Actividad 2.1.5
Interconexión (emparejamiento) de redes virtuales

CONTENIDO

1.- Objetivos

- Emparejar (interconectar) las redes virtuales creadas.
- Profundizar en el concepto de servicios en internet, y puertos TCP o UDP.
- Profundizar en el concepto de grupo de seguridad de red, y configurar reglas de acceso ICMP para las redes creadas.

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:

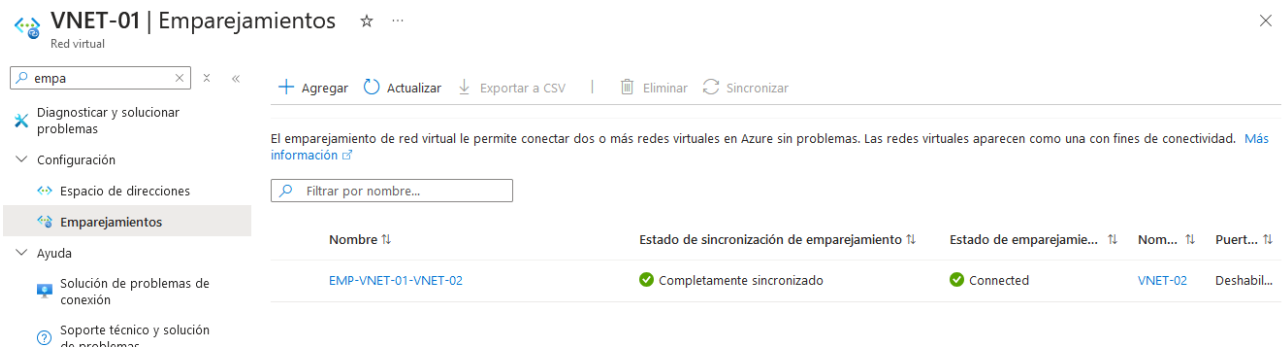
- En la que se activaba la cuenta y la suscripción de Azure for Students.
- En la que se creaban redes virtuales.
- En la que se configuraba la seguridad de la red.
- En la que se creaban máquinas virtuales.

3.- Calificación

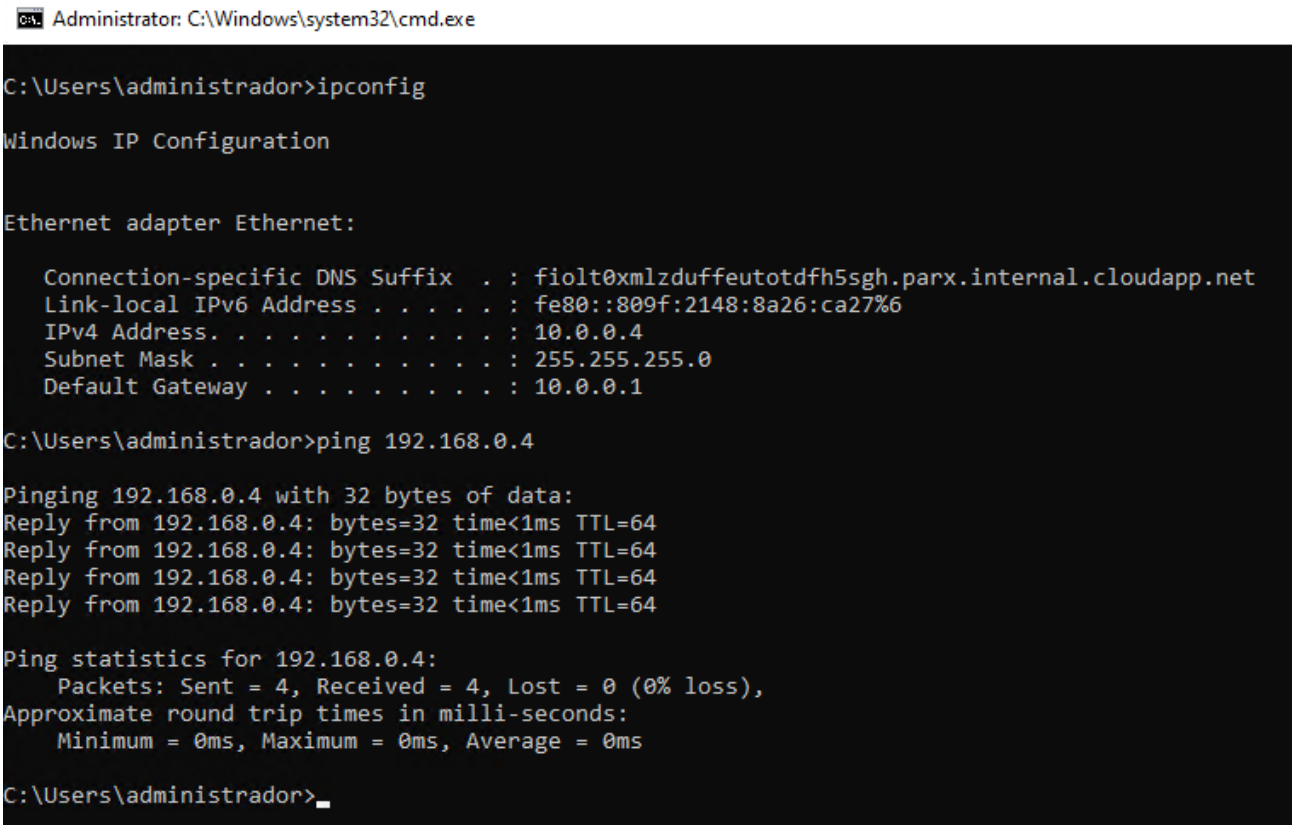
Para superar la actividad se deberán entregar seis capturas de pantalla:

