

Despliegue de aplicaciones web

Actividad 2.1.4 Creación de máquinas virtuales

CONTENIDO

1.- Objetivos	2
2.- Requisitos previos	2
3.- Calificación	2
4.- Actividades a realizar	3
4.1.- Creación de máquina virtual Linux Ubuntu Server, y conexión a una de las redes.....	3
4.2.- Análisis de recursos asociados a la máquina virtual.	6
4.3.- Conectar por SSH a la máquina virtual	7
4.4.- Creación de máquina virtual Windows Server o Windows 10, y conexión a una de las redes	8
4.5.- Conexión por escritorio remoto a la nueva máquina virtual Windows.....	8
4.6.- Prueba de ausencia de conectividad entre ambas máquinas	9

1.- Objetivos

- Conocer el servicio de máquinas virtuales de Azure.
- Conocer las opciones a la hora de elegir disco para máquinas virtuales, para poder elegir la opción más adecuada de cara a su uso en el aula.
- Conocer las distintas opciones del recurso IP pública para dar acceso a máquinas virtuales.
- Crear una máquina virtual Linux Ubuntu Server, y conectarla a una de las redes creadas.
- Crear una máquina virtual Windows Server / Windows 10, y conectarla a otra de las redes.
- Analizar y comprender los recursos asociados a las máquinas virtuales creadas.
- Probar la conectividad interna, entre máquinas en las diferentes redes virtuales.
- Probar la conectividad desde el exterior a través de IP pública.

2.- Requisitos previos

Que el centro haya proporcionado una cuenta del tipo @iesclaradelrey.es, válida para iniciar sesión en los distintos servicios de Microsoft.

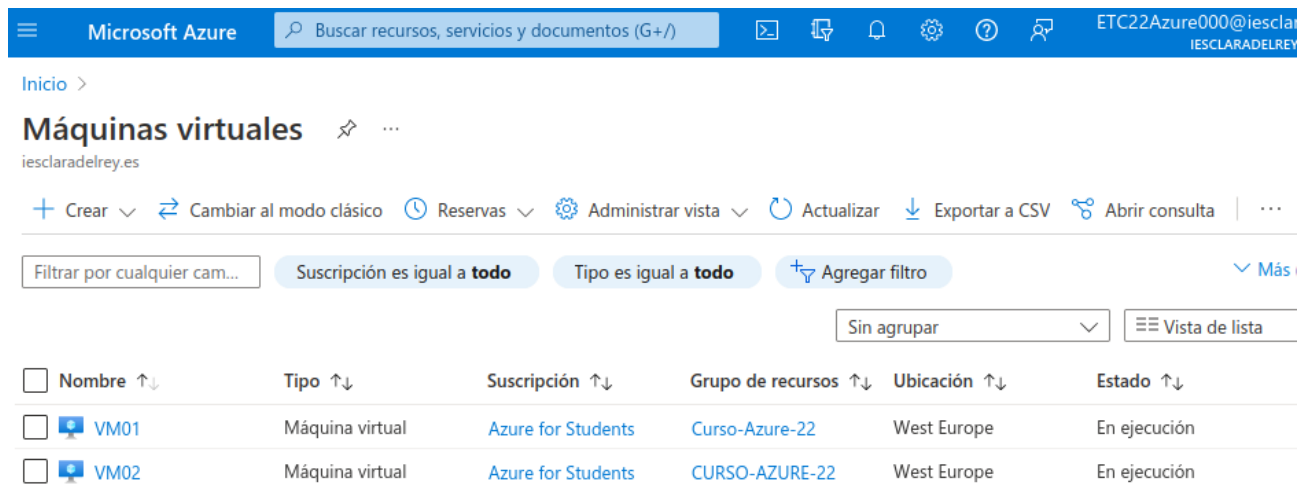
Que se hayan realizado las actividades:

- 1, en la que se activaba la cuenta y la suscripción de Azure for Students.
- 2, en la que se creaban redes virtuales y se emparejaban.

La actividad 3, en la que se creaba un grupo de seguridad de red para proteger las redes, es opcional. Si no se hizo se crearán automáticamente grupos de seguridad para las interfaces de red de las máquinas virtuales.

