



Máster en Ingeniería MultiCloud, DevOps y Seguridad.

AZURE LAB #5

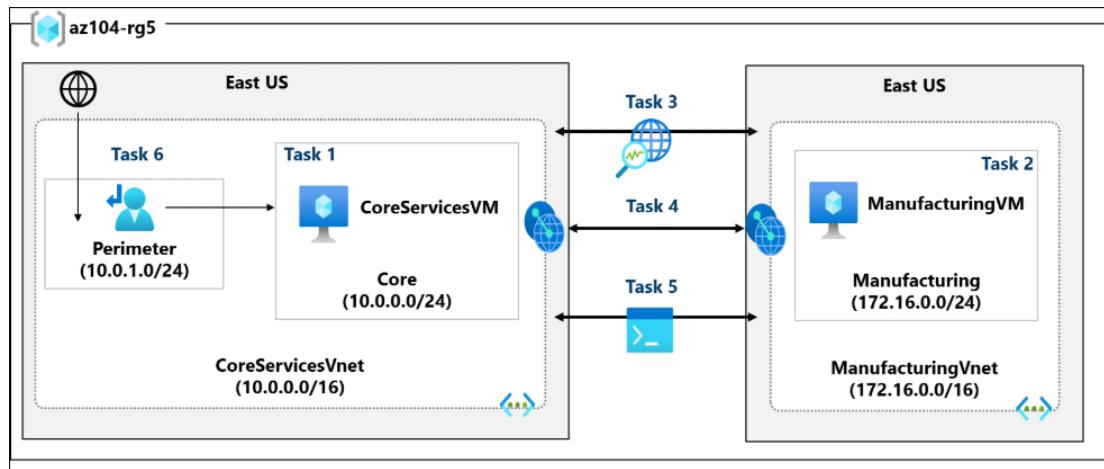
# Implementación de la conectividad entre sitios



## Contenido

Esquema del laboratorio .....	3
Creación de una máquina virtual de servicios principales y una red virtual.....	4
Cree una máquina virtual en otra red virtual.....	9
Utilizar Network Watcher para probar la conexión entre máquinas virtuales .....	11
Configuración de peering de redes virtuales entre redes virtuales .....	14
Uso de Azure PowerShell para probar la conexión entre máquinas virtuales .....	17
Creación de un route personalizado.....	18

## Esquema del laboratorio





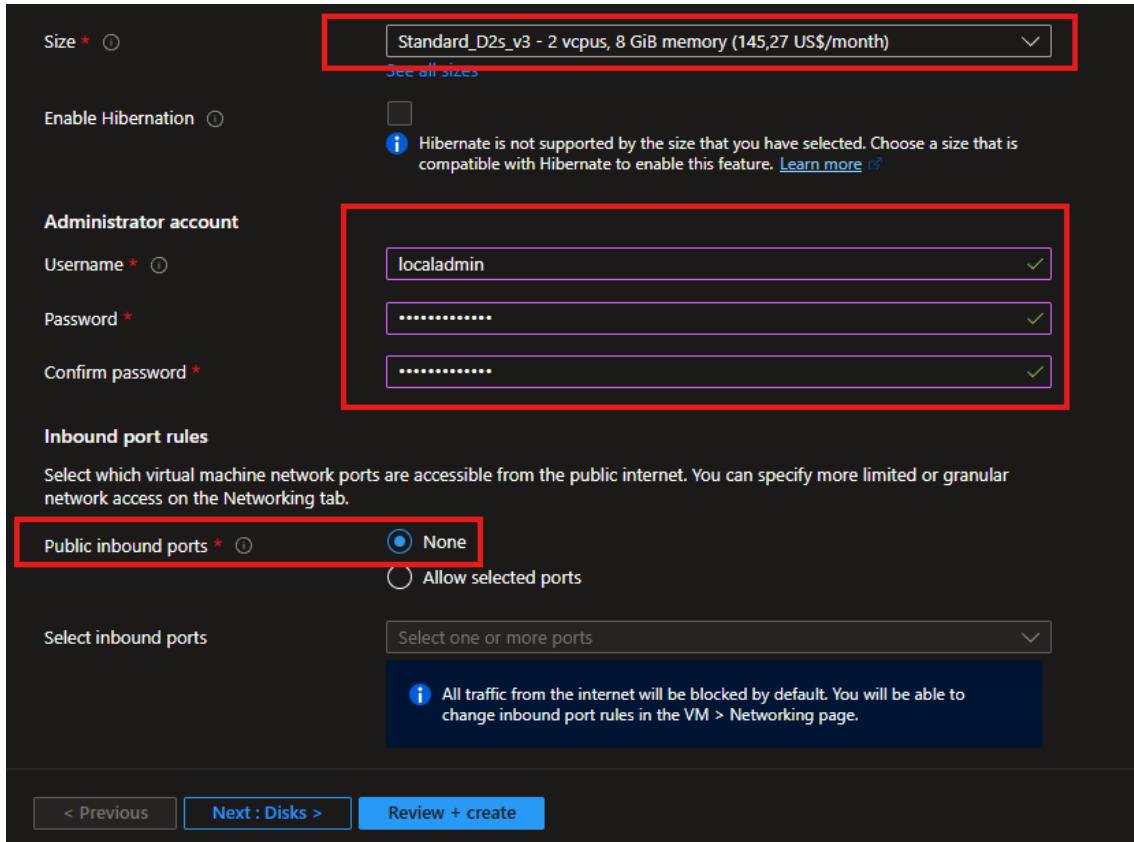
## Creación de una máquina virtual de servicios principales y una red virtual

