘ

Opciones de disponibilidad ⓘ

Imagen * ⓘ

[Examinar todas las imágenes públicas y privadas](#)

Instancia de Azure Spot ⓘ ☐ Sí ☒ No

Tamaño * ⓘ

Standard D2s v3
2 vcpu, 8 GiB de memoria (\$9,10 €/mes)
[Cambiar el tamaño](#)

Cuenta de administrador

Tipo de autenticación ⓘ ☐ Contraseña ☒ Clave pública SSH

Nombre de usuario * ⓘ

Clave pública SSH * ⓘ

[Más información sobre la creación y](#)

Reglas de puerto de entrada

Seleccione los puertos de red de máquina virtual que son accesibles desde la red Internet. La red más limitada o granular en la pestaña Red.

Puertos de entrada públicos * ⓘ ☐ Ninguno ☒ Permitir los puertos seleccionados

Seleccionar puertos de entrada *



cceso de

Datos Básicos

- **Tamaño:** Características hardware de la Máquina virtual a desplegar. Parámetros que definen el tamaño de los discos, las prestaciones de E/S y el número de núcleos
 - **Cambiar a B2s estándar**
- **Nombre de Usuario:** Usuario para iniciar sesión como administrador (Ej. capuser).
- **Tipo de autenticación:** Forma de autenticar el usuario. (Ej. Por Clave Pública SSH)
 - Ver la siguiente transparencia.
- **Puertos de Entrada**
 - Reglas del Firewall para el acceso a la máquina
 - 22 para poder hacer ssh.

Detalles del proyecto

Seleccione la suscripción para administrar recursos implementados y los costes. Use los grupos de recursos como carpetas para organizar y administrar todos los recursos.

Suscripción * ⓘ

Grupo de recursos * ⓘ

[Crear nuevo](#)

Detalles de instancia

Nombre de máquina virtual * ⓘ

Región * ⓘ

Opciones de disponibilidad ⓘ

Imagen * ⓘ

[Examinar todas las imágenes públicas y privadas](#)

Instancia de Azure Spot ⓘ ☐ Sí ☒ No

Tamaño * ⓘ **Standard D2s v3**
2 vcpu, 8 GiB de memoria (\$9,10 €/mes)
[Cambiar el tamaño](#)

Cuenta de administrador

Tipo de autenticación ⓘ ☐ Contraseña ☒ Clave pública SSH

Nombre de usuario * ⓘ

Clave pública SSH * ⓘ

[Más información sobre la creación y](#)

Reglas de puerto de entrada

Seleccione los puertos de red de máquina virtual que son accesibles desde la red Internet. La red más limitado o granular en la pestaña Red.

Puertos de entrada públicos * ⓘ ☐ Ninguno ☒ Permitir los puertos seleccionados

Seleccionar puertos de entrada *



- La conexión mediante claves SSH es más segura y reduce el riesgo de intrusiones
- Podemos dejar que Azure genere el par de claves o reutilizar un par de claves existente
 - La primera vez indicamos "Generar un par de claves nuevo" e indicamos un nombre (p.e **mvCAPXXSSHKeyPair**).
 - El portal generará el par de claves y nos permitirá descargar la clave privada cuando creamos la máquina.
 - La clave privada no puede volver a descargarse.
 - Para la próxima máquina, podemos reutilizar esta clave con la opción "Usar una clave existente almacenada en Azure".



i Ahora, Azure genera automáticamente un par de claves SSH y le permite almacenarlo para usarlo en el futuro. Es una forma rápida, sencilla y segura de conectarse a la máquina virtual.

