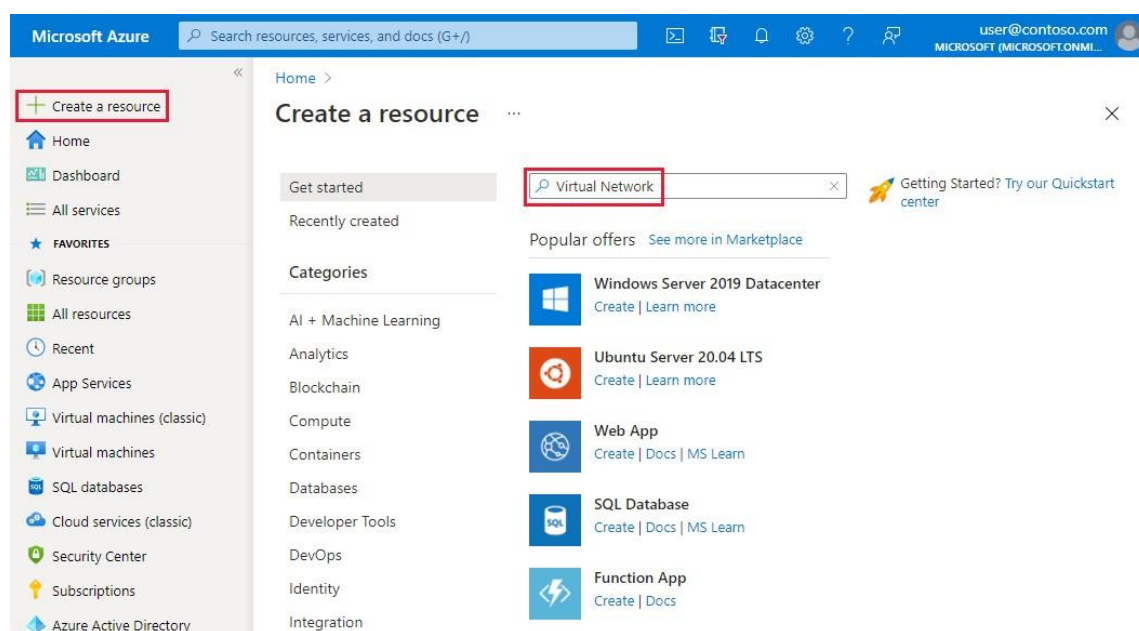


Los puntos de conexión de servicio de red virtual le permiten limitar el acceso a la red a algunos recursos de servicio de Azure a una subred de red virtual. También puede eliminar el acceso a Internet a los recursos. Los puntos finales de servicio proporcionan una conexión directa desde su red virtual a los servicios de Azure admitidos, lo que le permite usar el espacio de direcciones privadas de su red virtual para acceder a los servicios de Azure. El tráfico destinado a los recursos de Azure a través de puntos finales de servicio siempre permanece en la red troncal de Microsoft Azure.

- Crear una red virtual con una subred
- Agregue una subred y habilite un punto final de servicio
- Cree un recurso de Azure y permita el acceso a la red solo desde una subred
- Implemente una máquina virtual (VM) en cada subred
- Confirmar el acceso a un recurso desde una subred
- Confirme que se deniega el acceso a un recurso desde una subred e Internet

## Crear una red virtual

1. En el menú de Azure Portal, seleccione **+ Crear un recurso**.
2. Busque *Red virtual* y luego seleccione **Crear**.



3. En la **pestaña Básico**, ingrese la siguiente información y luego seleccione **Siguiente: Direcciones IP >**.

|                      |                           |
|----------------------|---------------------------|
| <b>Configuración</b> | <b>Valor</b>              |
| Suscripción          | Selecione su suscripción. |
| <b>Configuración</b> | <b>Valor</b>              |

grupo de recursos Seleccione **Crear nuevo** e ingrese *myResourceGroup* .

Nombre Ingrese a *miRedVirtual* .

Región Seleccione **Este de EE. UU.**

[Home](#) > [Virtual networks](#) >

## Create virtual network ...

**Basics** IP Addresses Security Tags Review + create

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation. [Learn more about virtual network](#)

### Project details

Subscription \* ⓘ

Azure Subscription

Resource group \* ⓘ

(New) MyResourceGroup

[Create new](#)

### Instance details

Name \*

myVirtualNetwork ✓

Region \*

East US

[Review + create](#)

[< Previous](#)

[Next : IP Addresses >](#)

[Download a template for automation](#)

- En la **pestaña Direcciones IP** , seleccione la siguiente configuración de dirección IP y luego seleccione **Revisar + crear** .

### Configuración

### Valor

espacio de direcciones IPv4

Dejar por defecto.

Nombre de subred

Seleccione **predeterminado** y cambie el nombre de la subred a "Pública".

Rango de direcciones de subred

Dejar por defecto.

## Create virtual network ...



Basics IP Addresses Security Tags Review + create

The virtual network's address space, specified as one or more address prefixes in CIDR notation (e.g. 192.168.1.0/24).

IPv4 address space

10.0.0.0/16 10.0.0.0 - 10.0.255.255 (65536 addresses)



☐ Add IPv6 address space ⓘ

The subnet's address range in CIDR notation (e.g. 192.168.1.0/24). It must be contained by the address space of the virtual network.

+ Add subnet Remove subnet

| <input type="checkbox"/> Subnet name | Subnet address range | NAT gateway |
|--------------------------------------|----------------------|-------------|
| <input type="checkbox"/> Public      | 10.0.0.0/24          | -           |

Use of a NAT gateway is recommended for outbound internet access from a subnet. You can deploy a NAT gateway and assign it to a subnet after you create the virtual network. [Learn more](#)

**Review + create**

< Previous

Next : Security >

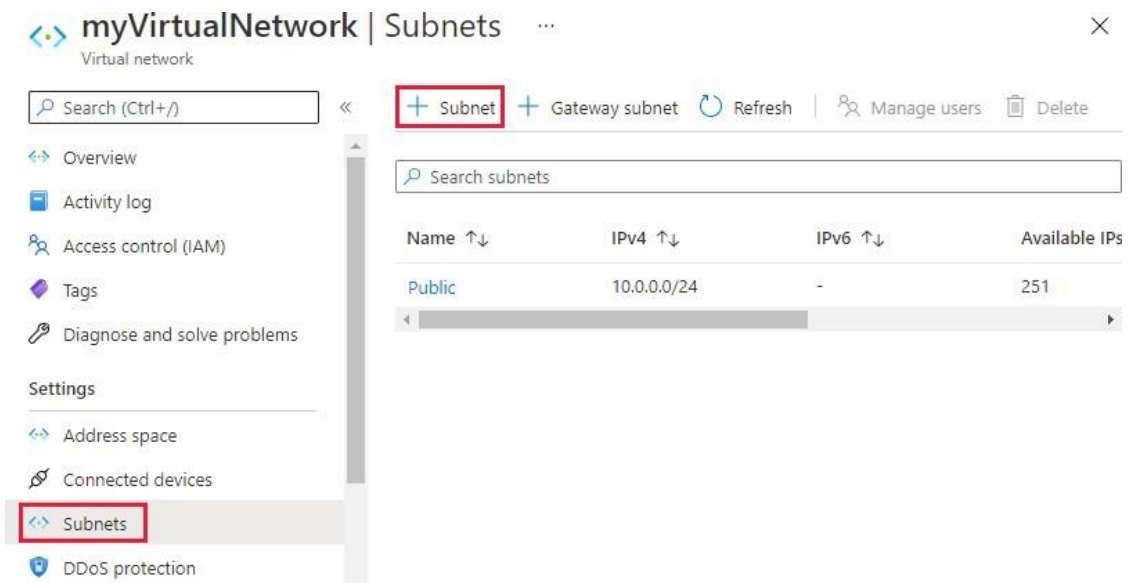
[Download a template for automation](#)

5. Si pasan las comprobaciones de validación, seleccione **Crear**.
6. Espere a que finalice la implementación, luego seleccione **Ir al recurso** o pase a la siguiente sección.