- Pantalla de configuración de emparejamientos de la primera red
- Pantalla de configuración de emparejamientos de la segunda red
- Pantalla con un ping con éxito desde la máquina de la primera red a la segunda. En la captura debe aparecer también la IP de la máquina de la primera red, con un comando *ip a* (en Linux) o *ipconfig* (en Windows)
- Pantalla con un ping con éxito desde la máquina de la segunda red a la primera. En la captura debe aparecer también la IP de la máquina de la segunda red, con un comando *ip a* (en Linux) o *ipconfig* (en Windows)
- Pantalla con un ping con éxito desde el pc del centro (o portátil propio) a la máquina de la primera red. Debe aparecer también la IP de la máquina local desde la que estamos haciendo la conexión.
- Pantalla con un ping con éxito desde el pc del centro (o portátil propio) a la máquina de la segunda red. Debe aparecer también la IP de la máquina local desde la que estamos haciendo la conexión.

Ejemplo de captura de pantalla de la configuración de emparejamiento:



Ejemplo de capturas de pantallas con ping con éxito entre máquinas:



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.- Revisión del estado inicial

Arrancar las dos máquinas virtuales creadas (Linux y Windows).

Verificar y anotar para su uso posterior las IP asignadas, tanto internas como externas (públicas).

En este punto, deberíamos tener lo siguiente

- Red 1: un espacio de direcciones (192.198.1.0/24)
  - Subred 1.1: 192.168.1.0/25
  - Subred 1.2: 192.168.128/25
- Red 2: dos espacios de direcciones (10.0.0.0/8 y 172.16.0.0/12)
  - Subred 2.1: 10.0.0.0/8
  - Subred 2.2: 172.16.0.0/12

La visibilidad entre máquinas conectadas a estas redes sería la siguiente:

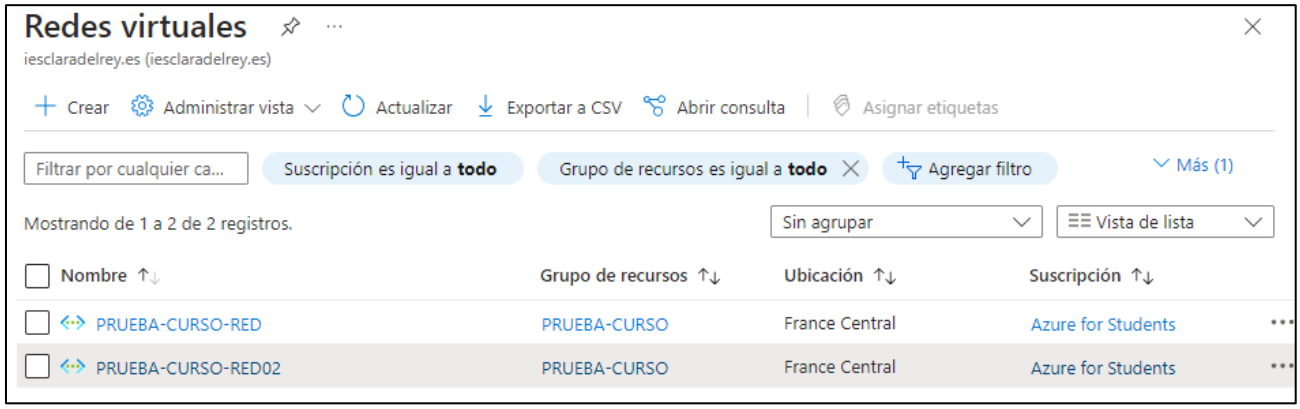
	SUBRED 1.1	SUBRED 1.2	SUBRED 2.1	SUBRED 2.2
SUBRED 1.1	SI	SI	NO	NO
SUBRED 1.2	SI	SI	NO	NO
SUBRED 2.1	NO	NO	SI	SI
SUBRED 2.2	NO	NO	SI	SI

Verificar con comandos ping en ambas máquinas que no hay conectividad entre ellas.