Nombre de usuario * ⓘ

azureuser ✓

Origen de clave pública SSH

Generar un par de claves nuevo ▼

Nombre de par de claves *

mvCAP00SSHKeypair ✓

Grid y Computación
de Altas Prestaciones

GRyCAP

- e un
- 

```

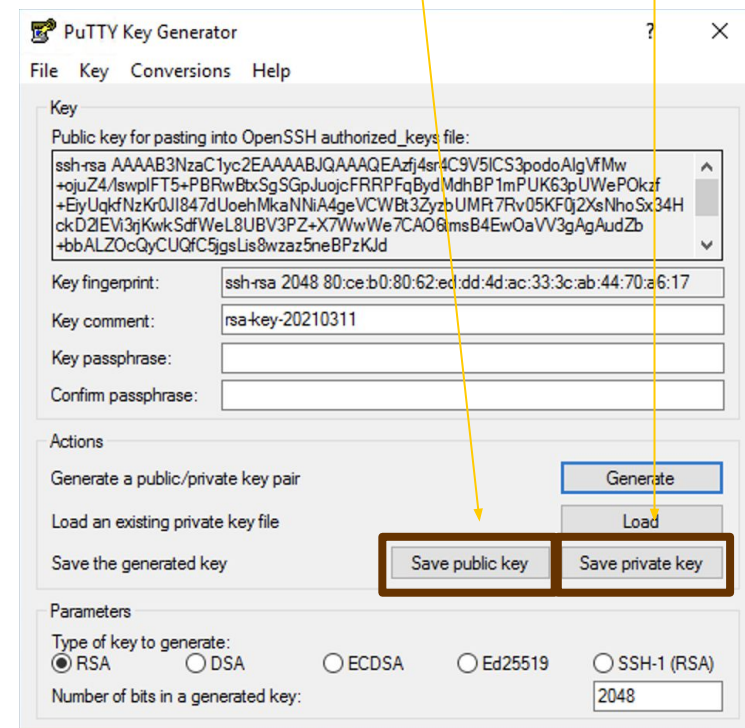
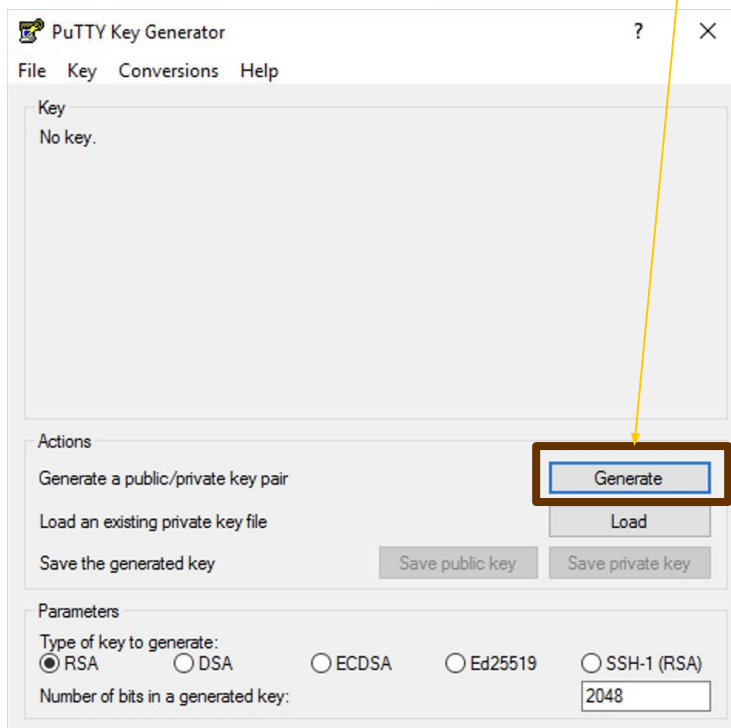
MacBook-Pro-de-Ignacio-2:Azure iblanque$ cat id_rsa_azure.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQCAQDImgKj5U10GCo2GL0BB14I/P
jpDP9re0niB10TUVkrhynn7TQyfh1rBjxKCUWwCm445v6YG8y+M4zH4aIGEMuf
b5CF8DqZa7LBUEarXL8/mvYU/ylobj4R9w2GtwzHnFljCLR1DKRP9CgRwDHXHT
PP4S0aUugTcr1aw30WRmtp+wnxkf+a0sW+z12wSOK1QLULZsZLi0LRUY3+0TjPt
NlaRCTtp0w2QH3lzyMHsN4nlEYCikwM+bEGW0SSa+pxlD6EIuEQk/36IGBUo+8
rQjFs0BQzaMq17Nk1WuvpqXtGU2NWeGKSzn3U+AiX3rFX0r3cD/4hs0v4FUIh+
NmL0nZ/g6EmbPz5n5z1x3Ig82L9be+BG5VjU/ehMDx0cJmWxdCAuyWBi1p9xF9
pmI0bzyYUq8M4GL3d3nFDr7xZZyxaK9suI2uQ4Z2xu2ifArTTDFWVfetJcZAYB
1fvsBzGCHtsPSW0pQKQWnaTtn54TyTTMvhl13TCaQuZGscTr13J3XgMiKMNcTa
Vy7h/J6/E1KXgnIpTvxtDDo4FufhMBY2em8jC81Wz6Gy4GQFsEZ3bN0075974k
MCJ6TL7j5kK6blvx8xB8/NSWE7frVuRBkN0FNf4eHcsWZ8NJbrurmNEFNiKWOT
lK0dmE9EQExWiAvEjNxxcXkpt2wYlSPR50yykvDpQ== iblanque@veraw154-1
49.wi-fi.upv.es
MacBook-Pro-de-Ignacio-2:Azure iblanque$
MacBook-Pro-de-Ignacio-2:Azure iblanque$