The screenshot shows the 'Create a virtual machine' wizard in the Azure portal. The 'Basics' tab is selected. In the 'Project details' section, the 'Subscription' dropdown is set to 'Azure for Students' and the 'Resource group' dropdown is set to 'az104-rg5'. In the 'Instance details' section, the 'Virtual machine name' is 'CoreServicesVM', 'Region' is '(Europe) Spain Central', 'Availability options' is 'No infrastructure redundancy required', 'Security type' is 'Standard', and 'Image' is 'Windows Server 2019 Datacenter - x64 Gen2'. A red box highlights the 'Resource group' and 'Virtual machine name' dropdowns.

Comenzamos creando la máquina virtual para los servicios principales, previamente he creado un grupo de recursos az104-rg5 donde voy a desplegar todos los recursos para el laboratorio.

Esta máquina virtual va a ser un windows server.

## AZURE LAB #5



The screenshot shows the Azure VM creation interface. Key highlighted sections include:

- Size:** Standard\_D2s\_v3 - 2 vcpus, 8 GiB memory (145,27 US\$/month). A red box highlights the dropdown menu.
- Administrator account:** Username: localadmin, Password: (redacted), Confirm password: (redacted). A red box highlights the password fields.
- Inbound port rules:** Public inbound ports: None (radio button selected). A red box highlights the radio button. A tooltip indicates that all traffic from the internet will be blocked by default.

Tamaño: Standard\_D2s\_v3 Rendimiento equilibrado: Ofrece 2 vCPUs y 8 GiB de RAM

Cuenta de Administrador (Administrator account): El Username es localadmin.

Reglas de Puerto de Entrada (Inbound port rules):

En la opción Public inbound ports (Puertos de entrada públicos), se ha seleccionado None (Ninguno).

Esto significa que no hay puertos accesibles desde el internet público de forma predeterminada.



## AZURE LAB #5

Home > Compute infrastructure | Virtual machines >

## Create a virtual machine

Help me choose the right VM size for my workload Help me create a low cost

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size

Basics Disks Networking Management Monitoring Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

**VM disk encryption**

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host  (i) Encryption at host is not registered for the selected subscription. [Learn more](#)

**OS disk**

OS disk size  Image default (127 GiB)

OS disk type \*  Premium SSD (locally-redundant storage)

Delete with VM

Key management  Platform-managed key

Enable Ultra Disk compatibility  Ultra disk is supported in Availability Zone(s) 2 for the selected VM size Standard\_D2s\_v3.

**Data disks for CoreServicesVM**

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM
					<input type="checkbox"/>

Create and attach a new disk Attach an existing disk

< Previous Next : Networking > Review + create

En la configuración de los discos duros de la máquina virtual los dejo como vienen por defecto.



## AZURE LAB #5

Home > Compute infrastructure | Virtual machines > Create a virtual machine >

vnet-spaincentral ...