## Habilitar un punto final de servicio

Los puntos finales de servicio están habilitados por servicio, por subred. Para crear una subred y habilitar un extremo de servicio para la subred:

1. Si aún no está en la página de recursos de la red virtual, puede buscar la red virtual recién creada en el cuadro en la parte superior del portal. Ingrese *myVirtualNetwork* y selecciónelo de la lista.
2. Seleccione **Subredes** en **Configuración** y luego seleccione **+ Subred**, como se muestra:



3. En la **página Agregar subred** , ingrese o seleccione la siguiente información y luego seleccione **Guardar** :

#### Configuración

Nombre

#### Valor

Privado

Intervalo de direcciones de subred

Dejar por defecto

Puntos finales de servicio

Seleccione

**Microsoft.Almacenamiento**

Políticas de punto final de servicio

Dejar por defecto. *0 seleccionado* .

## Add subnet



Name \*

Private



Subnet address range \* ⓘ

10.0.1.0/24

10.0.1.0 - 10.0.1.255 (251 + 5 Azure reserved addresses)

☐

Add IPv6 address space ⓘ

NAT gateway ⓘ

None



Network security group

None



Route table

None



### SERVICE ENDPOINTS

Create service endpoint policies to allow traffic to specific azure resources from your virtual network over service endpoints. [Learn more](#)

Services ⓘ

Microsoft.Storage



Service endpoint policies

0 selected



### SUBNET DELEGATION

Delegate subnet to a service ⓘ

None



### NETWORK POLICY FOR PRIVATE ENDPOINTS

The network policy affects all private endpoints in this subnet. To use network security groups, application security groups, or user defined routes to control traffic going to a private endpoint, set the private endpoint network policy to enabled. [Learn more](#)

Private endpoint network policy

Disabled



Save

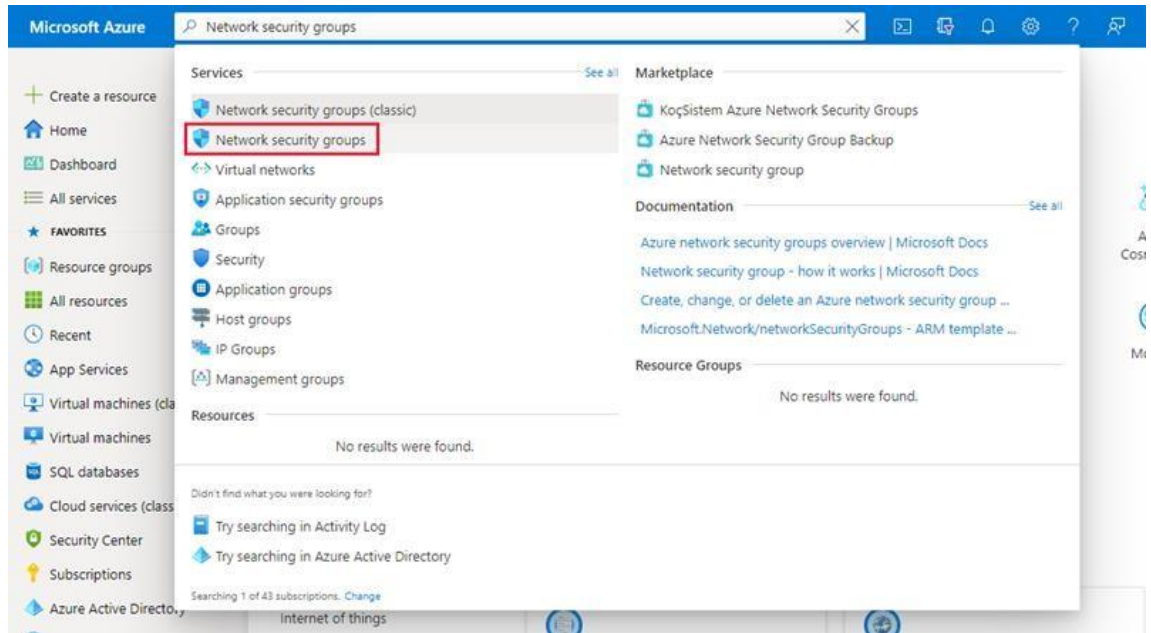
Cancel

4.

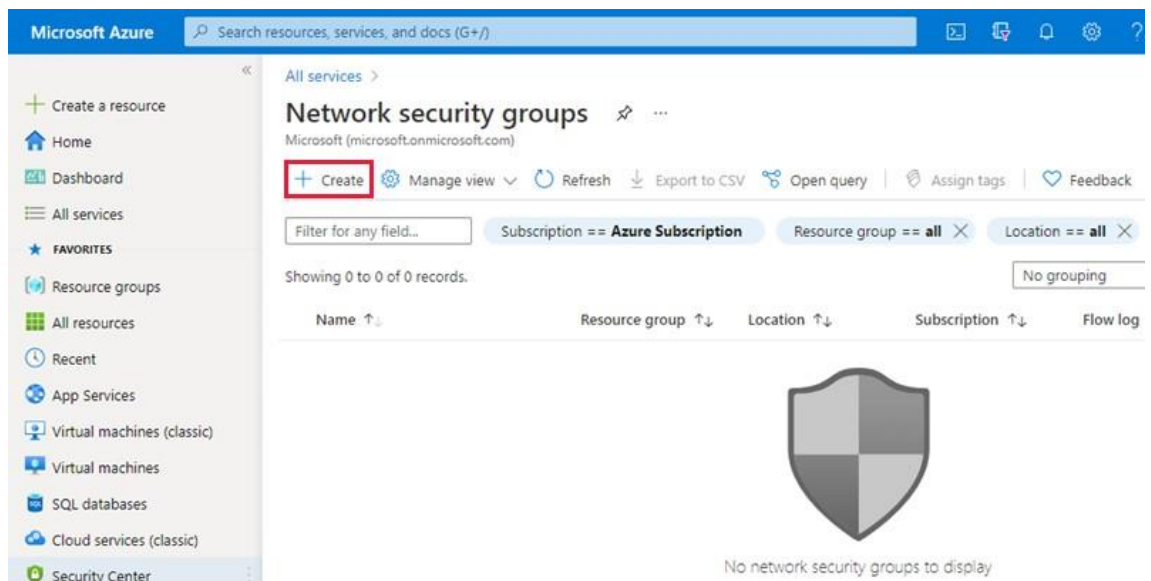
# Restringir el acceso a la red para una subred

De manera predeterminada, todas las instancias de máquinas virtuales en una subred pueden comunicarse con cualquier recurso. Puede limitar la comunicación hacia y desde todos los recursos en una subred creando un grupo de seguridad de red y asociándolo a la subred:

1. En el cuadro de búsqueda en la parte superior de Azure Portal, busque **grupos de seguridad de red**.



2. En la *página Grupos de seguridad de red*, seleccione **+ Crear**.



3. Ingrese o seleccione la siguiente información:

| Configuración     | Valor  |
|-------------------|--|
| Suscripción       | Selecione su suscripción                     |
| grupo de recursos | Selecione <i>myResourceGroup</i> de la lista |
| Nombre            | Ingresa <b>myNsgPrivate</b>                  |
| Ubicación         | Selecione <b>Este de EE. UU.</b>             |

4. Seleccione **Revisar + crear** y, cuando pase la verificación de validación, seleccione **Crear**.

## Create network security group ...

Basics Tags Review + create

### Project details

Subscription \* Azure Subscription ▼

Resource group \* myResourceGroup ▼  
[Create new](#)

### Instance details

Name \* myNsgPrivate ✓

Region \* (US) East US ▼

**Review + create**

< Previous

Next : Tags >

[Download a template for automation](#)

5. Después de crear el grupo de seguridad de red, seleccione **Ir al recurso** o busque *myNsgPrivate* en la parte superior de Azure Portal.
6. Seleccione **Reglas de seguridad de salida** en *Configuración* y luego seleccione **+ Agregar**.