```


Creación de pares de claves (Windows)



- Para generar un par de claves y conectarnos por ssh desde Windows, podemos utilizar putty
 - Putty es un cliente de conexión por línea de comandos (ssh) para windows <https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html>.
- Creación de la clave con Puttygen, y guardamos la clave pública y privada.



Introducir la clave en la creación de la máquina

- Seleccionar Tipo de Autenticación "Clave pública SSH", y "Usar la clave pública existente".
- Copiar el contenido del fichero con la clave pública generado en PUTTy.

Crear una máquina virtual - Microsoft Azure

Inicio > Máquinas virtuales >

Crear una máquina virtual

Nombre de máquina virtual *

Región *

Opciones de disponibilidad

Imagen *

Instancia de Azure de acceso puntual ☐

Tamaño *

Cuenta de administrador

Tipo de autenticación ☒ Clave pública SSH ☐ Contraseña

Ahora, Azure genera automáticamente un par de claves SSH y le permite almacenarlo para usarlo en el futuro. Es una forma rápida, sencilla y segura de conectarse a la máquina virtual.

Nombre de usuario *

Origen de clave pública SSH

Clave pública SSH * AAAAB3NzaC1yc2EAAAABJQAAAQEAz4sr4C9V5ICS3podoAlgVfMw+ojuZ..."/>

[Más información sobre la creación y el uso de claves SSH en Azure](#)

[Ver todas las imágenes](#)

[Ver todos los tamaños](#)

[Revisar y crear](#) [< Anterior](#) [Siguiente: Discos >](#)

- Discos
 - Recomendable seleccionar HDD estándar.
- Redes
 - Crear una subred para las máquinas virtuales propias y asociar una IP pública (p.e. identificador mvCAP**iblanque**LINUX-ip).
- Grupo de Seguridad
 - Conjunto de reglas de Firewall para aplicar a diferentes máquinas.
 - Podríamos por ejemplo restringir el acceso ssh únicamente desde nuestra máquina del laboratorio.
- Revisar y Crear.
 - Nos pedirá un correo y un teléfono
 - Podéis indicar vuestro correo y un número compatible con un teléfono ('666-666-6XX')



- Podremos acceder mediante SSH
 - Desde windows, podemos usar el subsistema Linux desde el terminal de Windows o putty.
 - Desde Linux podemos utilizar el comando (indicar el fichero con la clave privada y el usuario que hayamos utilizado:
 - `ssh -i azurekey capuser@IP_PÚBLICA`
 - La IP Pública la podemos obtener desde el Dashboard.