Name \* CoreServicesVnet

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

+ Add a subnet

10.0.0.0/16

10.0.0.0 /16 65.536 addresses

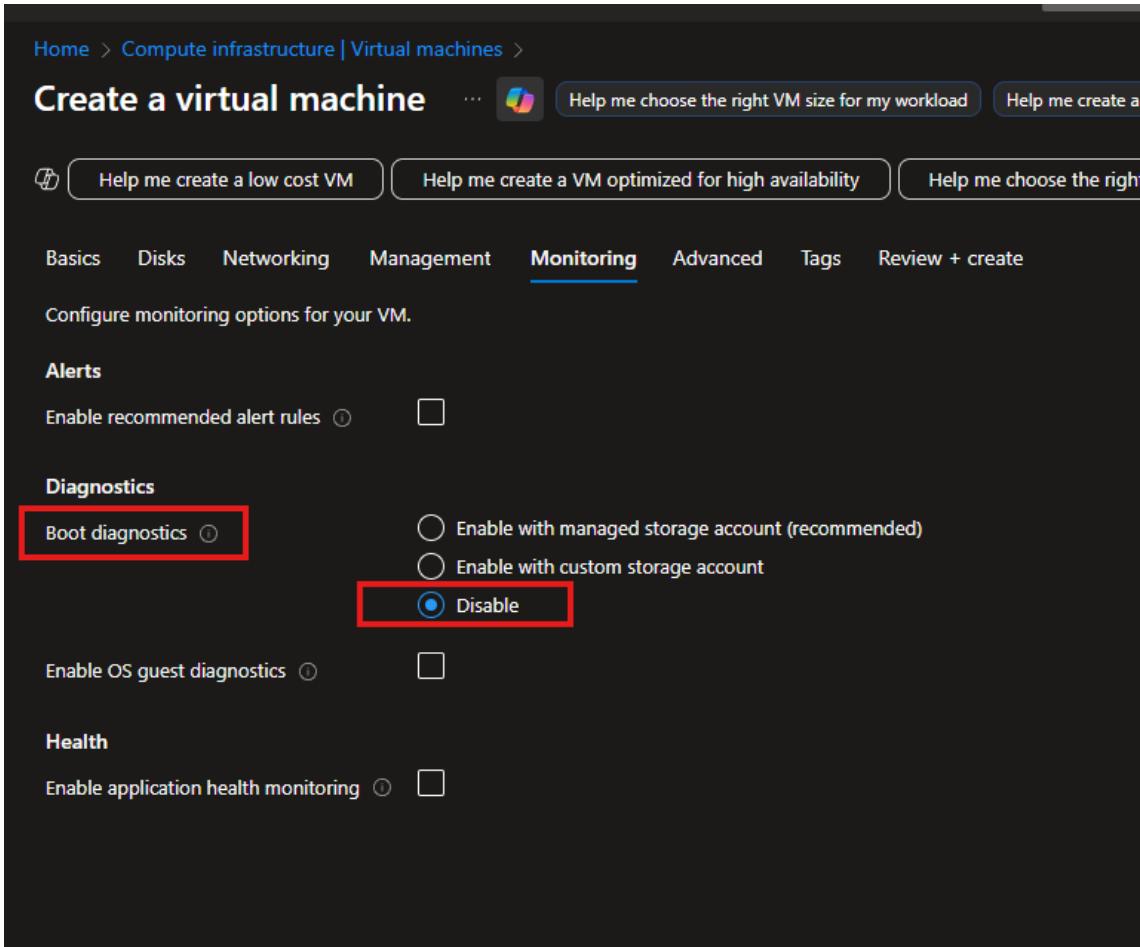
Subnets IP address range Size NAT gateway

Subnets	IP address range	Size	NAT gateway
Core	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

Add IPv4 address space | ▾

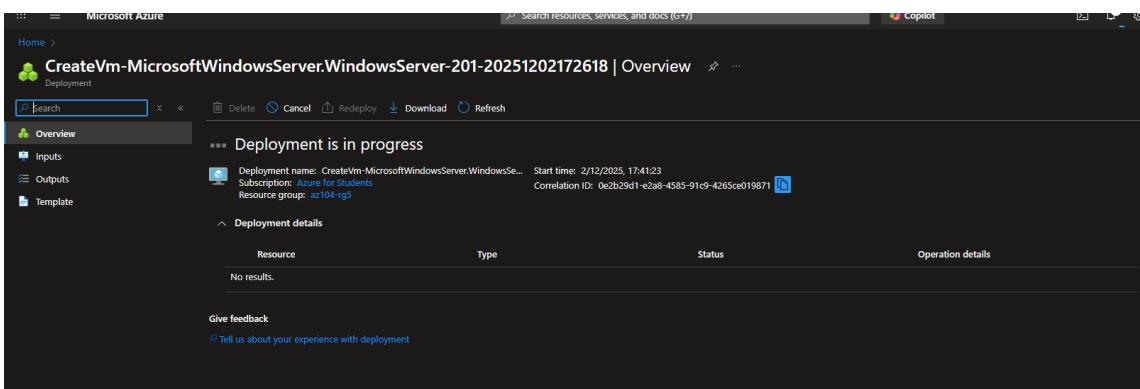
Creo la red y la subred para la máquina virtual.

 tajamar.	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #5	



The screenshot shows the Azure portal interface for creating a virtual machine. The 'Monitoring' tab is selected. In the 'Diagnostics' section, the 'Boot diagnostics' option is highlighted with a red box. Below it, there are two radio button options: 'Enable with managed storage account (recommended)' and 'Disable'. The 'Disable' option is selected and also highlighted with a red box. Other sections like 'Alerts' and 'Health' are visible but not highlighted.

Deshabilito el boot diagnostics para ahorrar costos de almacenamiento y, en algunos casos, para reducir el tiempo de aprovisionamiento.



The screenshot shows the Azure portal's deployment overview for a deployment named 'CreateVm-MicrosoftWindowsServer.WindowsServer-201-20251202172618'. The status bar at the top indicates 'Deployment is in progress'. The deployment details table shows one row: 'Resource' (Windows Server 2025), 'Type' (Virtual Machine), 'Status' (Creating), and 'Operation details' (No results). There is a feedback link at the bottom: 'Give feedback' and 'Tell us about your experience with deployment'.

Creo la máquina virtual.



## Cree una máquina virtual en otra red virtual

Home > Compute infrastructure | Virtual machines >

Create a virtual machine

Help me create a VM optimized for high availability Help me choose the right VM

Help me create a low cost VM Help me create a VM optimized for high availability Help me choose the right VM size for my needs

This subscription may not be eligible to deploy VMs of certain sizes in certain regions.