4.2.- Emparejamiento (interconexión) de redes virtuales

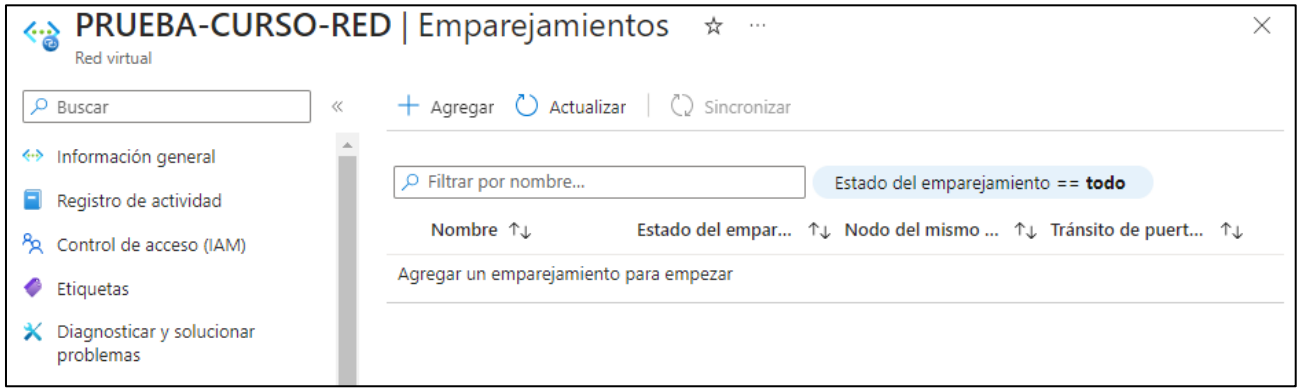
Para que las máquinas en la red 1 puedan ver las de la red dos y/o viceversa, se tiene que realizar lo que en Azure se denomina “Emparejamiento de redes”.

Para hacerlo, se accede, en el menú de Azure, a la página de redes virtuales, o se busca en el buscador general de Azure esta página. Aparece el listado de las redes (no las subredes) creadas.



Hacemos clic en cualquiera de las redes que queremos emparejar. Una vez en la página de la red virtual, hacemos clic en la opción del menú “Emparejamientos”.

Aparecerá el listado vacío de emparejamientos:



Hacemos clic en “Agregar” y completamos el formulario.

Primero, aunque no son los primeros campos del formulario, elegimos la red remota:

Y seleccionamos:

- Modelo de implementación:
  - Resource manager (modelo actual, desde 2014, permite más funciones)
  - Classic (en desuso, pero todavía disponible)

  En nuestro caso habremos creado las redes como ARM (Azure Resource Manager) por lo que elegimos esta opción, que estará seleccionada por defecto.

- Suscripción: estará seleccionada por defecto Azure for Students
- Red Virtual: seleccionamos la red virtual con la que queremos conectar

En este punto en el formulario ya aparecerán identificadas las redes por su nombre, lo que hace más fácil tomar decisiones. Vamos a suponer que se denominan RED-A (desde donde estamos creando el emparejamiento) y RED-B (la red emparejada).

Habrá que responder primero a las siguientes preguntas de RED-B:

- Nombre de emparejamiento de RED-B a RED-A. Es descriptivo, no tiene relevancia funcional, pero hay normas a seguir.
- Permitir RED-B acceder a RED-A: permite tráfico desde RED-B a RED-A.

- Permitir RED-B para recibir el tráfico reenviado desde RED-A: permite a RED-B recibir tráfico desde otras redes virtuales que están emparejadas con RED-A.
- Permitir que la puerta de enlace en RED-B reenvíe el tráfico a RED-A: Si estamos usando una puerta de enlace en RED-B, esta puerta de enlace podrá enviar tráfico a RED-A.
- Habilitar RED-B para usar la puerta de enlace remota de RED-A: sólo se puede usar si la red emparejada tiene puerta de enlace remota y tiene activadas algunas opciones para permitir el reenvío. Permite que desde las máquinas de RED-B se use la puerta de enlace remota de RED-A.