Home > myNsgPrivate

myNsgPrivate | Outbound security rules ☆ ...

Network security group

Search (Ctrl+/) + Add Hide default rules Refresh Delete Give feedback

Network security group security rules are evaluated by priority using the combination of source, source port, destination, destination port, and protocol to allow or deny the traffic. A security rule can't have the same priority and direction as an existing rule. You can't delete default security rules, but you can override them with rules that have a higher priority. [Learn more](#)

Filter by name

| Priority | Name                  | Port | Protocol | Source         | Destination    | Action |
|----------|-----------------------|------|----------|----------------|----------------|--------|
| 65000    | AllowNetOutBound      | Any  | Any      | VirtualNetwork | VirtualNetwork | Allow  |
| 65001    | AllowInternetOutBound | Any  | Any      | Any            | Internet       | Allow  |
| 65500    | DenyAllOutBound       | Any  | Any      | Any            | Any            | Deny   |

Overview  
Activity log  
Access control (IAM)  
Tags  
Diagnose and solve problems  
Settings  
Inbound security rules  
**Outbound security rules**  
Network interfaces

7. Cree una regla que permita la comunicación saliente con el servicio Azure Storage. Ingresa o seleccione la siguiente información y luego seleccione **Agregar**:

| <b>Configuración</b>                 | <b>Valor</b>  |
|--------------------------------------|---|
| Fuente                               | Seleccionar <b>etiqueta de servicio</b>   |
| Etiqueta de servicio de origen       | Seleccionar <b>red virtual</b>  |
| Intervalos de *<br>puertos de origen |   |
| Destino                              | Seleccionar <b>etiqueta de servicio</b>   |
| Etiqueta de servicio de destino      | Seleccionar <b>almacenamiento</b>   |
| Servicio                             | Deje el valor predeterminado como <i>Personalizado</i> .  |
| Intervalos de<br>puertos de destino  | Cambiar a <b>445</b> . El protocolo SMB se usa para conectarse a un recurso compartido de archivos creado en un paso posterior. |
| Protocolo                            | Cualquier   |
| Acción                               | Permitir  |
| Prioridad                            | 100   |
| Nombre                               | Renombrar a <b>Permitir-Almacenamiento-Todo</b>   |





## Add outbound security rule



myNsgPrivate

Source ⓘ

Service Tag



Source service tag \* ⓘ

VirtualNetwork



Source port ranges \* ⓘ

\*

Destination ⓘ

Service Tag



Destination service tag ⓘ

Storage



Service ⓘ

Custom



Destination port ranges \* ⓘ

445



Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMP

Action

☒ Allow

☐ Deny

Priority \* ⓘ

100

Name \*

Allow-Storage-All



Description

Add

Cancel

8.

9. Cree otra regla de seguridad de salida que niegue la comunicación a Internet. Esta regla anula una regla predeterminada en todos los grupos de seguridad de la red que permite la comunicación por Internet saliente. Complete los pasos 6-9 de arriba usando los siguientes valores y luego seleccione **Agregar** :

| Configuración                    | Valor  |
|----------------------------------|--|
| Fuente                           | Seleccionar <b>etiqueta de servicio</b>                  |
| Etiqueta de servicio de origen   | Seleccionar <b>red virtual</b>                           |
| Intervalos de puertos de origen  |  |
| Destino                          | Seleccionar <b>etiqueta de servicio</b>                  |
| Etiqueta de servicio de destino  | Seleccione <b>Internet</b>                               |
| Servicio                         | Deje el valor predeterminado como <i>Personalizado</i> . |
| Intervalos de puertos de destino |  |
| Protocolo                        | Cualquier  |
| Acción                           | Cambie el valor predeterminado a <b>Denegar</b> .        |
| Prioridad                        | 110  |
| Nombre                           | Cambiar a <b>Denegar-Internet-Todo</b>                   |



## Add outbound security rule

myNsgPrivate



Source ⓘ

Service Tag



Source service tag \* ⓘ

VirtualNetwork



Source port ranges \* ⓘ

\*

Destination ⓘ

Service Tag



Destination service tag ⓘ

Internet



Service ⓘ

Custom



Destination port ranges \* ⓘ

\*



Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMP

Action

☐ Allow

☒ Deny

Priority \* ⓘ

110

Name \*

Deny-Internet-All



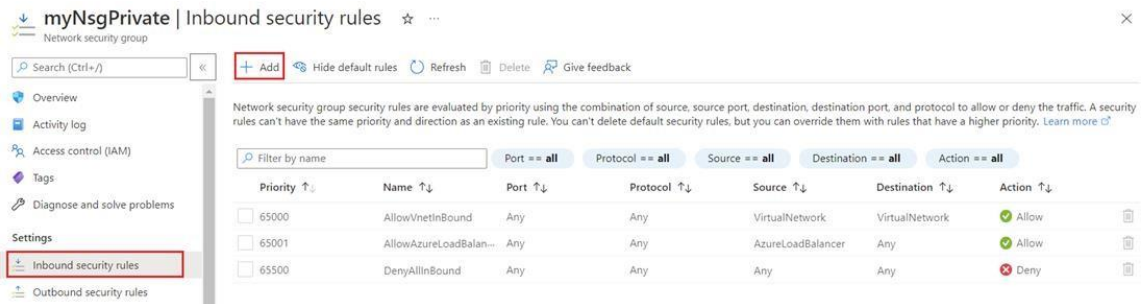
Description

Add

Cancel

10.

11. Cree una *regla de seguridad entrante* que permita el tráfico del Protocolo de escritorio remoto (RDP) a la subred desde cualquier lugar. La regla anula una regla de seguridad predeterminada que niega todo el tráfico entrante de Internet. Se permiten conexiones de escritorio remoto a la subred para que la conectividad se pueda probar en un paso posterior. Seleccione **Reglas de seguridad de entrada** en *Configuración* y luego seleccione **+ Agregar** .



12. Ingrese o seleccione los siguientes valores y luego seleccione **Agregar** .

| Configuración                    | Valor  |
|----------------------------------|--|
| Fuente                           | Cualquier  |
| Intervalos de puertos de origen  | *  |
| Destino                          | Seleccionar <b>etiqueta de servicio</b>                  |
| Etiqueta de servicio de destino  | Seleccionar <b>red virtual</b>                           |
| Servicio                         | Deje el valor predeterminado como <i>Personalizado</i> . |
| Intervalos de puertos de destino | Cambiar a 3389   |
| Protocolo                        | Cualquier  |
| Acción                           | Permitir   |
| Prioridad                        | 120  |
| Nombre                           | Cambiar a <i>Permitir-RDP-Todo</i>                       |