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*  Create new

**Instance details**

Virtual machine name \*

Region \*  Deploy to an Azure Extended Zone

Availability options

Security type

Image \*  See all images | Configure VM generation

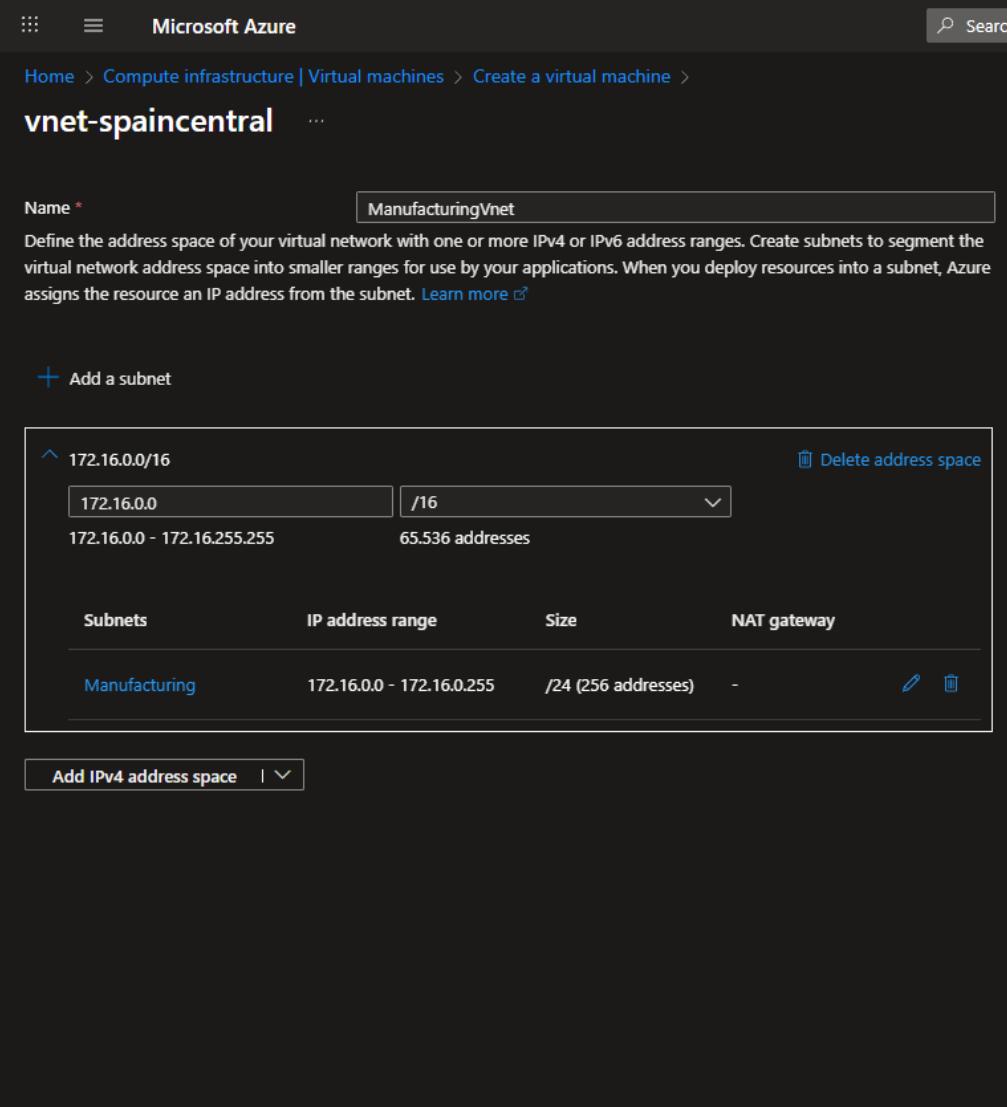
This image is compatible with additional security features. [Click here to swap to the Trusted launch security type.](#)

VM architecture  x64

Arm64 is not supported with the selected image.

Creamos la máquina virtual con las mismas características que la anterior solo que con un nombre diferente y en una red diferente.

 tajamar.	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #5	



Name \* ManufacturingVnet

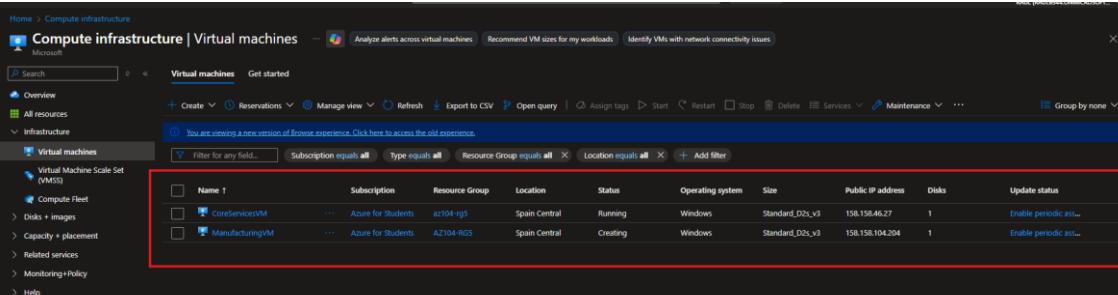
Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Create subnets to segment the virtual network address space into smaller ranges for use by your applications. When you deploy resources into a subnet, Azure assigns the resource an IP address from the subnet. [Learn more](#)

+ Add a subnet

Subnets	IP address range	Size	NAT gateway
Manufacturing	172.16.0.0 - 172.16.0.255	/24 (256 addresses)	-

Add IPv4 address space |

Red virtual y subred sobre la que trabaja la máquina virtual.