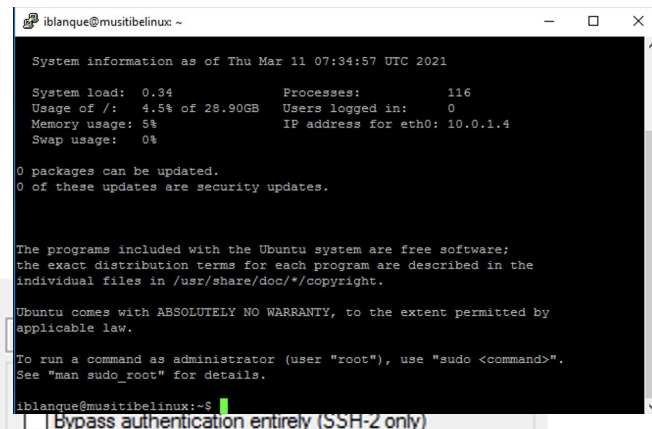
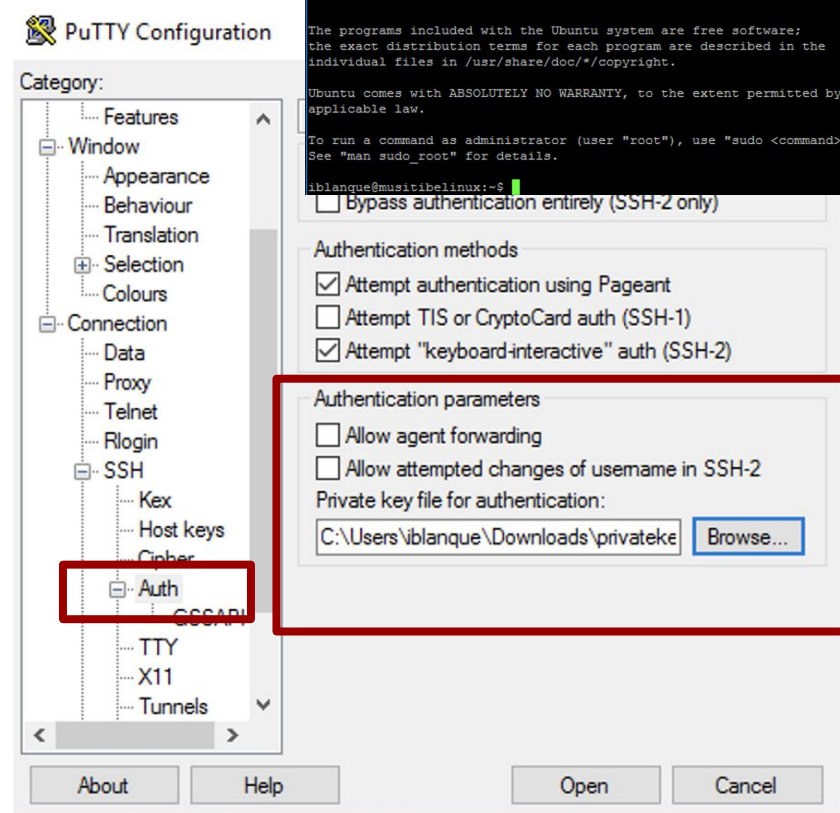
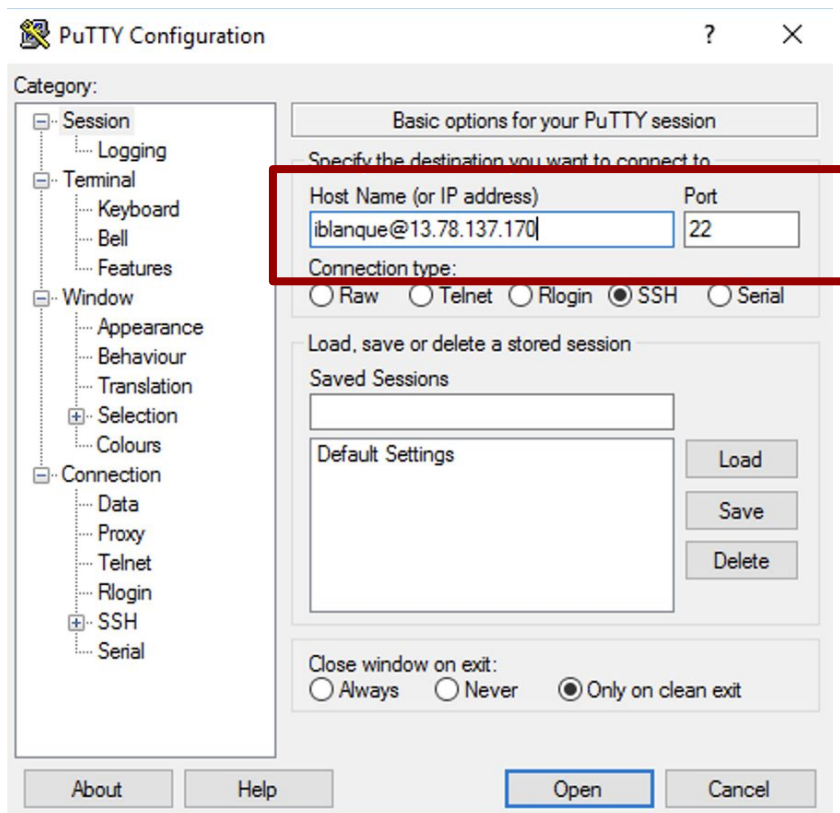


```
Azure — iblanque@mvCAPibe: ~ — ssh -i id_rsa_azure iblanque@52.234.149.10 — 109x34
~/Documents/Docencia/MUINF/CAP/2019-20/Azure — iblanque@mvCAPibe: ~ — ssh -i id_rsa_azure iblanque@52.234.149.10 +
MacBook-Pro-de-Ignacio-2:Azure iblanque$ ssh -i id_rsa_azure iblanque@52.234.149.10