## Add inbound security rule

myNsgPrivate



Source ⓘ

Any



Source port ranges \* ⓘ

\*

Destination ⓘ

Service Tag



Destination service tag ⓘ

VirtualNetwork



Service ⓘ

Custom



Destination port ranges \* ⓘ

3389



Protocol

☒ Any

☐ TCP

☐ UDP

☐ ICMP

Action

☒ Allow

☐ Deny

Priority \* ⓘ

110



Name \*

Allow-RDP-All

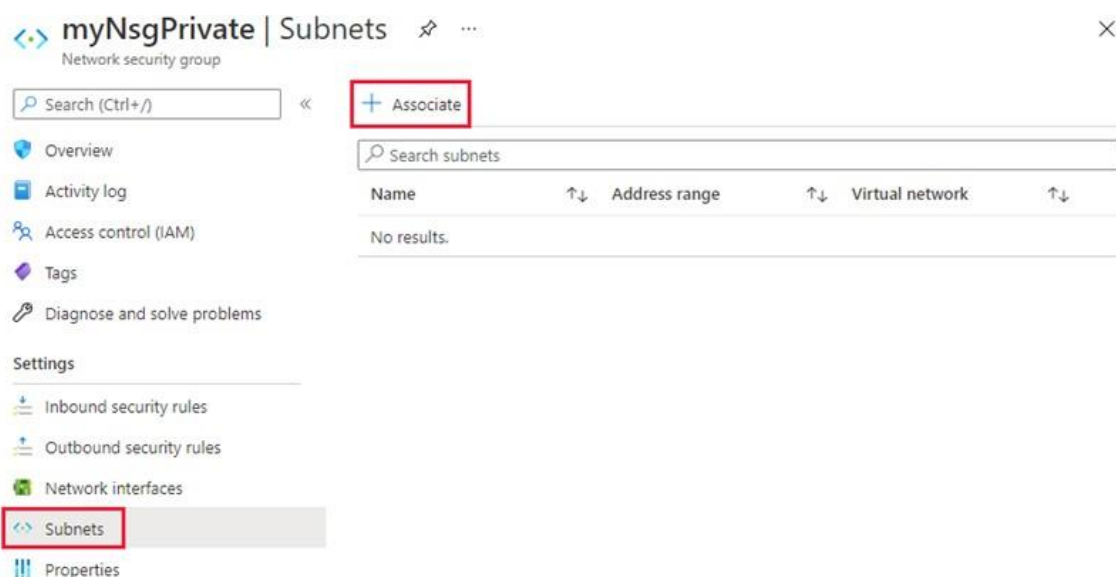


Description

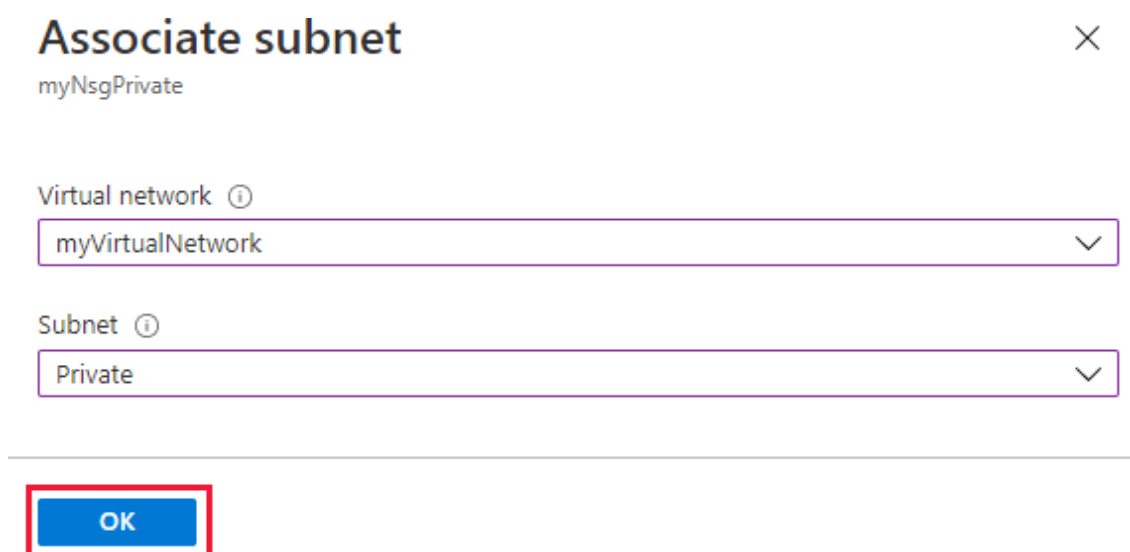
Add

Cancel

13. Seleccione **Subredes** en *Configuración* y luego seleccione **+ Asociar** .



14. Seleccione **myVirtualNetwork** en *Red virtual* y luego seleccione **Privado** en *Subredes* . Seleccione **Aceptar** para asociar el grupo de seguridad de red a la subred seleccionada.



## Restringir el acceso a la red a un recurso

Los pasos necesarios para restringir el acceso a la red a los recursos creados a través de los servicios de Azure, que están habilitados para los puntos de conexión del servicio, variarán según los servicios. Consulte la documentación de los servicios individuales para conocer los pasos específicos de cada servicio. El resto de este tutorial incluye pasos para restringir el acceso a la red para una cuenta de Azure Storage, como ejemplo.

## Crear una cuenta de almacenamiento

1. Seleccione **+ Crear un recurso** en la esquina superior izquierda de Azure Portal.
2. Ingrese "Cuenta de almacenamiento" en la barra de búsqueda y selecciónela en el menú desplegable. Luego seleccione **Crear**.
3. Ingrese la siguiente información:

| Configuración                         | Valor  |
|---------------------------------------|--|
| Suscripción                           | Seleccione su suscripción  |
| grupo de recursos                     | Seleccione <i>mi grupo de recursos</i>   |
| Nombre de la cuenta de almacenamiento | Introduzca un nombre que sea único en todas las ubicaciones de Azure. El nombre debe tener entre 3 y 24 caracteres de longitud, utilizando solo números y letras minúsculas. |
| Región                                |  |
| Actuación                             | Estándar   |
| Redundancia                           | Almacenamiento con redundancia local (LRS)   |

## Create a storage account ...

[Basics](#)   [Advanced](#)   [Networking](#)   [Data protection](#)   [Tags](#)   [Review + create](#)

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. [Learn more about Azure storage accounts](#)

### Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

|                  |  |
|------------------|--|
| Subscription *   | <div>Azure Subscription</div>                                    |
| Resource group * | <div>myResourceGroup</div> <div><a href="#">Create new</a></div> |

### Instance details

If you need to create a legacy storage account type, please click [here](#).

|                          |   |
|--------------------------|---|
| Storage account name ⓘ * | <div>mystorage007</div>   |
| Region ⓘ *               | <div>(US) East US</div>   |
| Performance ⓘ *          | <div><input checked="" type="radio"/> <b>Standard:</b> Recommended for most scenarios (general-purpose v2 account)</div> <div><input type="radio"/> <b>Premium:</b> Recommended for scenarios that require low latency.</div> |
| Redundancy ⓘ *           | <div>Locally-redundant storage (LRS)</div>  |

[Review + create](#)

[< Previous](#)


[Next : Advanced >](#)

- 
- 
- 
- 
5. Seleccione **Crear + revisión** y, cuando hayan superado las comprobaciones de validación, seleccione **Crear** .
6. Después de crear la cuenta de almacenamiento, seleccione **Ir al recurso**

## Crear un recurso compartido de archivos en la cuenta de almacenamiento

1. Seleccione **Recursos compartidos de archivos** en *Almacenamiento de datos* y, a continuación, seleccione **+ Compartir archivos** .



mystorage007 | File shares  ...