3.- Calificación

Para superar la actividad bastará con entregar una captura de pantalla en la que se vea el listado de las máquinas virtuales creadas. Algo similar a esto:



Nombre ↑↓	Tipo ↑↓	Suscripción ↑↓	Grupo de recursos ↑↓	Ubicación ↑↓	Estado ↑↓
<input type="checkbox"/> VM01	Máquina virtual	Azure for Students	Curso-Azure-22	West Europe	En ejecución
<input type="checkbox"/> VM02	Máquina virtual	Azure for Students	CURSO-AZURE-22	West Europe	En ejecución

La plataforma Azure es un sistema en constante cambio y evolución, por lo que cualquier captura de pantalla de esta actividad puede ser diferente a la pantalla real actual.

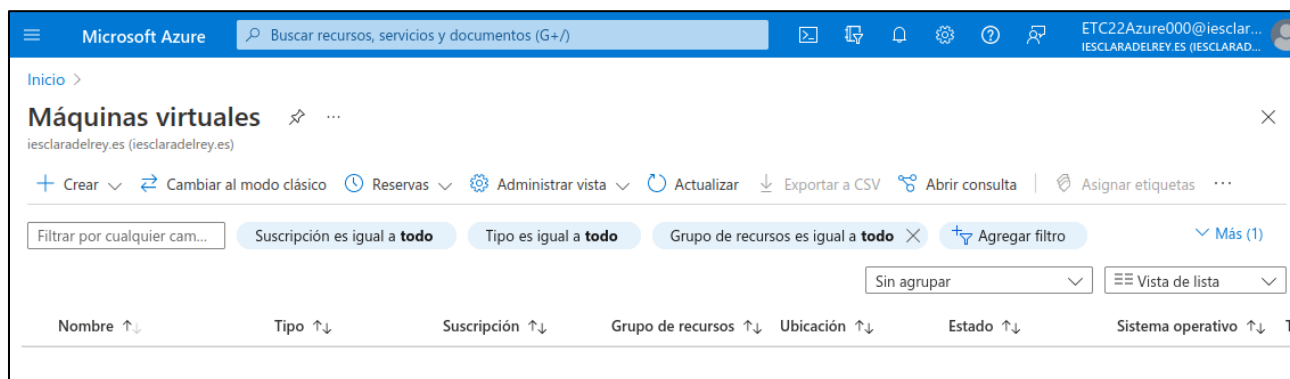
4.- Actividades a realizar

4.1.- Creación de máquina virtual Linux Ubuntu Server, y conexión a una de las redes.

Vamos a:

- Crear una máquina con SO Ubuntu Server 20.04 LTS.
- Conectarla a la subred 192.168.1.0/25. Con IP dinámica (DHCP).
- Crear una IP pública para poder acceder a la máquina.

Accedemos al listado de máquinas virtuales. Si no hemos creado ninguna antes aparecerá vacío.



Hacemos clic en “Crear”

Cuando se van a crear máquinas virtuales, Azure nos da a elegir entre cuatro opciones:

- Máquina virtual de Azure. Esta es la opción que elegiremos normalmente.
- Máquina virtual de Azure con configuración preestablecida. Esta opción es igual que la primera, pero se parte de una configuración sugerida por Microsoft para distintas cargas de trabajo.
- Más máquinas virtuales y soluciones relacionadas. Aquí podremos encontrar soluciones para nubes híbridas, en las que se gestionan de forma unificada máquinas en Azure y máquinas en otras plataformas de virtualización, incluso on premise, y también encontraremos soluciones integradas y predefinidas, similares a las de configuración preestablecida, pero que van un paso más allá para dejar sistemas funcionales completos. Por ejemplo, un servidor LAMP (Linux + Apache + MySQL + PHP)



Como se ha indicado, vamos a trabajar siempre creando una máquina virtual de Azure, y haciendo la configuración completa. Esto nos permite ajustar mejor sus características y el coste final asociado a cada máquina. Cuando hagamos clic en esta opción, Aparecerá un formulario con varias secciones.

En las distintas secciones no siempre aparecen las mismas opciones. Depende de la región geográfica podemos tener o no, por ejemplo, soporte para redundancia de infraestructura.

Vamos a ver qué tenemos que seleccionar en cada una de ellas.