Name	Subscription	Resource Group	Location	Status	Operating system	Size	Public IP address	Disk	Update status
CoreServicesVM	Azure for Students	az104_rg5	Spain Central	Running	Windows	Standard_D2s_v3	158.158.46.27	1	Enable periodic ass...
ManufacturingVM	Azure for Students	AZ104-RG5	Spain Central	Creating	Windows	Standard_D2s_v3	158.158.104.294	1	Enable periodic ass...

Comprobamos que ambas máquinas virtuales han sido creadas y sus respectivas redes.



## Utilizar Network Watcher para probar la conexión entre máquinas virtuales

Network Watcher es un servicio de diagnóstico y supervisión de red en Azure que te permite analizar, medir y verificar el estado y la configuración de los recursos de red de tu máquina virtual (VM).

The screenshot shows the Microsoft Azure portal interface for the Network Watcher service. The top navigation bar includes the Microsoft Azure logo, a three-dot menu, and a three-line menu icon. Below the navigation bar, the breadcrumb trail shows 'Home > Network Watcher'. The main content area features a 'Search' bar with a magnifying glass icon. On the left, there is a sidebar with several options: 'Overview' (selected and highlighted in blue), 'Get started', 'Monitoring', 'Network diagnostic tools' (expanded), 'IP flow verify', 'NSG diagnostics', 'Next hop', 'Effective security rules', 'VPN troubleshoot', 'Packet capture', 'Connection troubleshoot' (highlighted with a red box), 'Metrics', and 'Logs'. The 'Connection troubleshoot' option is specifically highlighted with a red rectangular box.

Accedemos a connection troubleshoot desde el servicio de network watcher.



## AZURE LAB #5

Connection troubleshoot ...

