

Virtual machine networking

In this chapter, we'll cover Azure **Virtual Machines (VMs)** and the **network interface (NIC)** that is used as an interconnection between Azure VMs and Azure Virtual Network.

We will cover the following recipes in this chapter:

- Creating Azure VMs
- Viewing VM network settings
- Creating a new NIC
- Attaching an NIC to a VM
- Detaching an NIC from a VM

Technical requirements

For this chapter, the following is required:

- An Azure subscription

Creating Azure VMs

Azure VMs depend on virtual networking, and during the creation process, we need to define the network settings.

Getting ready

Before we start, open a web browser and go to the Azure portal at <https://portal.azure.com>.

How to do it...

In order to create a new VM using the Azure portal, we must use the following steps:

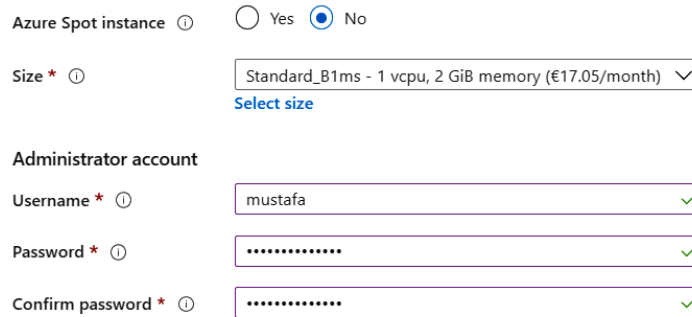
1. In the Azure portal, select **Create a resource** and choose the **Windows Server 2016 Datacenter** VM (or search for any VM image by searching for **image** in the **Search the Marketplace** search bar).
2. In the **Create a virtual machine** pane, we need to provide information for various options; not all of these are related to networking. First, we need to provide information on our Azure **Subscription** and **Resource group** (create a new resource group or provide an existing one).
3. In **Instance details**, we need to provide information for the **Virtual machine name**, **Region**, **Availability options**, and **Image** fields (for the **Image** field, leave the default or change to a different image from the drop-down menu). Some example settings are shown in *Figure 2.1*:

The screenshot displays the 'Create a virtual machine' pane in the Azure portal. It is divided into two main sections: 'Subscription and Resource group' and 'Instance details'. In the first section, 'Subscription' is set to 'Microsoft Azure Sponsorship' and 'Resource group' is set to 'Packt-Networking-Portal'. Below these is a link to 'Create new'. The 'Instance details' section contains five fields: 'Virtual machine name' (set to 'Packt' with a green checkmark), 'Region' (set to '(Europe) West Europe'), 'Availability options' (set to 'No infrastructure redundancy required'), and 'Image' (set to 'Windows Server 2016 Datacenter'). Below the 'Image' field is a link to 'Browse all public and private images'.

Subscription *	Microsoft Azure Sponsorship
Resource group *	Packt-Networking-Portal
Create new	
Instance details	
Virtual machine name *	Packt ✓
Region *	(Europe) West Europe
Availability options	No infrastructure redundancy required
Image *	Windows Server 2016 Datacenter
Browse all public and private images	

Figure 2.1: Providing information for Instance details

4. Next, we need to select whether we want to use **Azure Spot instance** (where the VM runs on unused datacenter capacity at a lower price but can be turned off if resources are needed elsewhere) and provide information on our VM's **Size**, **Username**, and **Password**. Note that for **Username**, you can't use names such as admin, administrator, sysadmin, or root. The password must be at least 12 characters long and satisfy three of the four common rules (that is, having uppercase letters, lowercase letters, special characters, and numbers). An example of the completed screen is shown in *Figure 2.2*:



Azure Spot instance ⓘ ☐ Yes ☒ No

Size * ⓘ Standard_B1ms - 1 vcpu, 2 GiB memory (€17.05/month) ▼
[Select size](#)