4.1.1.- Datos básicos

- Suscripción y grupo de recursos. Como cualquier recurso de Azure, es imprescindible que elijamos estas dos opciones. El grupo de recursos se puede crear “al vuelo” si deseamos que la máquina se ubique en un nuevo grupo de recursos.
- Nombre de máquina. Será el nombre de la máquina virtual en Azure, pero también el nombre inicial de la máquina en el SO que elijamos.
- Región. Ubicación geográfica de la máquina. Normalmente usaremos la misma para todos los recursos, y la misma que el grupo de recursos.
- Opciones de disponibilidad. Elegiremos “No se requiere redundancia de la infraestructura”. Hay ubicaciones geográficas que permiten redundancia y otras que no.
- Tipo de seguridad. Podemos elegir inicio seguro o estándar. No es relevante de cara a nuestras actividades. Algunas imágenes pueden no ser compatibles con máquinas con seguridad estándar o con máquinas de inicio seguro.
- Imagen. Es la imagen de SO que queremos utilizar. En nuestro caso elegiremos Ubuntu Server 20.04 LTS – Gen2 (puede haber imágenes más modernas, pero mejor trabajar todos con la misma imagen). Bajo este selector hay dos enlaces:
 - Ver todas las imágenes. Esto nos permite navegar y buscar entre todos los SO, distribuciones e imágenes preconfiguradas que hay en Azure (más de 11000 a 15/09/2024). Hay que tener en cuenta que algunas imágenes de SO implican un mayor coste que otras, por cuestiones relacionadas fundamentalmente con licencias o simplemente porque el organismo o empresa que ha montado la imagen quiere rentabilizar su trabajo.
 - Configurar generación de máquinas virtuales. En general, se recomienda utilizar siempre la segunda generación. Sólo se recomienda usar la primera generación si el SO o el disco virtual que se va a usar en una máquina no es compatible con UEFI.
- Arquitectura de VM: Elegiremos x64. Arm64 puede tener mejor rendimiento, pero no todo el software es compatible con esta arquitectura. La arquitectura x64 es en general compatible con un mayor espectro de software.
- Ejecución de Azure Spot con descuento. No lo marcamos. Esto es un modo de provisionar máquinas que no nos garantiza la disponibilidad de estas. En este modo, máquinas con mejores prestaciones, que resultarían más o menos caras, pueden resultar mucho más baratas, a costa de que en un momento dado no tengamos acceso a ellas o Azure decida pararlas para utilizar los recursos para otros clientes.
- Tamaño. Este es el tamaño de la máquina en términos de núcleos, memoria y capacidad de procesamiento o E/S. Para poder ver todos los tamaños y elegir el que más nos convenza podemos:
 - Hacer clic en “Ver todos los tamaños”. Se abrirá una ventana con un listado de tamaños disponibles, agrupados por series. Las series y familias son agrupaciones lógicas que hace Microsoft para categorizar los distintos tamaños de máquinas. Ojo, para cerrar el listado no hay que hacer clic en “Atrás” en el navegador, sino en la X que aparece en la parte superior derecha.
 - En el selector que hay a la derecha, estará seleccionado “agrupar por serie”. Seleccionamos “Sin agrupar”, y ahora podremos ordenar por costo/mes, y podemos elegir la más barata. Para Ubuntu Server un solo núcleo y medio GB de memoria es suficiente para pruebas. Hay que tener en cuenta que no todos los tamaños están disponibles en todas las ubicaciones, y que dependiendo de la imagen de SO seleccionada habrá tamaños no disponibles.
 - Hacer clic en el tamaño que elijamos y clic en “Seleccionar”
- Tipo de autenticación. Hay dos opciones:
 - Contraseña. Esta es la opción que elegiremos en esta actividad.
 - Claves públicas SSH. Esta opción permite generar una clave SSH para el acceso remoto, o usar una ya existente.

- Nombre de usuario. El nombre del usuario sudoer que se creará en la máquina virtual.
- Contraseña y confirmar contraseña. Hay reglas para garantizar cierta fortaleza.
- Reglas de puerto de entrada. Podemos:
 - Ninguno (impedir el acceso desde la red pública). Elegiremos esta opción si ya hemos creado un grupo de seguridad de red que permita el acceso SSH a la red en la que conectaremos la máquina, porque el grupo ya lo hemos configurado correctamente.
 - Permitir acceso a ciertos puertos. Elegiremos esta opción si no hemos creado un grupo de seguridad de red para la red. Tendremos que crear uno para la máquina.

