# Virtual Network

Virtual networks (VNets) are used in Azure to provide private connectivity between Azure Virtual Machines and other Azure services. Services that are part of the same VN can access one another by default, and you canconfigure the network to allow access to the external service, including your on-premises servers.

## Address spaces

If the VNet will be connected to other VNets, you must select address ranges that are not overlapping. This is the range of private addresses that the VMs and services in your network can use. Azure will treat any address range as part of the private VNet IP address space if it is only reachable within the VNet, within interconnected VNets, and from your on-premises location.

## Subnets

You can create one or more subnets for your virtual network. You do this to break up your network into more manageable sections. For example, you might assign 10.1.0.0 to VMs, 10.2.0.0 to back-end services, and 10.3.0.0 to SQL Server VMs. Azure reserves the first four addresses and the last address in each subnet for its use.

## Security

You can set up Network Security Groups (NSGs), which allow you to control the traffic flow to and from subnets and to and from VMs. NSGs act as software firewalls, applying custom rules to each inbound or outbound request at the network interface and subnet level.

## Azure VM IP addresses

Azure VMs communicate on a virtual network. They can also have an optional public IP address assigned to them. With a public IP, we can interact with the VM over the Internet. Alternatively, we can set up a virtual private network (VPN) that connects our on-premises network to Azure - letting us securely connect to the VM without exposing a public IP. You can pay more to assign static addresses, if you want to connect directly to an IP address and need to ensure that the IP address will not change.

# Resources

Just like a physical computer in your datacenter, VMs have several elements that are needed to do their job, Azure will create all these resources if necessary, or you can supply existing ones.

* The VM itself
* Storage account for the disks
* Virtual network (shared with other VMs and services)
* Network interface to communicate on the network
* Network Security Group(s) to secure the network traffic
* Public Internet address (optional)

# VM name

You can specify a name of up to 15 characters on a Windows VM and 64 characters on a Linux VM. This name also defines a manageable Azure resource, and it's not trivial to change later. That means you should choose names that are meaningful and consistent, so you can easily identify what the VM does.

# VM location

You must select a region where you want the resources (CPU, storage, etc.) to be allocated. This lets you place your VMs as close as possible to your users to improve performance and to meet any legal, compliance, or tax requirements. Each region has different hardware available and some configurations are not available in all regions, also, there are price differences between locations.

# VM size

Azure provides a wide range of VM size options allowing you to select the appropriate mix of compute, memory, and storage for what you want to do. Based on the workload, you're able to choose from a subset of available VM sizes. Workload options are classified as follows on Azure:

|  |  |
| --- | --- |
| **Option** | **Description** |
| General purpose | General-purpose VMs are designed to have a balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers. |
| Compute optimized | Compute optimized VMs are designed to have a high CPU-to-memory ratio. Suitable for medium traffic web servers, network appliances, batch processes, and application servers. |
| Memory optimized | Memory optimized VMs are designed to have a high memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics. |
| Storage optimized | Storage optimized VMs are designed to have high disk throughput and IO. Ideal for VMs running databases. |
| GPU | GPU VMs are specialized virtual machines targeted for heavy graphics rendering and video editing. These VMs are ideal options for model training and inferencing with deep learning. |
| High performance computes | High performance compute is the fastest and most powerful CPU virtual machines with optional high-throughput network interfaces. |

Azure allows you to change the VM size when the existing size no longer meets your needs. You can upgrade or downgrade the VM - as long as your current hardware configuration is allowed in the new size.

Be careful about resizing production VMs - they will be rebooted automatically which can cause a temporary outage and change some configuration settings such as the IP address.

# VM storage

All Azure virtual machines will have at least two virtual hard disks (VHDs). The first disk stores the operating system, and the second is used as temporary storage. You can add additional disks to store application data; the maximum number is determined by the VM size selection (typically two per CPU).

Virtual disks can be backed by either **Standard** (magnetic disks) or **Premium** (solid state disks) Storage accounts.

|  |  |
| --- | --- |
| **Option** | **Description** |
| Unmanaged disks | With unmanaged disks, you are responsible for the storage accounts that are used to hold the VHDs that correspond to your VM disks. You pay the storage account rates for the amount of space you use. A single storage account has a fixed-rate limit of 20,000 I/O operations/sec. This means that a storage account is capable of supporting 40 standard virtual hard disks at full utilization. If you need to scale out with more disks, then you'll need more storage accounts, which can get complicated. |
| Managed disks | Managed disks are the newer and recommended disk storage model. They elegantly solve this complexity by putting the burden of managing the storage accounts onto Azure. You specify the size of the disk, up to 4 TB, and Azure creates and manages both the disk and the storage. You don't have to worry about storage account limits, which makes managed disks easier to scale out. |

# Pricing model

By separating these costs, you scale them independently and only pay for what you need.

## Compute costs

It’s a per-hour basis but billed on a per-minute basis. You are not charged for compute capacity if you stop and deallocate the VM since this release the hardware. It includes the charge for the operating system, so Linux-based instances are cheaper.