Storage account

Search (Ctrl+/,) << **+ File share** Refresh

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage Explorer (preview)

Data storage

Containers

**File shares**

Queues

**File share settings**

Active Directory: **Not configured** Soft delete: **7 days** Share capacity: **5 TiB**

Search file shares by prefix (case-sensitive)

☐ Show deleted shares

| Name   | Modified | Tier | Quota |
|--|----------|------|-------|
| You don't have any file shares yet. Click '+ File share' to get started. |          |      |       |

2. Ingrese o configure los siguientes valores para el recurso compartido de archivos y luego seleccione **Crear** :

### Configuración Valor

Nombre mi-archivo-compartido

Cuota Seleccione **Establecer al máximo** .

Nivel Déjelo por defecto, *Optimizado para transacciones* .

## New file share



Name \*

my-file-share



Quota ⓘ

5120



[Set to maximum](#)

GiB

Tiers ⓘ



Premium

Transaction optimized

Hot

Cool

Create

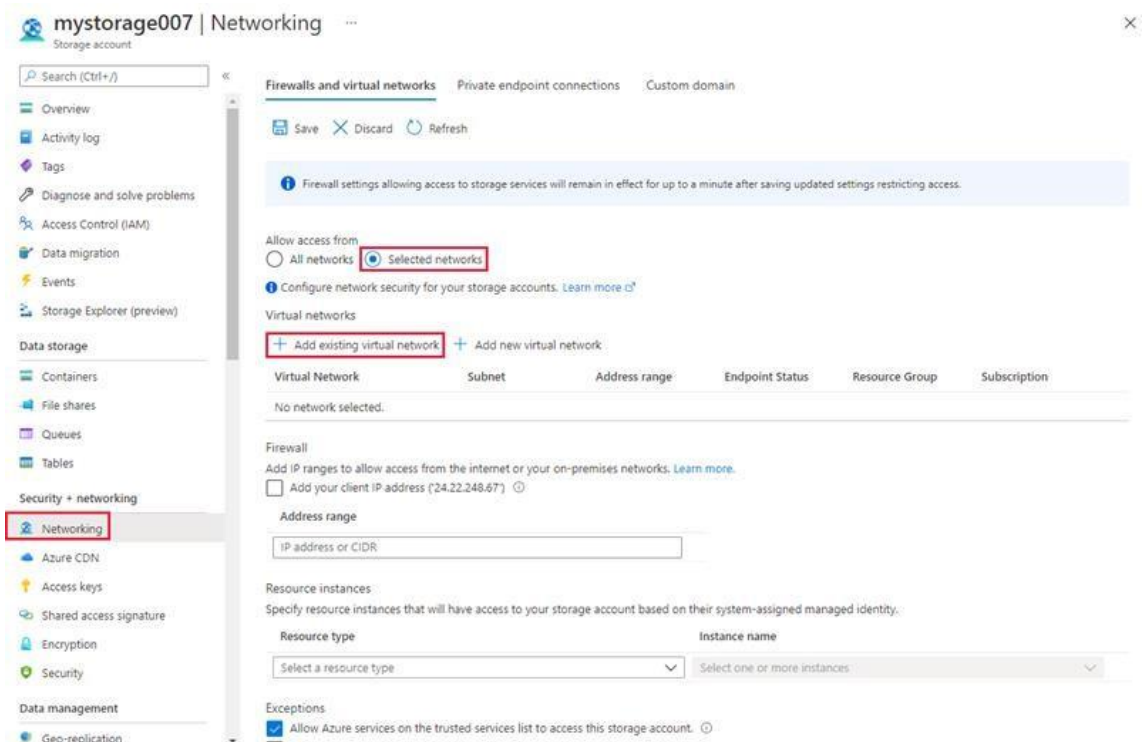
Discard

3. El nuevo archivo compartido debería aparecer en la página de archivos compartidos, si no, seleccione el **botón Actualizar** en la parte superior de la página.

## Restringir el acceso a la red a una subred

De forma predeterminada, las cuentas de almacenamiento aceptan conexiones de red de clientes en cualquier red, incluida Internet. Puede restringir el acceso a la red desde Internet y todas las demás subredes en todas las redes virtuales (excepto la *subred privada* en la *red virtual myVirtualNetwork* ). Para restringir el acceso a la red a una subred:

1. Seleccione **Redes** en *Configuración* para su cuenta de almacenamiento (con un nombre único).
2. Seleccione *Permitir acceso desde* **redes seleccionadas** y luego seleccione **+ Agregar red virtual existente** .



3. En **Agregar redes** , seleccione los siguientes valores y luego seleccione **Agregar** :

### Configuración Valor

Suscripción Seleccione su suscripción

Redes virtuales **miRedVirtual**

Subredes **Privado**

## Add networks

Subscription \*

Azure Subscription

Virtual networks \* ⓘ

myVirtualNetwork

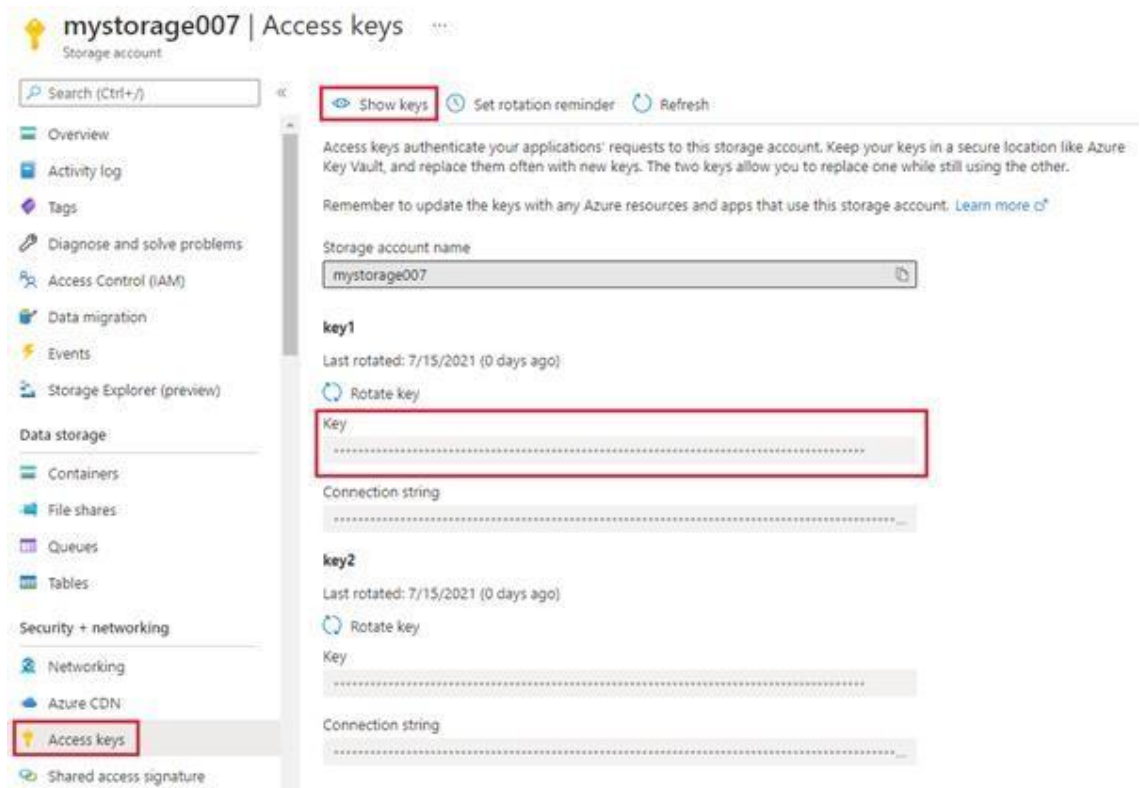
Subnets \*

Private

Add

- 4.
5. Seleccione el **botón Guardar** para guardar las configuraciones de red virtual.