4.1.2.- Discos

- Cifrado del disco de la máquina virtual.
 - Esta opción no aparecerá disponible, porque la suscripción para estudiantes no la admite.
- Disco del SO
 - Tamaño del disco del SO. Aparecerá el predeterminado de la imagen que hayamos elegido, que además es el mínimo que nos dejará seleccionar. Se puede elegir un disco más grande, a un coste que se descontará del crédito.
 - Tipo de disco del SO. Elegir siempre HDD. Los discos SDD y SDD premium son mejores, con más rendimiento, pero también bastante más caros. En general para actividades de formación los HDD son más que suficiente.
 - Eliminar con la VM. Si marcamos esta opción, cuando se elimine la MV se eliminará el disco. Si no lo hacemos, el disco se mantendrá y se seguirá facturando, aunque se elimine la máquina.
 - Administración de claves. Por defecto, Azure cifra automáticamente los discos de datos y de SO que no se estén utilizando, usando una clave privada que administra la propia plataforma (nosotros no la conocemos). Esta opción permitiría usar claves privadas propias, o compartidas con la plataforma, pero implica crear más recursos y configurar más elementos.
 - Habilitar compatibilidad con Ultra Disks: No marcaremos esta opción, reservada para máquinas de producción con sistemas de alto volumen de E/S y necesidades de alta disponibilidad.
- Discos de datos. Se pueden crear discos de datos adicionales, pero de momento sólo usaremos el del sistema.

4.1.3.- Redes

Cuando se crea una MV se crea automáticamente una interfaz de red asociada, que debemos configurar.

- Red y subred virtual. Elegimos la red a la que queremos conectar la máquina. En este caso es la subred 192.168.1.0/25
- IP pública de la interfaz de red. Hay dos opciones:
 - Asignar IP pública. Esta es la opción que vamos a utilizar de momento. Hay dos niveles de servicio:
 - Estándar: IP fija. Es el más compatible con otros servicios de Azure. Implica un pequeño coste mensual.
 - Básico. Puede ser IP fija o dinámica (cambia cuando apagamos y volvemos a encender una máquina virtual). En principio elegiremos este servicio, con IP pública dinámica, y resolveremos los posibles problemas de cambios de IP con los servicios DNS de Azure.
 - No asignar IP pública. No podremos acceder directamente a la máquina desde internet. En ese caso tendríamos dos opciones (entre otras) para conectar a la máquina:
 - Acceder a otra máquina de la red virtual que sí tenga IP pública y permita a su vez otro “salto” a la máquina.

- Usar Azure Bastion, que permite acceder a las máquinas sin IP pública a través de terminales SSH y RDP en el navegador, desde el portal de Azure. Ojo con esta opción, porque requiere más configuración de red, y es cara, pudiendo agotar el crédito de la suscripción muy rápidamente, incluso si no nos conectamos a las máquinas.
- Grupo de seguridad de red. Si ya tenemos configurado un grupo de seguridad en la red a la que conectamos la máquina, no es necesario especificar grupo de seguridad. Si no, podemos crear al vuelo un grupo de seguridad específico para la máquina. En cualquier caso, si se desea, se puede añadir un grupo de seguridad específico para esta interfaz de red.
- Eliminar IP pública y NIC cuando se elimine la máquina. Marcamos esta opción.
- Habilitar redes aceleradas. Según el tipo de imagen y tamaño de máquina elegido, puede estar disponible o no.
- Equilibrio de carga. Elegimos ninguno.

4.1.4.- Administración

- Habilitar identidad administrada asignada por el sistema. No lo marcamos. Es algo que se usa para la integración de nuestra máquina con ciertos servicios.
- Iniciar sesión con Azure Entra ID (antiguo Azure Active Directory). No lo marcamos porque no vamos a usar un directorio activo.
- Apagado automático. Seleccionamos el apagado automático diario, a la hora que más convenga. En el caso de los alumnos de tarde solemos poner las 21h según el horario de Madrid, y no marcamos el envío de email para avisar del apagado.
- Copias de seguridad. No las habilitamos
- Actualizaciones de SO. Dejamos la opción por defecto (valor predeterminado de la imagen).

4.1.5.- Supervisión

- Deshabilitar los diagnósticos de arranque.
- Dejar el resto de las opciones sin seleccionar.

4.1.6.- Finalizar creación de la máquina









Dejar el resto de las secciones (opciones avanzadas y etiquetas) sin cambios, y hacer clic en “Revisar y crear”

Se mostrará un pequeño informe en el que veremos si hay algún error de configuración, y el coste de la máquina por hora. Si todo es correcto, hacer clic en “Crear”.

Cuando se complete la implementación de la máquina virtual se habrán creado todos los recursos necesarios para la máquina, y la máquina estará arrancada.

4.2.- Análisis de recursos asociados a la máquina virtual.