## Storage costs

Even if the VM is stopped/deallocated, you will be charged for the storage used by the disks. You're able to choose from two payment options for compute costs:

|  |  |
| --- | --- |
| **Option** | **Description** |
| Pay as you go | With the pay-as-you-go option, you pay for compute capacity by the second, with no long-term commitment or upfront payments. You're able to increase or decrease compute capacity on demand as well as start or stop at any time. Prefer this option if you run applications with short-term or unpredictable workloads that cannot be interrupted. For example, if you are doing a quick test, or developing an app in a VM, this would be the appropriate option. |
| Reserved Virtual Machine Instances | The Reserved Virtual Machine Instances (RI) option is an advance purchase of a virtual machine for one or three years in a specified region. The commitment is made up front, and in return, you get up to 72% price savings compared to pay-as-you-go pricing. RIs are flexible and can easily be exchanged or returned for an early termination fee. Prefer this option if the VM has to run continuously, or you need budget predictability, and you can commit to using the VM for at least a year. |

# Resource Manager templates

Resource Manager templates are JSON files that define the resources you need to deploy for your solution. You can create resource templates from the **Settings** section for a specific VM by selecting the **Export template** option. You have the option to save the resource template for later use or immediately deploy a new VM based on this template.

# Azure VM Extensions

Azure VM extensions are small applications that allow you to configure and automate tasks on Azure VMs after initial deployment. Azure VM extensions can be run with the Azure CLI, PowerShell, Azure Resource Manager templates, and the Azure portal.

# Azure Automation Services

Azure Automation allows you to integrate services that allow you to automate frequent, time-consuming, and error-prone management tasks with ease. These services include process automation, configuration management, and update management

* **Process Automation** allows you to set up watcher tasks that can respond to events that may occur in your datacenter.
* **Configuration Management** allows you to track the updates and take action as required. You use Microsoft Endpoint Configuration Manager to manage your company's PC, servers, and mobile devices. You can extend this support to your Azure VMs with Configuration Manager.
* **Update Management** incorporates services that provide process and configuration management. You enable update management for a VM directly from your Azure Automation account. You can also allow update management for a single virtual machine from the virtual machine pane in the portal.

# Availability

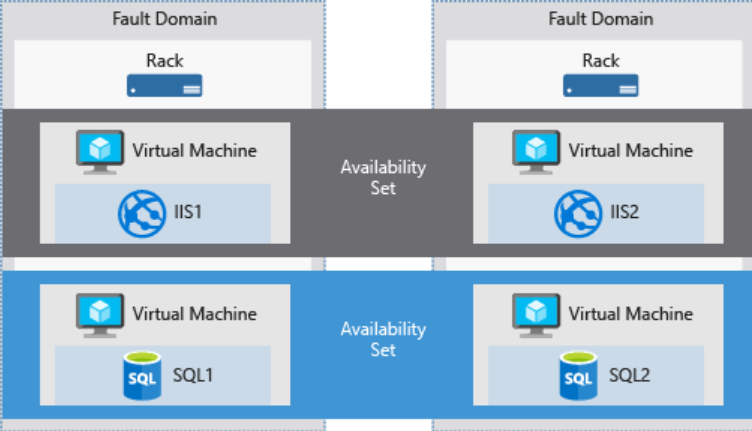
Availability is the percentage of time a service is available for use. If the physical server fails, the virtual machines hosted on that server will also fail. If this happens, Azure will move the VM to a healthy host server automatically. However, this self-healing migration could take several minutes, during which, the application(s) hosted on that VM will not be available. To avoid this, it's recommended to deploy at least two instances of each VM. This feature is called an availability set.

## Availability set

Availability sets are a powerful feature to ensure the services running in your VMs are always available to your customers. You can create availability sets through the Azure portal in the disaster recovery section. Also, you can build them using Resource Manager templates, or any of the scripting or API tools. When you place VMs into an availability set, Azure guarantees to spread them across Fault Domains and Update Domains.

***Fault domain***

A fault domain is a logical group of hardware in Azure that shares a common power source and network switch. You can think of it as a rack within an on-premises datacenter.



***Update domain***

An update domain is a logical group of hardware that can undergo maintenance or be rebooted at the same time. Azure will automatically place availability sets into update domains to minimize the impact when the Azure platform introduces host operating system changes. Azure then processes each update domain one at a time.

# Azure Backup

Maintaining a good backup strategy will ensure you aren't scrambling when data or software needs to be restored. Azure Backup is a backup as a service offering that protects physical or virtual machines no matter where they reside: on-premises or in the cloud. Azure Backup was designed to work in tandem with other Azure services and provides several distinct benefits.

* **Automatic storage management**. Azure Backup automatically allocates and manages backup storage and uses a pay-as-you-use model. You only pay for what you use.
* **Unlimited scaling**. Azure Backup uses the power and scalability of Azure to deliver high availability.
* **Multiple storage options**. Azure Backup offers locally redundant storage where all copies of the data exist within the same region and geo-redundant storage where your data is replicated to a secondary region.
* **Unlimited data transfer**. Azure Backup does not limit the amount of inbound or outbound data you transfer. Azure Backup also does not charge for the data that is transferred.
* **Data encryption**. Data encryption allows for secure transmission and storage of your data in Azure.
* **Application-consistent backup**. An application-consistent backup means that a recovery point has all required data to restore the backup copy. Azure Backup provides application-consistent backups.
* **Long-term retention**. Azure doesn't limit the length of time you keep the backup data.