Y ahora a las de RED-A. Estas son iguales que la red B, pero a la inversa, para habilitar los mismos tipos de tráfico en sentido contrario.

En esta actividad simplemente habilitaremos el tráfico desde la RED A hacia la red B y viceversa, pero sois libres de marcar más opciones, aunque en principio no tendrán consecuencias para nosotros.

Clic en “Agregar”. Esto creará los emparejamientos que permitirán el tráfico de red entre las dos redes, según las normas que hayamos establecido. Se crean dos emparejamientos, uno en la RED-A y otro en la RED-B.

Comprobar, entrando en la configuración de ambas redes, que se han creado los emparejamientos.

4.3.- Comprobación de los emparejamientos

Una vez creados los emparejamientos, debería haber conectividad entre ellas. Recordemos que antes de crear los emparejamientos los comandos ping no alcanzaban a las máquinas en la otra red.

Si hacemos un ping desde la máquina Windows (10.0.0.4) a la máquina Linux (192.168.1.4) debería responder.

```
Pinging 192.168.1.4 with 32 bytes of data:
Reply from 192.168.1.4: bytes=32 time=1ms TTL=64
Reply from 192.168.1.4: bytes=32 time<1ms TTL=64
Reply from 192.168.1.4: bytes=32 time=1ms TTL=64
Reply from 192.168.1.4: bytes=32 time=1ms TTL=64

Ping statistics for 192.168.1.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Pero el ping de Linux a Windows lo más probable es que no funcione. Esto es porque en Windows hay que configurar el firewall para que responda a los paquetes ICMP del ping.

```
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
^C
--- 10.0.0.4 ping statistics ---
10 packets transmitted, 0 received, 100% packet loss, time 9200ms
```

Windows tiene por defecto activadas una serie de reglas para evitar el acceso a ciertos puertos TCP/UDP.

Para habilitar las respuestas ICMP hay que activar en el firewall de Windows la regla de entrada “File and Printer Sharing (Echo Request - ICMPv4-In)”. Una vez habilitada, ya funcionará el ping.

```
PING 10.0.0.4 (10.0.0.4) 56(84) bytes of data.
64 bytes from 10.0.0.4: icmp_seq=1 ttl=128 time=3.02 ms
64 bytes from 10.0.0.4: icmp_seq=2 ttl=128 time=1.12 ms
64 bytes from 10.0.0.4: icmp_seq=3 ttl=128 time=1.15 ms
64 bytes from 10.0.0.4: icmp_seq=4 ttl=128 time=7.57 ms
64 bytes from 10.0.0.4: icmp_seq=5 ttl=128 time=4.69 ms
```

Y así comprobamos que el emparejamiento que realizamos en la actividad 2 funciona correctamente.

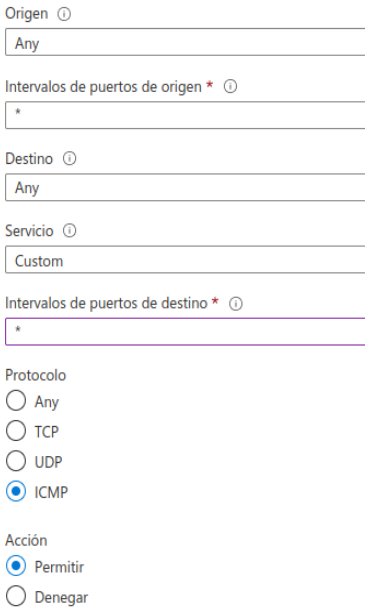
4.4.- Añadir regla de entrada para ICMP en el grupo de seguridad de red

Si desde el exterior hacemos un ping a la IP pública de cualquiera de las dos máquinas, no funcionará.

Esto es, otra vez, porque tenemos restringido el tráfico de paquetes ICMP, pero en esta ocasión la restricción está en el grupo de seguridad de red.

Vamos a abrir el tráfico ICMP en el grupo de seguridad de red para que podamos hacer ping a las IP públicas.

- Abrir la página con el listado de grupos de seguridad de red y hacer clic en el nombre de nuestro grupo.
- Hacer clic en el menú del grupo de seguridad en la opción “Reglas de seguridad de entrada”
- Hacer clic en “Agregar”.
- Completar la regla de forma similar a las que creamos previamente para RDP o SSH, pero teniendo en cuenta que en este caso el protocolo tiene que ser ICMP.
- Pulsar “Agregar”.



El ping a las IP públicas debería funcionar ahora.