The authenticity of host '52.234.149.10 (52.234.149.10)' can't be established.
ECDSA key fingerprint is SHA256:ch+ixb5obJ61p7L+Q3fFhuybN1/GAMb/oskRuS5Pyn8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.234.149.10' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.4 LTS (GNU/Linux 5.0.0-1031-azure x86_64)

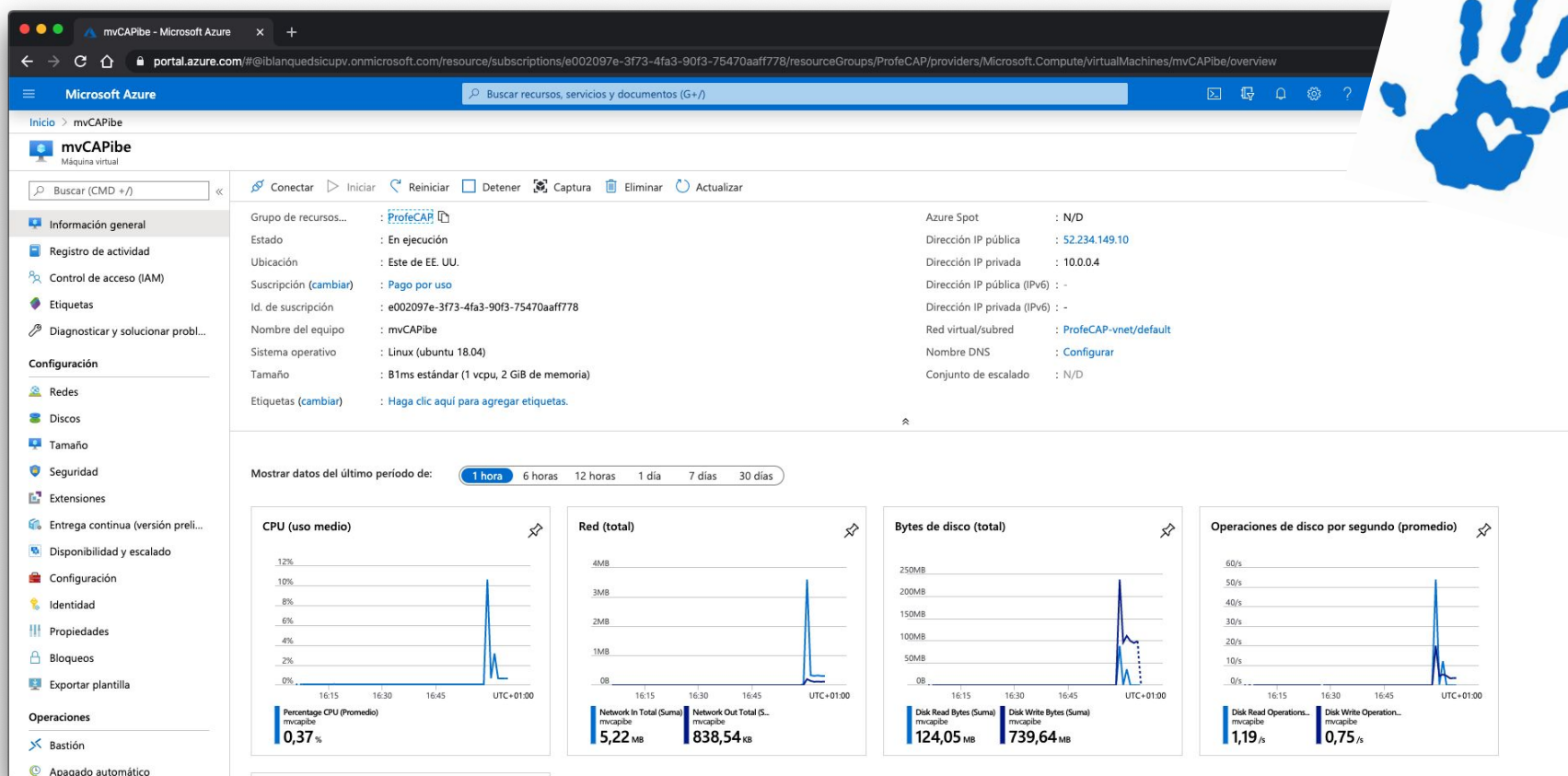
* Documentation:  https://help.ubuntu.com
```