Administrator account

Username * ⓘ ✓

Password * ⓘ ✓

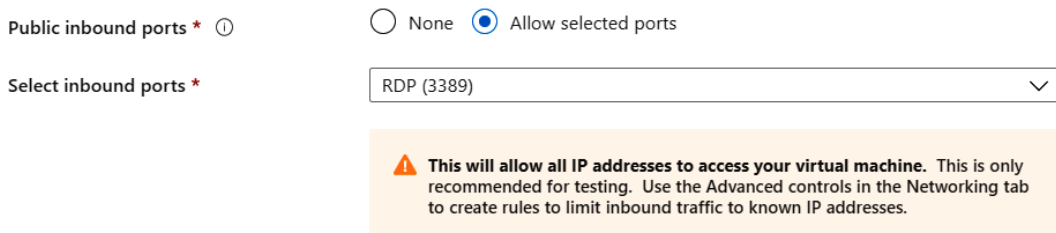
Confirm password * ⓘ ✓

Figure 2.2: Configuring Azure Spot instance

5. Next, we arrive at an option that concerns networking. We need to define whether we are going to allow any type of connection over a public IP address. We can select whether we want to deny all access or allow a specific port. Optionally, we can use **Hybrid Benefit** to use an existing license to save on costs. In the following example, I'm choosing **RDP (3389)**, but the dropdown also offers options for **SSH (22)**, **HTTP (80)**, and **HTTPS (443)**:

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 * RDP (3389) ▼

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

Save up to 49% with a license you already own using Azure Hybrid Benefit. [Learn more](#)

Already have a Windows Server license? * ☐ Yes ☒ No

ⓘ

Figure 2.3: Defining inbound port rules

6. In the next section, we need to define disks. We can choose between **Premium SSD**, **Standard SSD**, and **Standard HDD**. An OS disk is required and must be defined. We can attach additional data disks as needed. Disks can be added at a later time, as well. The default encryption option is to use platform-managed keys, but we can select customer-managed keys if needed. An example of disk settings with only the OS disk is shown in *Figure 2.4*:

Basics **Disks** Networking Management 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](#)

Disk options

OS disk type * ⓘ

Premium SSD

Encryption type *

(Default) Encryption at-rest with a platform-managed key

Enable Ultra Disk compatibility ⓘ

☐ Yes ☒ No

Ultra disk is available only for Availability Zones in westeurope.

Data disks

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
-----	------	------------	-----------	--------------

[Create and attach a new disk](#) [Attach an existing disk](#)

Figure 2.4: Setting up storage options

7. After defining disks, we get to the networking settings. Here, we need to define the **Virtual network** and **Subnet** options that the VM will use. These two options are mandatory. You can choose to assign the **Public IP** address to the VM (you can choose to disable the **Public IP** address, create a new one, or assign an existing IP address). The last part of the network settings relates to **NIC network security group**, where we need to choose whether we are going to use no network security group, a basic one, or an advanced one. There is also another option where we will define whether we will allow public ports. We can also configure **Accelerated networking** or **Load balancing** as additional options. An example of these VM network settings is shown in *Figure 2.5*:

Network interface

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

Virtual network * ⓘ

Packt-Portal

[Create new](#)

Subnet * ⓘ

FrontEnd (10.10.0.0/25)

[Manage subnet configuration](#)

Public IP ⓘ

(new) Packt-ip

[Create new](#)

NIC network security group ⓘ

☐ None ☒ Basic ☐ Advanced

Public inbound ports * ⓘ

☐ None ☒ Allow selected ports

Select inbound ports *

RDP (3389)



This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Accelerated networking ⓘ

☐ On ☒ Off

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?