tests\*. Learn more. ⓘ

**Source**

Source type \* ⓘ Virtual machine

Virtual machine \* ⓘ CoreServicesVM Select virtual machine

**Destination**

Destination type ⓘ  Select a virtual machine  Specify manually

Virtual machine \* ⓘ ManufacturingVM Select virtual machine

**Probe settings**

Preferred IP version ⓘ Both

Protocol ⓘ  TCP  ICMP

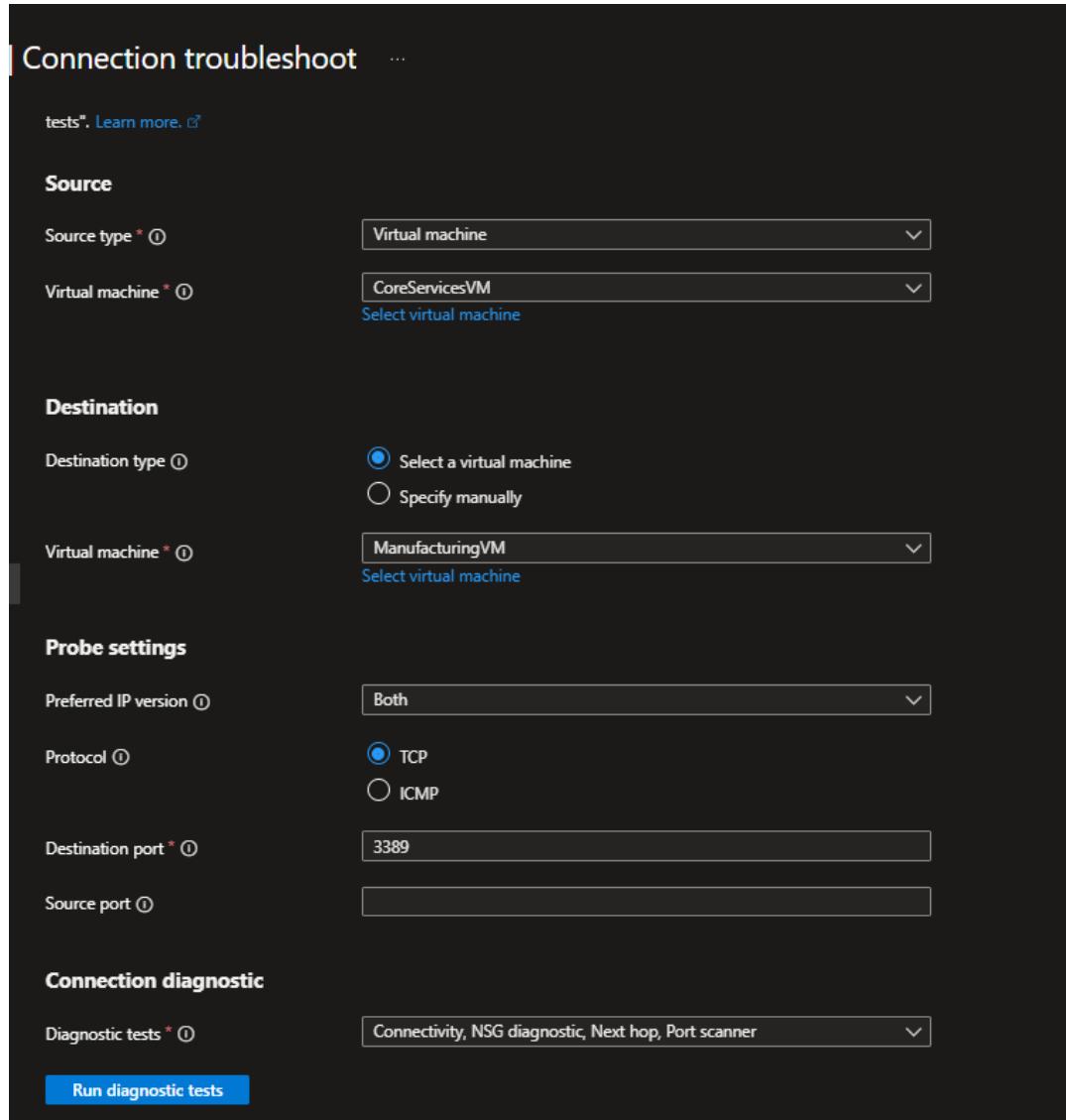
Destination port \* ⓘ 3389

Source port ⓘ

**Connection diagnostic**

Diagnostic tests \* ⓘ Connectivity, NSG diagnostic, Next hop, Port scanner

**Run diagnostic tests**



Estoy usando Network Watcher para que Azure me diga, punto por punto, qué firewall, regla o configuración de red está bloqueando mi acceso RDP al servidor que es el puerto de destino.



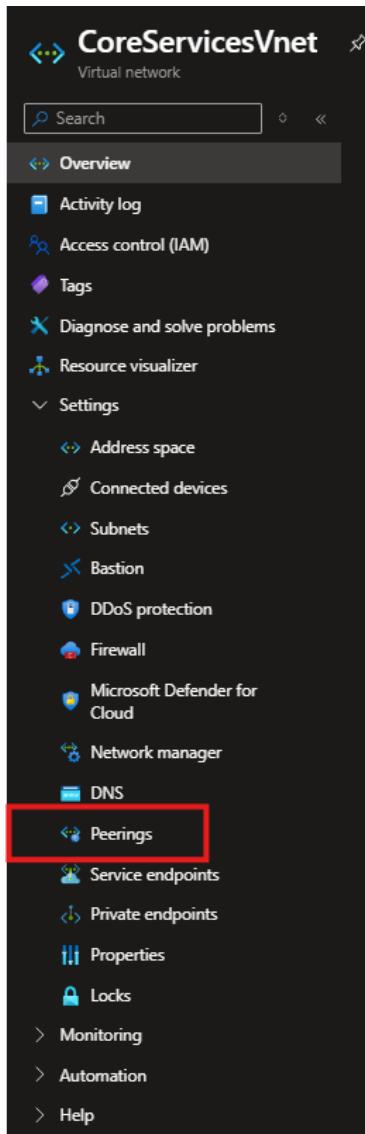
## AZURE LAB #5

Results			
Test(s) ran: Connectivity, NSG diagnostic, Next hop, Port scanner			
Source: CoreServicesVM Destination: ManufacturingVM			
<a href="#">Export to CSV</a>			
Diagnostic tests			
Test	Status	Details	
Connectivity test	<span style="color: red;">✖</span> Unreachable	Probes sent: 316, probes failed: 316	<a href="#">See details</a>
Outbound NSG diagnostic	<span style="color: red;">✖</span> Deny	There are failed tests in the following NSGs: • CoreServicesVM-nsg	<a href="#">See details</a>
Inbound NSG diagnostic	<span style="color: red;">✖</span> Deny	There are failed tests in the following NSGs: • ManufacturingVM-nsg	<a href="#">See details</a>
Next hop (from source)	<span style="color: green;">✓</span> Success	Next hop type: None Route table: System Route	
Destination port accessible	<span style="color: green;">✓</span> Reachable		

Resultados del test.

## AZURE LAB #5

## Configuración de peering de redes virtuales entre redes virtuales



Dentro de la red virtual accedo a peerings.

 tajamar.	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #5	

Home > Network foundation | Virtual networks > CoreServicesVnet | Peerings >

## Add peering

CoreServicesVnet

Virtual network peering enables you to seamlessly connect two or more virtual networks in Azure. This will allow resources in either virtual network to directly connect and communicate with resources in the peered virtual network.