Acceso mediante pares de claves (Windows)

- Accedemos mediante PUTTY, indicando usuario e IP y cargando la clave privada generada en PuttyGen, en la opción SSH/Auth.



Información desde el panel



Configuración de un servidor web

- Poner en funcionamiento una máquina virtual Ubuntu
- Instalar un servidor web apache
 - `sudo apt update`
 - `sudo apt install apache2`
 - Modificar `/var/www/html/index.html`
 - Modificar la línea 224 con nuestro nombre
 - Por ejemplo: `sudo vi /var/www/html/index.html`
- Probar la conexión con un navegador.
- Abrir el puerto correspondiente para que podamos acceder al servidor web.
 - Configuración / Redes / Agregar Regla de seguridad de Entrada
 - Puerto 80 para las conexiones http
- Volver a probar el acceso desde un navegador.



Destruir los recursos



- Si destruimos una máquina, destruiremos únicamente la instancia activa
 - Los discos, IPs, etc. No se destruyen y siguen facturándose.
- Es recomendable ir al Grupo de recursos y destruirlo completamente
 - Inicio, Seleccionar el grupo de Recursos, marcar todo y hacer "Delete Resource Group".

Microsoft Azure portal showing the 'ProfeCAP' resource group. The table lists resources:

Nombre	Tipo	Ubicación
mvCAPibe	Máquina virtual	Este de EE. UU.
mvCAPibe-ip	Dirección IP pública	Este de EE. UU.
mvCAPibe-nsg	Grupo de seguridad de red	Este de EE. UU.
mvcapibe5S8	Interfaz de red	Este de EE. UU.
mvCAPibe_disk1_888fe352b9d34d959a2303b331bd821c	Disco	Este de EE. UU.
ProfeCAP-vnet	Red virtual	Este de EE. UU.
profecapdiag	Cuenta de almacenamiento	Este de EE. UU.

- Azure proporciona máquinas preparadas para funcionar con MPI sobre una red Infiniband.
 - Desde 1€ la hora
- Sin embargo, es posible configurar el MPI entre las instancias convencionales.
- Para ello hay que tener en cuenta los siguientes aspectos
 - Tener en cuenta las limitaciones de los Puertos públicos.
 - Intentar la Máxima proximidad.
 - Configuración apropiada.