Si en este momento accedemos al listado de todos los recursos creados tendremos algo similar a esto:

<input type="checkbox"/> Nombre ↑↓	Tipo ↑↓	Grupo de recursos ↑↓	Ubicación ↑↓
<input type="checkbox"/>  NetworkWatcher_westeurope	Network Watcher	NetworkWatcherRG	West Europe
<input type="checkbox"/>  NSG-CURSO-AZ	Grupo de seguridad de red	Curso-Azure-22	West Europe
<input type="checkbox"/>  RED-CURSO-AZ-01	Red virtual	Curso-Azure-22	West Europe
<input type="checkbox"/>  RED-CURSO-AZ-02	Red virtual	Curso-Azure-22	West Europe
<input type="checkbox"/>  VM01	Máquina virtual	Curso-Azure-22	West Europe
<input type="checkbox"/>  VM01-IP	Dirección IP pública	Curso-Azure-22	West Europe
<input type="checkbox"/>  vm01717	Interfaz de red	Curso-Azure-22	West Europe
<input type="checkbox"/>  VM01_OsDisk_1_8d05f24f76ac4bbbb8a906c29945be82	Disco	CURSO-AZURE-22	West Europe

Tendremos:

- Un recurso de tipo network watcher. Relacionado con la monitorización de redes y otros recursos, y Azure lo crea automáticamente cuando se crean ciertos recursos, entre otros la redes.
- Dos recursos de tipo red virtual. Las redes creadas en la actividad 2.
- Un recurso de tipo grupo de seguridad de red. El creado en la actividad 3, y con el que regulamos el acceso a las redes.
- Los recursos necesarios para la máquina virtual recién creada:
 - Recurso tipo máquina virtual. El recurso “principal”.
 - Recurso tipo disco. El disco principal o de sistema de la máquina virtual.
 - Recurso tipo interfaz de red. La tarjeta de red con la que la máquina se conecta a la red.
 - Recurso tipo IP pública. La configuración de IP pública de la interfaz de red.

4.3.- Conectar por SSH a la máquina virtual

Ir al listado de máquinas virtuales, y hacer clic en la máquina virtual a la que queremos conectar.

En la pestaña “información general” hacer clic en “Conectar”. Aparecerán distintas opciones de conexión, pero realmente nos sirve con la IP pública, que aparece claramente indicada.

Conectándose mediante
Dirección IP pública | 52.174.141.44

Nombre de usuario del administrador: administrador

Puerto (cambiar) : 22 No se puede comprobar ⓘ

Directiva Just-In-Time : No compatible con el plan ⓘ

Recomendaciones Más comunes

SSH mediante CLI de Azure
Conéctate rápidamente en el explorador. Admite la autenticación Azure AD. La clave privada no es necesaria.
Dirección IP pública (52.174.141.44)
Seleccionar

SSH nativo
No se necesita software adicional. Clave privada necesaria para la conexión. Ideal para aquellos con herramientas SSH existentes.
Dirección IP pública (52.174.141.44)
Seleccionar

Al hacer clic en la opción “SSH nativo”, Azure comprueba si hay impedimentos para conectar a la máquina. Si tenemos grupo de seguridad de red puede indicar que no se puede, pero aun así será posible hacerlo.

También indica los pasos a seguir para conectar, pero no necesariamente serán los adecuados. Cada sistema operativo o distribución puede usar distintos clientes ssh.

Es posible que Azure sugiera un comando ssh para conectar usando claves ssh:

```
ssh -i <ruta de acceso de clave privada> usuario@ip
```

Pero como vamos a conectar usando usuario y contraseña, usaremos

```
ssh usuario@ip
```

4.4.- Creación de máquina virtual Windows Server o Windows 10, y conexión a una de las redes

Vamos a:

- Crear una máquina con SO Windows. Podemos usar Windows Server o Windows cliente (10, por ejemplo), pero hay que tener en cuenta:
 - En Windows Server, hay muchas imágenes de este SO. Para elegir una, intentar elegir una que tenga UI, no elegir las versiones “Core”, que no tienen UI.
 - Para Windows 10, hay que tener en cuenta que, por seguridad, no admiten por defecto la conexión de escritorio remoto, a no ser que sea en modo administrador.
- Conectarla a la subred 10.0.0.0/8. Con IP dinámica (DHCP).
- Crear una IP pública para poder acceder a la máquina.