**Remote virtual network summary**

Peering link name *	ManufacturingVnet-to-CoreServicesVnet
I know my resource ID ⓘ	<input type="checkbox"/>
Subscription *	Azure for Students
Virtual network *	ManufacturingVnet (az104-rg5)

**Remote virtual network peering settings**

Allow 'ManufacturingVnet' to access 'CoreServicesVnet' ⓘ	<input checked="" type="checkbox"/>
Allow 'ManufacturingVnet' to receive forwarded traffic from 'CoreServicesVnet' ⓘ	<input checked="" type="checkbox"/>
Allow gateway or route server in 'ManufacturingVnet' to forward traffic to 'CoreServicesVnet' ⓘ	<input type="checkbox"/>
Enable 'ManufacturingVnet' to use 'CoreServicesVnet's remote gateway or route server ⓘ	<input type="checkbox"/>

Estoy creando la conexión desde la red CoreServicesVnet hacia la red ManufacturingVnet.

Aquí estoy definiendo las reglas de flujo de tráfico entre las dos redes:

Allow 'ManufacturingVnet' to access 'CoreServicesVnet' (Permitir que 'ManufacturingVnet' acceda a 'CoreServicesVnet'):

Activado. Esto establece el permiso de acceso de la red remota a mi red local.

Allow 'ManufacturingVnet' to receive forwarded traffic from 'CoreServicesVnet' (Permitir que 'ManufacturingVnet' reciba tráfico reenviado desde 'CoreServicesVnet'):

Activado. Esto es esencial si tengo una tercera red que se conecta a CoreServicesVnet y necesito que ese tráfico pueda llegar a ManufacturingVnet a través de mi red central.



## AZURE LAB #5

**Local virtual network summary**

Peering link name \*

**Local virtual network peering settings**

Allow 'CoreServicesVnet' to access 'ManufacturingVnet'

Allow 'CoreServicesVnet' to receive forwarded traffic from 'ManufacturingVnet'

Allow gateway or route server in 'CoreServicesVnet' to forward traffic to 'ManufacturingVnet'

Enable 'CoreServicesVnet' to use 'ManufacturingVnet's' remote gateway or route server

Lo mismo para esta red pero al contrario.

**Peerings**

Name	Peering sync status	Peering state	Remote VNet	Virtual Network	Cross-tenant
CoreServicesVnet-to-ManufacturingVnet	Fully Synchronized	Connected	ManufacturingVnet	Disabled	No

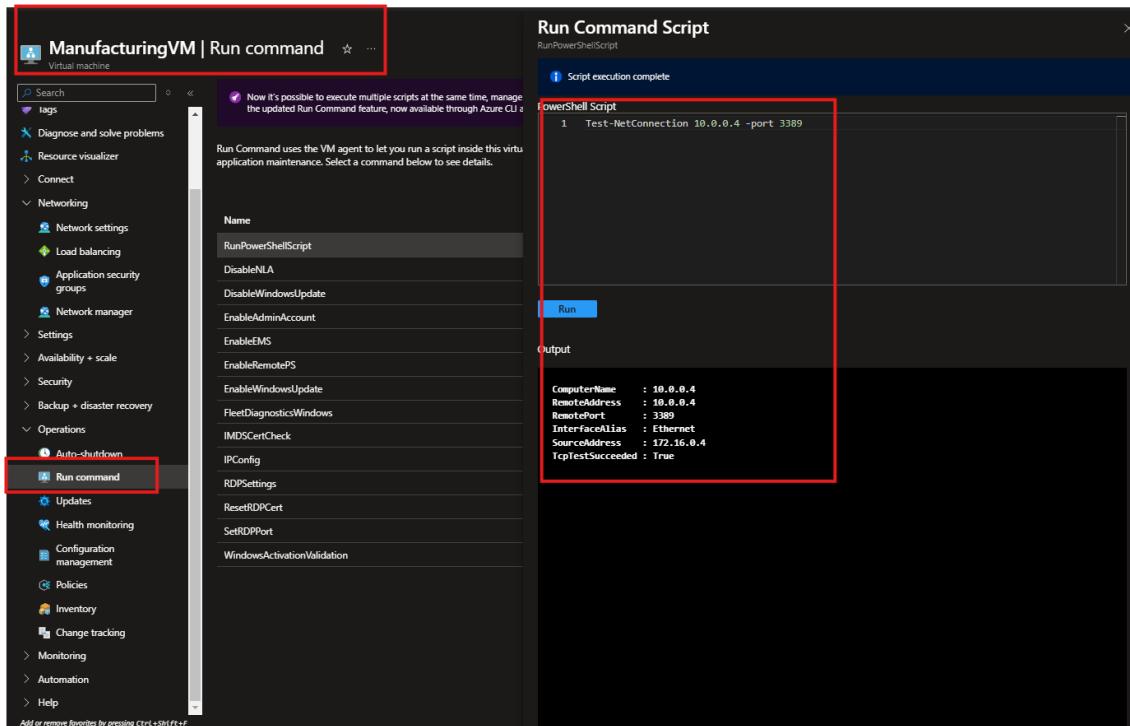
**Peerings**

Name	Peering sync status	Peering state	Remote VNet	Virtual Network	Cross-tenant
ManufacturingVnet-to-CoreServicesVnet	Fully Synchronized	Connected	CoreServicesVnet	Disabled	No

Compruebo que el peering está en funcionamiento en ambos sentidos.