6. Seleccione **Claves de acceso** en *Seguridad y redes* para la cuenta de almacenamiento y seleccione **Mostrar claves** . Tenga en cuenta el valor de key1 para usarlo en un paso posterior al asignar el recurso compartido de archivos en una máquina virtual.



## Crear máquinas virtuales

Para probar el acceso de red a una cuenta de almacenamiento, implemente una máquina virtual en cada subred.

### Crear la primera máquina virtual

1. En Azure Portal, seleccione **+ Crear un recurso** .
2. Seleccione **Calcular** y luego **Crear** en *Máquina virtual* .
3. En la *pestaña Conceptos básicos* , ingrese o seleccione la siguiente información:

| Configuración                | Valor  |
|------------------------------|--|
| Suscripción                  | Seleccione su suscripción                                      |
| grupo de recursos            | Seleccione <b>myResourceGroup</b> , que se creó anteriormente. |
| Nombre de la máquina virtual | Ingrese <i>myVmPublic</i>                                      |
| Región                       |  |
| Opciones de disponibilidad   | de zona de disponibilidad                                      |

## Configuración Valor

zona de disponibilidad 1

Imagen Seleccione una imagen del sistema operativo. Para esta VM, *Windows Server 2019 Datacenter - Gen1* . se selecciona

Tamaño Seleccione el tamaño de instancia de VM que desea usar

Nombre de usuario Introduzca un nombre de usuario de su elección.

Contraseña Introduzca una contraseña de su elección. La contraseña debe tener al menos 12 caracteres y cumplir con los [requisitos de complejidad definidos](#) .

Puertos públicos de entrada Permitir puertos seleccionados

Seleccionar puertos de entrada Deje el valor predeterminado en *RDP (3389)*

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

**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 \*

Availability options

Availability zone \*

Image \*  [See all images](#)

Azure Spot instance ☐

Size \*  [See all sizes](#)

**Administrator account**

Username \*

Password \*

Confirm password \*

**Inbound port rules**

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports \* ☐ None ☒ Allow selected ports

Select inbound ports \*

**Licensing**

Save up to 40% with a license you already own using Azure Hybrid benefit. [Learn more](#)

Would you like to use an existing Windows Server license? \* ☐

[Review Azure hybrid benefit compliance](#)

[Review + create](#) [Previous](#) [Next: Disks >](#)

4. En la **pestaña Redes** , ingrese o seleccione la siguiente información:

| Configuración                 | Valor   |
|-------------------------------|---|
| red virtual                   | Seleccione <b>miRedVirtual</b> .  |
| subred                        | Seleccione <b>Público</b> .   |
| Grupo de seguridad de red NIC | Seleccione <b>Avanzado</b> . El portal crea automáticamente un grupo de seguridad de red para usted que permite el puerto 3389. Necesitará este puerto abierto para conectarse a la máquina virtual en un paso posterior. |

Create a virtual machine

Basic Disks Networking Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network \*  [Create new](#)

Subnet \*  [Manage subnet configuration](#)

Public IP \*  [Create new](#)

NIC network security group ☐ None ☐ Basic ☒ Advanced

Configure network security group \*  [Create new](#)

Accelerated networking ☐ The selected VM size does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? ☐

[Review + create](#) [< Previous](#) [Next: Management >](#)

5. Seleccione **Revisar y crear** , luego **Crear** y espere a que finalice la implementación.
7. Seleccione **Ir al recurso** o abra la **página Inicio > Máquinas virtuales** y seleccione la VM que acaba de crear *myVmPublic* , que debe iniciarse.

## Crear la segunda máquina virtual

1. Repita los pasos 1 a 5 para crear una segunda máquina virtual. En el paso 3, nombre la máquina virtual *myVmPrivate* . En el paso 4, seleccione la **subred privada** y configure *el grupo de seguridad de la red NIC* en **Ninguno** .

**Create a virtual machine**

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

**Network interface**  
When creating a virtual machine, a network interface will be created for you.

Virtual network  [Create new](#)

Subnet  [Manage subnet configuration](#)

Public IP  [Create new](#)

NIC network security group ☒ None ☐ Basic ☐ Advanced

**Accelerated networking** ☐ The selected VM size does not support accelerated networking.

**Load balancing**  
You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Place this virtual machine behind an existing load balancing solution? ☐

[Review + create](#) [Previous](#) [Next: Management](#)

2. Seleccione **Revisar y crear** , luego **Crear** y espere a que finalice la implementación.

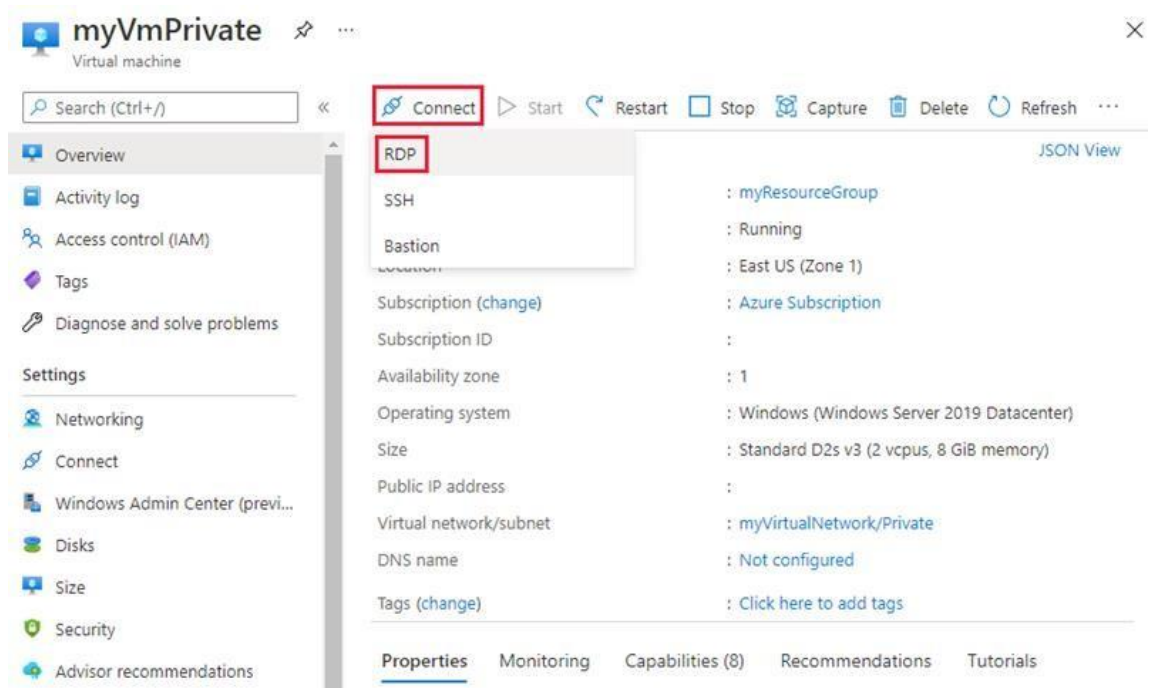
Advertencia

No continúe con el siguiente paso hasta que se complete la implementación.