☐ Yes ☒ No

Figure 2.5: Defining the virtual network and subnet options

8. After the networking section, we need to set up **Management** as shown in *Figure 2.6*:

Monitoring

Boot diagnostics ⓘ ☒ On ☐ Off

OS guest diagnostics ⓘ ☐ On ☒ Off

Diagnostics storage account * ⓘ

(new) packtnetworkingportal468 ▼

[Create new](#)

Identity

System assigned managed identity ⓘ ☐ On ☒ Off

Auto-shutdown

Enable auto-shutdown ⓘ ☐ On ☒ Off

Backup

Enable backup ⓘ ☐ On ☒ Off

Figure 2.6: Enabling management features

9. In **Advanced options**, we can set up post-deployment configuration steps by adding software installations, configuration scripts, custom data, and more. The **Advanced options** screen is shown in *Figure 2.7*:

Add additional configuration, agents, scripts or applications via virtual machine extensions or cloud-init.

Extensions

Extensions provide post-deployment configuration and automation.

Extensions ⓘ [Select an extension to install](#)

Custom data

Pass a script, configuration file, or other data into the virtual machine while it is being provisioned. The data will be saved on the VM in a known location. [Learn more about custom data for VMs](#) ↗

Custom data

i Custom data on the selected image will be processed by cloud-init. [Learn more about custom data and cloud init](#) ↗

Figure 2.7: Setting up post-deployment configuration

10. In the second part of **Advanced options**, we can select a **Host group** setting (this option provides a dedicated host that allows us to provision and manage a physical server in an Azure datacenter), a **Proximity placement group** (for grouping servers in the same region), and whether we want to use VMs from **Gen 1** or **Gen 2**. The default options are shown in *Figure 2.8*:

Host

Azure Dedicated Hosts allow you to provision and manage a physical server within our data centers that are dedicated to your Azure subscription. A dedicated host gives you assurance that only VMs from your subscription are on the host, flexibility to choose VMs from your subscription that will be provisioned on the host, and the control of platform maintenance at the level of the host. [Learn more](#)

Host group ⓘ

No host group found

Proximity placement group

Proximity placement groups allow you to group Azure resources physically closer together in the same region. [Learn more](#)

Proximity placement group ⓘ

No proximity placement groups found

VM generation

Generation 2 VMs support features such as UEFI-based boot architecture, increased memory and OS disk size limits, Intel® Software Guard Extensions (SGX), and virtual persistent memory (vPMEM).

VM generation ⓘ



Gen 1



Gen 2



Generation 2 VMs do not yet support some Azure platform features, including Azure Disk Encryption.

Figure 2.8: Allotting a dedicated host to provision and manage a physical server

11. The last setting that we can edit concerns tags. Tags apply additional metadata to Azure resources to logically organize them into a taxonomy. The **Tags** tab is shown in *Figure 2.9*:

Create a virtual machine

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

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. [Learn more about tags](#)

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name ⓘ

Value ⓘ

Resource

:

12 selected



Figure 2.9: Applying tags to Azure resources

12. After all the settings are defined, we get to the validation screen, where all our settings are checked for the last time. After validation is passed, we confirm the creation of a VM by clicking the **Create** button, as shown in Figure 2.10:

Create a virtual machine

✓
Validation passed

Basics
Disks
Networking
Management
Advanced
Tags
Review + create

PRODUCT DETAILS

Standard B1ms
by Microsoft

[Terms of use](#) | [Privacy policy](#)

Subscription credits apply ⓘ

0.0234 EUR/hr

[Pricing for other VM sizes](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Create

< Previous

Next >

Download a template for automation

Figure 2.10: Creation of a VM

How it works...

When a VM is created, an NIC is created in the process. An NIC is used as a sort of interconnection between the VM and the virtual network. An NIC is assigned a private IP address by the network. As an NIC is associated with both the VM and the virtual network, the IP address is used by the VM. Using this IP address, the VM can communicate over a private network with other VMs (or other Azure resources) on the same network. Additionally, NICs and VMs can be assigned public IP addresses as well. A public address can be used to communicate with the VM over the internet, either to access services or to manage the VM.

Now that we have created an Azure VM and defined network settings; in the next section, we'll see how to review these network settings.

There's more...