## AZURE LAB #5

## Uso de Azure PowerShell para probar la conexión entre máquinas virtuales



Dentro de la máquina virtual manufacturing accedo a operations para lanzar un comando powershell para probar la conexión entre las maquinas virtuales.

Para ello necesito la ip privada de la máquina, dicha ip se obtiene metiéndome dentro de la configuración de la máquina virtual y mirando.



## AZURE LAB #5

## Creación de un route personalizado.

Name	IPv4	IPv6	Available IPs	Delegated to	Security group	Route table
Core	10.0.0.0/24	-	250	-	-	-
perimeter	10.0.1.0/24	-	251	-	-	-

Creo una subred nueva dentro de la VNET.

**Basics** Tags Review + create

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Resource group \*  Create new

**Instance details**

Region \*

Name \*

Propagate gateway routes \*  Yes  No

Creo una nueva tabla de rutas.

Actúan como un conjunto de reglas que controlan cómo debe dirigirse el tráfico de red (paquetes de datos) saliente desde una subred específica.



Home > Microsoft.RouteTable-20251202181930 | Overview > az104-rg5 > rt-CoreServices

## rt-CoreServices | Routes

Route table

Search Add Refresh Give feedback

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Resource visualizer Settings Configuration Routes

Subnets Properties Locks Monitoring Automation Help

No results.

 tajamar.	Máster en Ingeniería MultiCloud, DevOps y Seguridad.
AZURE LAB #5	

## Add route

rt-CoreServices

A user defined route (UDR) is a static route that overrides Azure's default system routes, or adds a route to a subnet's route table. [Learn more](#)

Route name \*

Destination type \*

Destination IP addresses/CIDR ranges \*

Next hop type \*

Next hop address \*

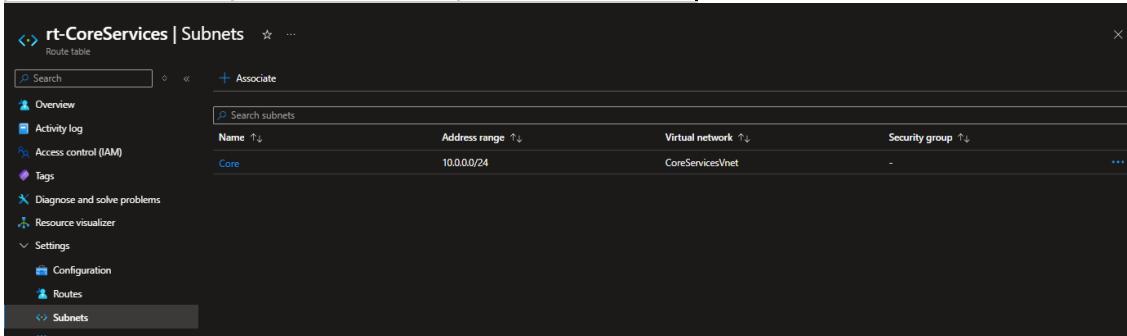
**Info** Ensure you have IP forwarding enabled on your virtual appliance. You can enable this by navigating to the respective network interface's IP address settings.

Configuración	Valor Elegido	Significado
Nombre de la Ruta (Route name)	PerimetertoCore	Es un nombre descriptivo para identificar que esta ruta maneja el tráfico del perímetro hacia la red central (Core).
Rango de Destino (Destination IP addresses/CIDR ranges)	10.0.0.0/16	Esta ruta aplicará a todo el tráfico destinado a la red 10.0.0.0/16 (un rango interno privado común).
Tipo de Próximo Salto (Next hop type)	Virtual appliance	Es la instrucción clave: No envíes el tráfico directamente.



## AZURE LAB #5

		Forzarás que pase por un dispositivo de red específico
Dirección del Próximo Salto (Next hop address)	10.0.1.7	Esta es la dirección IP privada del dispositivo virtual (firewall, router virtual, etc.) al que debe dirigirse el tráfico antes de llegar a su destino final (10.0.0.0/16).



En esencia, la configuración crea la estructura para una red perimetral o DMZ (Zona Desmilitarizada) que centraliza la seguridad:

Se crea la subred perimeter (10.0.1.0/24): Aquí es donde se alojará el dispositivo de seguridad (NVA o Firewall).

Se crea la Tabla de Rutas rt-CoreServices: Este es el contenedor de las reglas de enrutamiento.

Se añade la Ruta Estática (PerimeterToCore): Esta es la regla crucial que le dice a Azure que, si el tráfico va a cualquier lugar dentro del rango 10.0.0.0/16, su próximo salto debe ser la IP del Firewall (10.0.1.7) en lugar de ir directamente.

Se asocia la Tabla de Rutas a la subred Core: Esto aplica la regla de la ruta estática a todas las máquinas virtuales dentro de la subred Core.

El resultado final es que el tráfico de la subred Core hacia el rango de destino especificado ahora pasa por el Dispositivo Virtual (Virtual appliance) en la IP 10.0.1.7 para inspección.