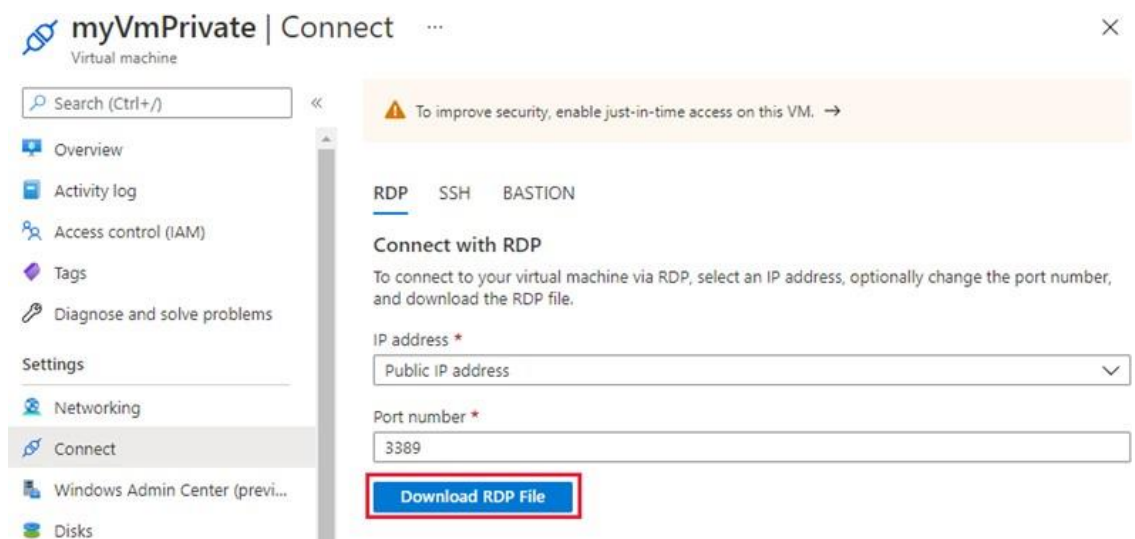
3. Seleccione **Ir al recurso** o abra la **página Inicio > Máquinas virtuales** y seleccione la VM que acaba de crear *myVmPrivate* , que debe iniciarse.

## Confirmar el acceso a la cuenta de almacenamiento

1. la *máquina virtual myVmPrivate* Una vez que se haya creado , vaya a la página de descripción general de la máquina virtual. Conéctese a la máquina virtual seleccionando el **botón Conectar** y luego seleccione **RDP** en el menú desplegable.

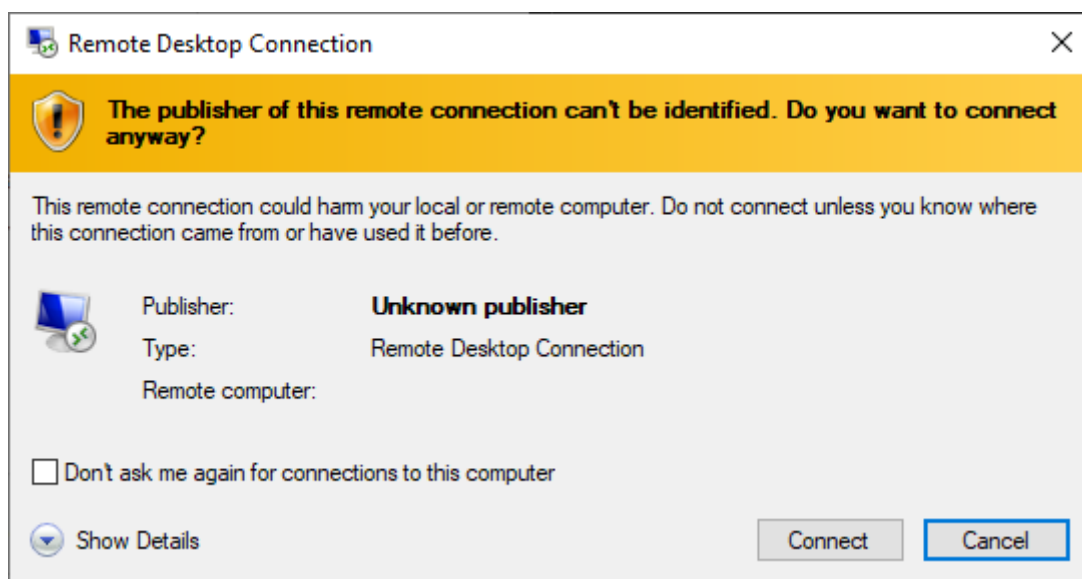


2. Seleccione **Descargar archivo RDP** para descargar el archivo de escritorio remoto a su equipo.

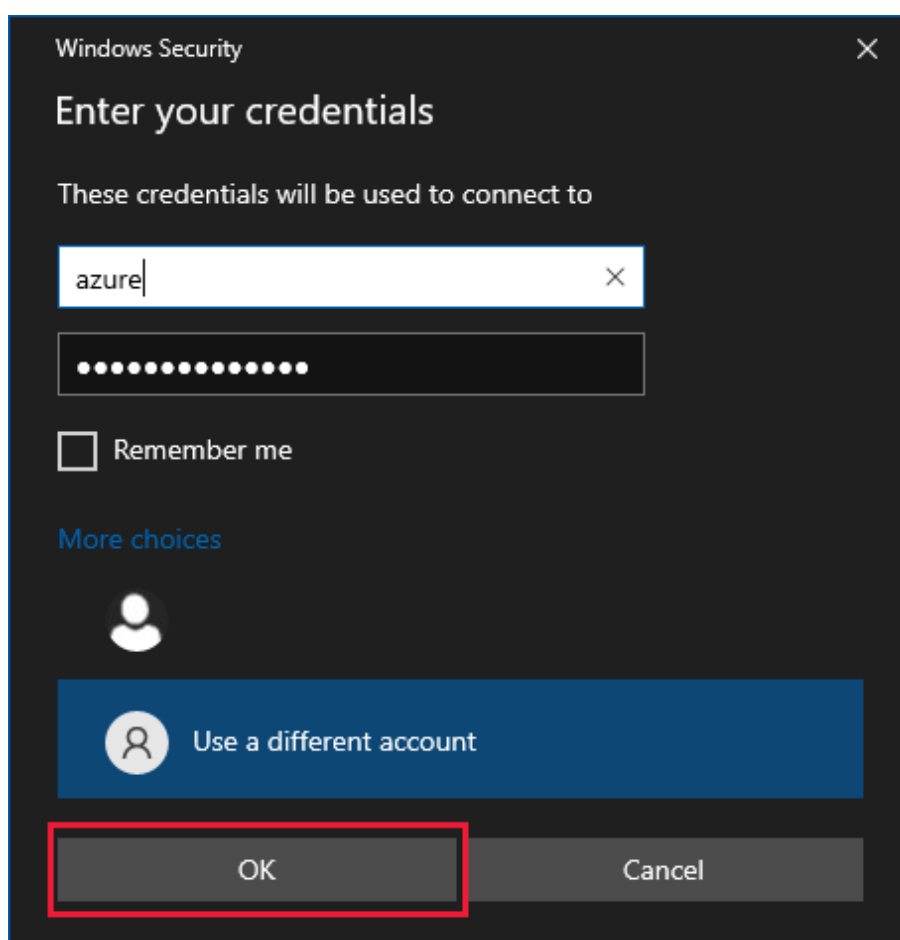


3. Abra el archivo rdp descargado. Cuando se le solicite, seleccione **Conectar**.





4. Ingrese el nombre de usuario y la contraseña que especificó al crear la máquina virtual. Es posible que deba seleccionar **Más opciones** y luego **Usar una cuenta diferente** para especificar las credenciales que ingresó cuando creó la máquina virtual. Para el campo de correo electrónico, ingrese las credenciales de "Cuenta de administrador: nombre de usuario" que especificó anteriormente. Seleccione **Aceptar** para iniciar sesión en la máquina virtual.