- Sólo es posible abrir 100 puertos públicos en las máquinas de Azure
 - Además, el interfaz es bastante manual e incómodo para rangos de puertos.
 - MPI es complejo de configurar para que se limite a un rango de puertos.
 - Si se desea crear un cluster MPI se deben crear todas las máquinas en el mismo grupo y subred.
- Se puede comprobar que entre dos máquinas del mismo grupo están los puertos abiertos, pero no desde el exterior
 - Por ejemplo, ping no funcionará desde fuera, pero sí entre ellas, utilizando las IPs privadas o los nombres internos.

- Instalación y Configuración OPEN MPI
 - Maquina Master
 - La primera máquina (p.e. **<usuario>**MasterMPI) se tiene que instalar tanto los binarios de openmpi como el entorno de desarrollo
 - `sudo apt-get update`
 - `sudo apt-get install -y openmpi-bin libopenmpi-dev gcc`
 - En el resto de máquinas (p.e. **<usuario>**Nodo**<X>**MPI), solamente necesitamos los binarios.
 - `sudo apt-get update`
 - `sudo apt-get install -y openmpi-bin`
 - En la máquina master crearemos un fichero "machinefile" con las IPs privadas de las máquinas.



• Acceso ssh sin contraseña

- Todas las máquinas deberán tener un par de claves ssh y la clave pública en el fichero `authorized_keys`
- Aunque podemos reutilizar las claves disponibles, es más fácil regenerarlas.
- Generación de las claves (p.e. en la máster)
 - `ssh-keygen -m PEM -t rsa -b 4096`
 - Sin contraseña, los ficheros deben estar en el directorio `.ssh` y tener los permisos adecuados.
 - También se podría reaprovechar la clave existente, copiando la clave privada que tenemos en `$HOME/.ssh/id_rsa`, con los permisos adecuados (`chmod 400 id_rsa`)
 - Añadimos la clave pública (contenido de `id_rsa.pub`) al final del fichero `authorized_keys` en el directorio `$HOME/.ssh`.
 - **NO BORRAR LA CLAVE EXISTENTE PORQUE PERDERÍAMOS EL ACCESO.**
- Copiamos el contenido de los tres ficheros en todas las máquinas y con los mismos permisos.
- Comprobamos que funciona
 - `ssh <usuario>Nodo<X>MPI`



Creación de un clúster MPI (3/3)

- Compilamos y ejecutamos el código MPI (Ej. mpihello.c) en la máquina Master.
 - `mpicc -o mpihello mpihello.c`
- Copiamos el ejecutables a cada Nodo MPI donde se tiene que ejecutar
 - `scp mpihello IP_PRIVADA:.`
- Ejecutamos desde la maquina Master el programa MPI
 - `mpirun -machinefile machinefile
-np 4 --oversubscribe mpihello`



- Las diferentes instancias tienen una diferente capacidad de proceso.
- Podemos utilizar diferentes benchmarks
 - HPL(<http://www.netlib.org/benchmark/hpl/>)
 - Linpack(<http://www.netlib.org/benchmark/linpackc>)
- En poliformaT hay una versión modificada del test de linpack de netlib

Comprobar la capacidad de proceso de instancias diferentes

- Ejecutar en dos tipos de instancias la versión modificada de test de linpack de netlib
 - Descargar de poliformaT el fichero `mtlinpack.c`.
 - Elegir dos máquinas diferentes de entre las siguientes que pienses que tendrán diferentes prestaciones:
 - **B1ls, B1ms, B2s, DS2_v3, B4ms**
 - Instalar el compilador de "C"
 - `sudo apt install -y gcc`
 - Copiar y compila el fichero desde la máquina local
 - `scp linpack.tgz -i azurekey capuser@IP_PUB:linpack.tgz`
 - `tar -xzf linpack.tgz`
 - `gcc -O3 -o linpack -DDP -DUNROLL -w linpack.c -lm`
 - Ejecuta el ejecutable de Linpack y compara tiempos (ejecutar un par de veces en cada máquina y obtener la media)
 - `./linpack`
 - Unrolled Double Precision **XXXX** Kflops; 10000 Reps