If you are interested in finding out more about Azure VMs, you can read my book, [Hands-On Cloud Administration in Azure](#), from Packt Publishing, where VMs are covered in more detail.

Viewing VM network settings

After an Azure VM is created, we can review the network settings in the VM pane.

Getting ready

Before you start, open a web browser and go to the Azure portal at <https://portal.azure.com>. Here, locate the previously created VM.

How to do it...

In order to review the VM network settings, we must follow the steps given here:

1. In the VM pane, locate the **Networking** settings. Here, you can see **Network interface**, **Application security groups**, and the **Network security group** associated with the VM. An example of this is shown in *Figure 2.11*:

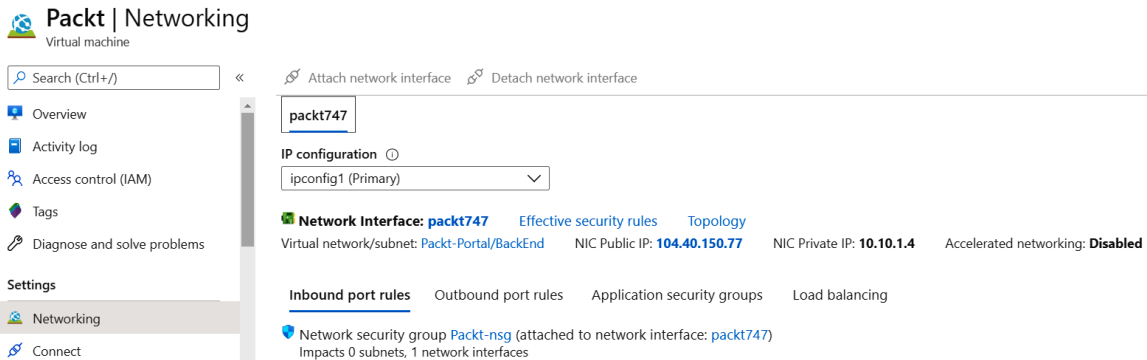


Figure 2.11: Network settings of a VM

2. If we select any of the associated network elements, we can discover more details. For example, if we select the **Network Interface** option associated with the VM, we can see other networking information such as **Private IP address**, **Public IP address**, **Virtual network/subnet**, **Network security group**, **IP configurations**, **DNS servers**, and more. The NIC view is shown in *Figure 2.12*:

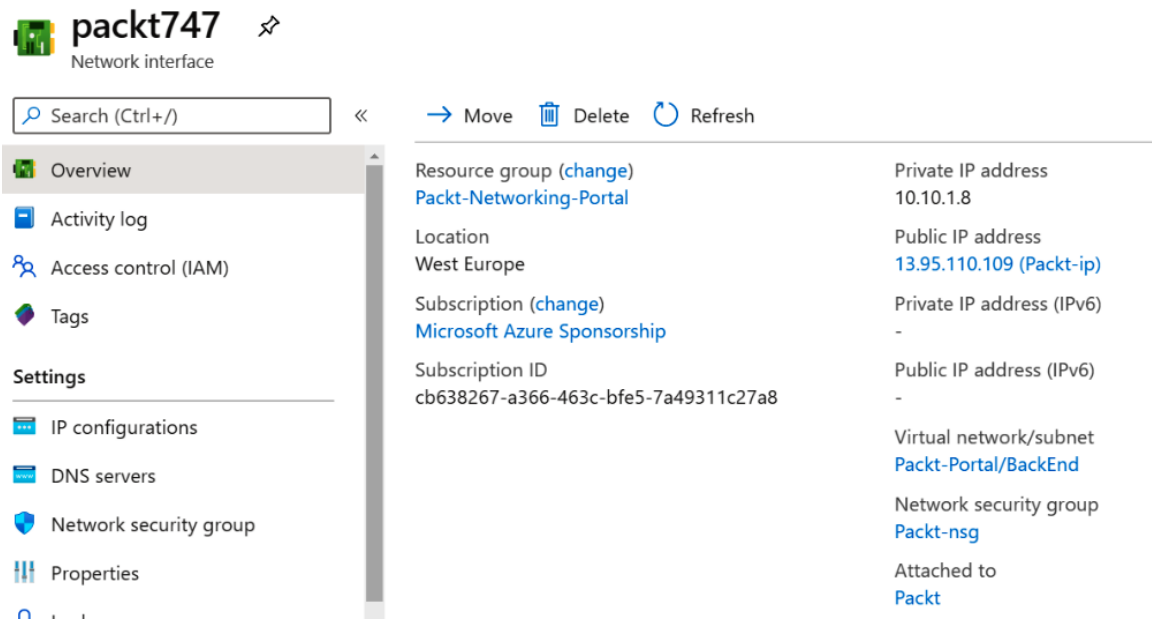


Figure 2.12: Viewing networking information from the NIC

How it works...

Networking information is displayed in several places, including in the VM's network settings. Additionally, each Azure resource has a separate pane and exists as an individual resource, so we can view these settings in multiple places. However, the most complete picture of VM network settings can be found in the VM pane and the NIC pane.

Creating a new NIC

An NIC is usually created during the VM creation process, but each VM can have multiple NICs. Based on this, we can create an NIC as an individual resource and attach it or detach it as needed.

Getting ready

Before you start, open a web browser and go to the Azure portal at <https://portal.azure.com>.

How to do it...

In order to create a new NIC using the Azure portal, we must take the following steps:

1. In the Azure portal, select **Create a resource** and choose **Network interface** under **Networking** services (or search for **network interface** in the search bar).
2. In the creation pane, we need to provide information for the **Name** and **Virtual network** fields, as well as giving the subnet that the NIC will be associated with. Other information to be provided includes the IP address assignment type (**Dynamic** or **Static**), whether we want the NIC to be associated with a **Network security group** type, and whether we want to use **IPv6**. All Azure resources require information on the **Subscription**, **Resource group**, and **Region**, and NICs are no exception. The information needed to create a new NIC is shown in *Figure 2.13*:

Create network interface

Project details

Subscription *

Resource group * [Create new](#)

Instance details

Name * ✓

Region *

Virtual network ⓘ [Manage selected virtual network](#)

Subnet * ⓘ

Private IP address assignment ☒ Dynamic ☐ Static

Network security group ⓘ

Private IP address (IPv6) ☐

Figure 2.13: Creating an NIC using the Azure portal

How it works...

An NIC can't exist without a network association, and this association must be assigned to a virtual network and subnet. This is defined during the creation process and cannot be changed later. On the other hand, association with a VM can be changed and the NIC can be attached or detached from a VM at any time.

Attaching an NIC to a VM

Each VM can have multiple NICs. Because of this, we can add a new NIC at any time.

Getting ready

Before you start, open a web browser and go to the Azure portal at <https://portal.azure.com>. Here, locate the VM we created earlier in this chapter.

How to do it...

To attach an NIC to a VM, we must do the following:

1. In the VM pane, make sure the VM is stopped (that is, deallocated).
2. Locate the **Networking** settings in the VM pane.
3. At the top of the **Networking** settings screen in the VM pane, select the **Attach network interface** option.
4. A new option will appear, allowing you to create a new NIC or select an already-existing NIC that is not associated with the VM.
5. Click **OK** and, in a few moments, the process will finish and the NIC will be associated with the VM. An example of this is shown in *Figure 2.14*:

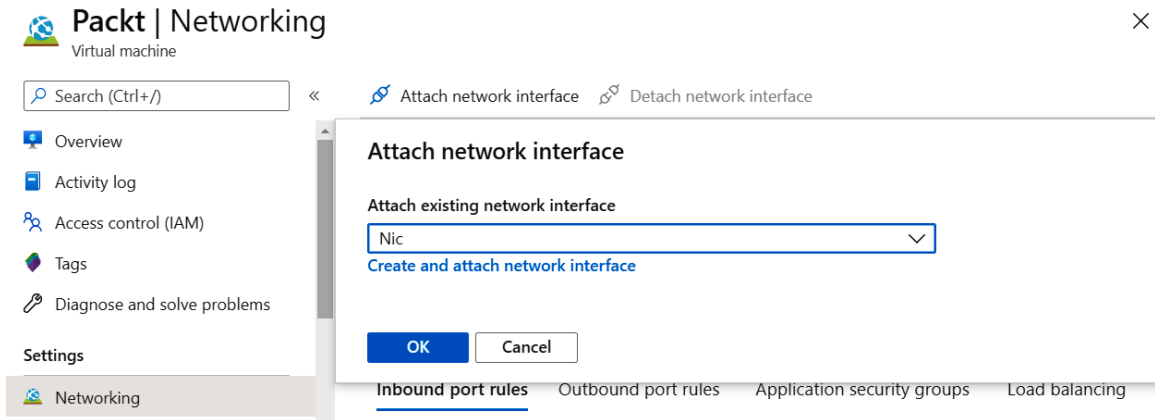


Figure 2.14: Attaching an NIC

How it works...

Each VM can have multiple NICs. The number of NICs that can be associated with a VM depends on the type and size of the VM. To attach an NIC to a VM, the VM needs to be stopped (that is, deallocated); you can't add an additional NIC to a running VM.

Detaching an NIC from a VM

Just as with attaching an NIC, we can detach an NIC at any time and attach it to another VM.

Getting ready

Before you start, open a web browser and go to the Azure portal at <https://portal.azure.com>. Here, locate the previously created VM.

How to do it...

To detach an NIC from a VM, we must do the following:

1. In the VM pane, make sure the VM is stopped (that is, deallocated).
2. Locate the **Networking** settings in the VM pane.
3. At the top of the **Networking** settings screen in the VM pane, select the **Detach network interface** option.
4. Select the NIC you want to detach from the VM.
5. Click **OK** and, in a few moments, the process will finish and the NIC will be removed from the VM. An example of this is shown in *Figure 2.15*:

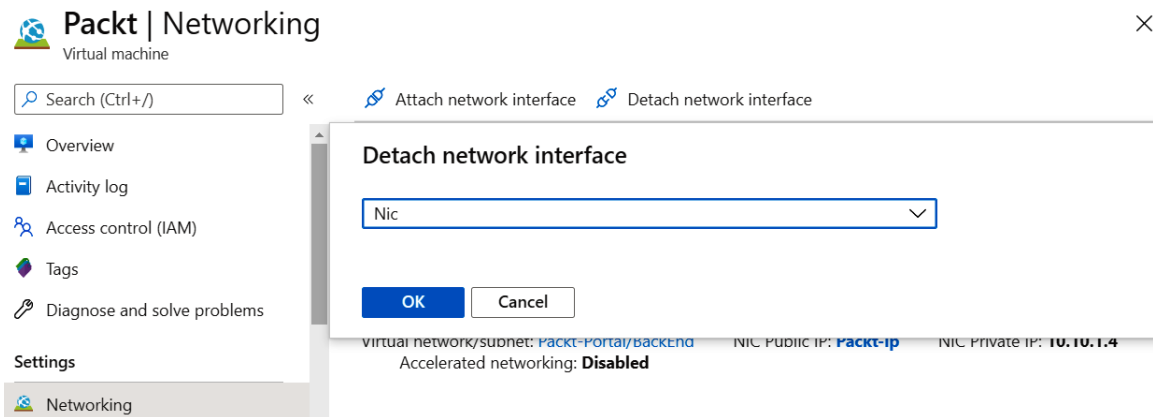


Figure 2.15: Detaching an NIC

How it works...

To detach an NIC, the VM associated with the NIC must be stopped (that is, deallocated). At least one NIC must be associated with the VM—so you can't remove the last NIC from a VM. All network associations stay with the NIC—they are assigned to the NIC, not to the VM.