- Una vez que haya iniciado sesión, abra Windows PowerShell. Con el siguiente script, asigne el recurso compartido de archivos de Azure a la unidad Z mediante PowerShell. Reemplazar <storage-account-key>y ambos <storage-account-name>variable con los valores que proporcionó y anotó anteriormente en los [pasos Crear una cuenta de almacenamiento](#).

```
$acctKey = ConvertTo-SecureString -String "<storage-account-key>" -AsPlainText -Force
```

```
$credential = New-Object System.Management.Automation.PSCredential -ArgumentList "Azure\<storage-account-name>", $acctKey
```

```
New-PSDrive -Name Z -PSProvider FileSystem -Root "\\<storage-account-name>.file.core.windows.net\my-file-share" -Credential $credential
```

PowerShell devuelve una salida similar a la siguiente salida de ejemplo:

| Name | Used (GB) | Free (GB) | Provider   | Root   |
|------|-----------|-----------|------------|--|
| Z    |           |           | FileSystem | \\mystorage007.file.core.windows.net\my-f... |

- El recurso compartido de archivos de Azure se asignó correctamente a la unidad Z.
- Cierre la sesión de escritorio remoto en la *máquina virtual myVmPrivate*.

## Confirmar acceso denegado a la cuenta de almacenamiento

### Desde myVmPublic:

- Ingresa *myVmPublic* en el **cuadro Buscar recursos, servicios y documentos** en la parte superior del portal. Cuando **myVmPublic** aparezca en los resultados de búsqueda, selecciónelo.
- Repita los pasos 1 a 5 anteriores en [Confirmar el acceso a la cuenta de almacenamiento](#) para la *máquina virtual myVmPublic*.

Después de una breve espera, recibe un New-PSDrive : Access is deniederror. Se deniega el acceso porque la *máquina virtual myVmPublic* se implementa en la *subred pública*. La *subred pública* no tiene un punto de conexión de servicio habilitado para Azure Storage. La cuenta de almacenamiento solo permite el acceso a la red desde la *subred privada*, no desde la *subred pública*.

```
New-PSDrive : Access is denied
```

```
At line:1 char:1
```

```
+ New-PSDrive -Name Z -PSProvider FileSystem -Root "\\mystorage007.file ...
```

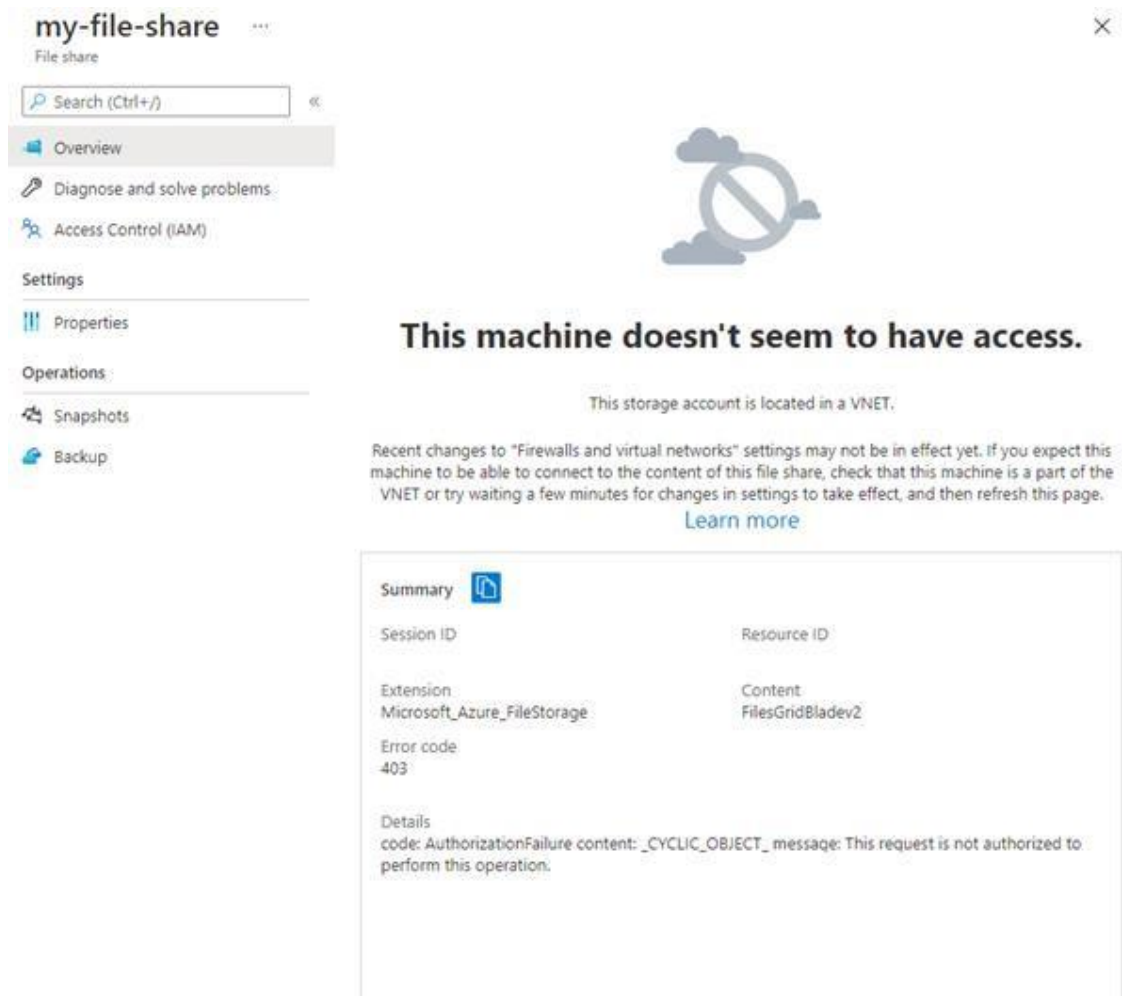
```
+
```

```
~~~~~
+ CategoryInfo          : InvalidOperation: (Z:PSDriveInfo) [New-PSDrive], Win32Exception
+                        Fu                      llyQualifiedErrorId          :
CouldNotMapNetworkDrive,Microsoft.PowerShell.Commands.NewPSDriveCommand
```

2. Cierre la sesión de escritorio remoto en la *máquina virtual myVmPublic* .

## Desde una máquina local:

1. En Azure Portal, vaya a la cuenta de almacenamiento con nombre exclusivo que creó anteriormente. Por ejemplo, *mystorage007* .
2. Seleccione **Recursos compartidos de archivos** en *Almacenamiento de datos* y, a continuación, seleccione el *recurso compartido de archivos* que creó anteriormente.
3. Debería recibir el siguiente mensaje de error:



The screenshot shows the Azure Portal interface for a file share named 'my-file-share'. The left sidebar contains navigation links: Overview, Diagnose and solve problems, Access Control (IAM), Settings, Properties, Snapshots, and Backup. The main content area displays a large error message: 'This machine doesn't seem to have access.' Below this, it states 'This storage account is located in a VNET.' and provides a link to 'Learn more'. A 'Summary' box at the bottom contains the following details:

| Session ID  | Resource ID               |
|---|---------------------------|
| Extension: Microsoft_Azure_FileStorage  | Content: FilesGridBladev2 |
| Error code: 403   |                           |
| Details<br>code: AuthorizationFailure content: _CYCLIC_OBJECT_ message: This request is not authorized to perform this operation. |                           |

Se denegó el acceso porque su equipo no está en la *subred privada* de la *red virtual MyVirtualNetwork* .

## Limpiar recursos

Cuando ya no sea necesario, elimine el grupo de recursos y todos los recursos que contiene:

1. Ingrese *myResourceGroup* en el **cuadro de búsqueda** en la parte superior del portal. Cuando vea **myResourceGroup** en los resultados de búsqueda, selecciónelo.
2. Seleccione **Eliminar grupo de recursos** .
3. Ingrese *myResourceGroup* para **ESCRIBIR EL NOMBRE DEL GRUPO DE RECURSOS:** y seleccione **Eliminar** .