Seguir los mismos pasos que para la máquina Linux, pero hay que tener en cuenta algunas diferencias:

- No todos los tamaños de máquina son válidos para todas las imágenes, así que habrá que elegir entre los tamaños disponibles.
- En reglas de entrada no permitiremos ningún puerto, pero esto es así porque los hemos habilitado a través del grupo de seguridad de red asociado a las redes creadas en la actividad 2.
- En el caso de máquinas Windows, se puede usar licencias compradas previamente, o que la máquina incluya el coste de licencia.

Una vez creada la máquina virtual aparecerá en el listado de máquinas virtuales y ya estará arrancada.

4.5.- Conexión por escritorio remoto a la nueva máquina virtual Windows

Ir al listado de máquinas virtuales, y hacer clic en la máquina virtual a la que queremos conectar.

En la pestaña “información general” hacer clic en “Conectar”. Aparecen distintas opciones de conexión, entre ellas uso de RDP.

Conectándose mediante
Dirección IP pública | 13.80.5.58

Nombre de usuario del administrador
administrador

Puerto (cambiar)
3389 [Comprobación de acceso](#)

Directiva Just-In-Time
No compatible con el plan

Más comunes

RDP nativo
Conéctese a través de RDP nativo sin necesidad de software adicional. Recomendado solo para pruebas.
Dirección IP pública (13.80.5.58)
[Seleccionar](#)

Configurar los requisitos previos para RDP nativo
Azure debe configurar algunas características para conectarse a la máquina virtual.

No se pudieron configurar los requisitos previos

Acceso al puerto 3389
No se puede configurar Just-In-Time en la máquina virtual: "La directiva JIT estándar no está configurada en esta máquina virtual." [Más información](#)

Cambie el puerto para conectarse a esta máquina virtual en la página Conectar de la máquina virtual.

Dirección IP pública: 13.80.5.58
Se requiere una dirección IP pública para conectarse a través de este método de conexión.
[Configurar](#)

2 Abrir conexión a Escritorio remoto (en Windows)
Abrir la conexión a Escritorio remoto o cambiar el sistema operativo de la máquina local para ver más instrucciones. [Más información](#)

3 Descargar y abrir el archivo RDP
Descargar y abrir el archivo RDP para conectarse a la máquina virtual.

Username
administrador [Copiar](#)

[Descargar archivo RDP](#)

Otra información

Azure comprueba si hay algún impedimento para conectar a la máquina, y si lo hay lo indica.

Aparecerá la IP pública y el puerto al que tenemos que conectarnos.

También podemos descargar el fichero de conexión RDP. Si tenemos un cliente de escritorio remoto asociado al tipo de fichero RDP, podremos conectar haciendo doble clic en el fichero.

En el caso de Windows 10 (y otras versiones de Windows “cliente”), como por defecto no se admite la conexión por RDP, se puede usar el siguiente comando para conectar con permisos de administración:

```
mstsc -v <ip-de-la-máquina> /admin
```

4.6.- Prueba de ausencia de conectividad entre ambas máquinas

Aunque las dos máquinas estén alojadas en Azure, y dentro de la misma suscripción, zona, y grupo de recursos, si las hemos ubicado en distintas redes, no se podrá alcanzar una máquina desde la otra.

Para ver la dirección IP interna asignada a cada una de las máquinas, tenemos dos opciones:

- Consultar el portal de Azure, en el que se puede ver la IP interna y la IP pública de cada una de las máquinas.

 **Interfaz de red: vm02214** [Reglas de seguridad vigentes](#) [Solucionar problemas de conexión de VM](#) [Topología](#)
Red virtual/subred: RED-CURSO-AZ-02/RED-CURSO-AZ-02A IP pública de NIC: **137.117.142.191** IP privada de NIC: **10.0.0.4**

- Utilizar un comando en las máquinas virtuales para consultar la configuración de la red:
 - En Linux: `ip -a`
 - En Windows: `ipconfig`

Una vez obtenidas las IP de cada una de las máquinas, podemos intentar hacer ping desde la máquina Linux a la máquina Windows, y viceversa, y veremos que no se recibe respuesta.

Por ejemplo, desde la máquina Linux a la máquina Windows:

```
administrador@LINUX-01:~$ ping 10.0.0.4
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
^C
--- 10.0.0.4 ping statistics ---
124 packets transmitted, 0 received, 100% packet loss, time 125930ms
```

Y desde la máquina Windows a la máquina Linux:

```
Pinging 192.168.0.4 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.0.4:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```