# Creating an Azure VM

VMs can be defined and deployed on Azure in several ways: the Azure portal, a script (using the Azure CLI or Azure PowerShell), or an Azure Resource Manager template. In all cases, you will need to supply several pieces of information that we'll cover shortly.

The Azure Marketplace also provides preconfigured images that include both an OS and favorite software tools installed for specific scenarios.

# Opening ports in Azure VMs

There are two steps to adjusting the configuration to support different protocols on the network. When you create a new VM, you have an opportunity to open a few common ports (RDP, HTTP, HTTPS, and SSH). However, if you require other changes to the firewall, you will need to adjust them manually.

1. Create a network security group.
2. Create an inbound rule allowing traffic on the ports you need.

## Network security group

NSGs are an optional security layer that provides a software firewall by filtering inbound and outbound traffic on the VNet.

## Security group rules

NSGs use rules to allow or deny traffic moving through the network. Each rule identifies the source and destination address (or range), protocol, port (or range), direction (inbound or outbound), a numeric priority, and whether to allow or deny the traffic that matches the rule. The rules are evaluated in priority order, starting with the lowest priority rule. Deny rules always stop the evaluation.

# Linux virtual machine

## SSH

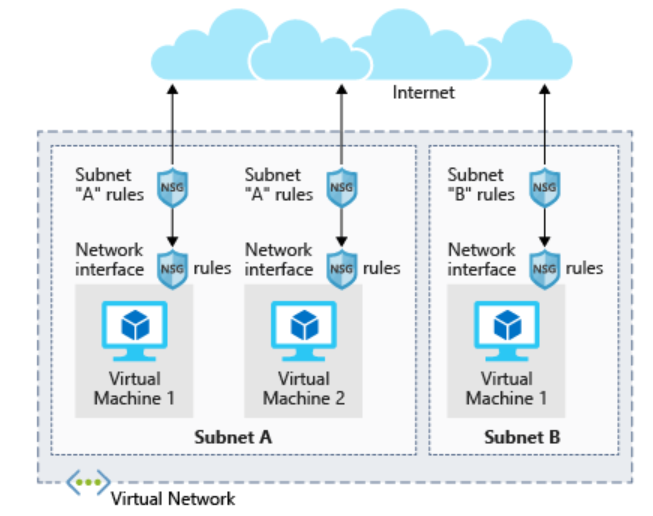
Secure Shell (SSH) is an encrypted connection protocol that allows secure sign-ins over unsecured connections. SSH allows you to connect to a terminal shell from a remote location using a network connection.

* ***Username and password:*** Using it leaves the VM vulnerable to brute-force attacks, but if you need to be able to access the Linux VM from a variety of locations, it might be a better approach
* ***SSH key pair:*** A more secure and preferred method of connecting to a Linux VM with SSH, if you only plan to sign in to the VM from a few computers, is a public-private key pair, also known as SSH keys. On Linux, Windows 10, and macOS, you can use the built-in **ssh-keygen** command to generate the SSH public and private key files.
* ***Private key passphrase:*** You can provide a passphrase while generating your private key. This is a password you must enter when you use the key. If a passphrase protects a private key, it cannot be used by that attacker. This provides an additional layer of security for your infrastructure on Azure.

## Connecting to the VM with SSH

To connect to the VM via SSH, you need:

* the public IP address of the VM
* the username of the local account on the VM
* a public key configured in that account
* access to the corresponding private key
* port 22 open on the VM



# Windows virtual machines

## Remote Desktop Protocol

RDP enables you to sign in to a remote physical or virtual Windows computer and control that computer as if you were seated at the console. An RDP connection enables you to carry out the vast majority of operations that you can do from the console of a physical computer, with the exception of some power and hardware-related functions.

Microsoft provides RDP clients for the following operating systems:

* Windows (built-in)
* macOS
* iOS
* Android

There are also open-source Linux clients, such as **Remmina** that enable you to connect to a Windows PC from an Ubuntu distribution.

## Using RDP

In the Azure portal, you go to the properties of your VM, and at the top, click **Connect**. This will show you the IP addresses assigned to the VM and give you the option to download a **preconfigured.rdp** file that Windows then opens in the RDP client. You can choose to connect over the public IP address of the VM in the RDP file. Instead, if you're connecting over VPN or ExpressRoute, you can select the internal IP address. You can also select the port number for the connection.

It uses port 3389 by default so this port is the standard port you would open if you wanted to use an RDP client to administer your Windows virtual machines.

## Initialize data disks

Any additional drives you create from scratch will need to be initialized and formatted. The process for doing this is identical to a physical drive.

1. Launch the **Disk Management** tool from the Start Menu. You may have to go to the Computer Management tool first, then Disk Management, or try searching for "Disk Management" in the Start Menu.
2. It will display a warning that it has detected an uninitialized disk.
3. Screenshot showing the disk management tool warning about an uninitialized data disk in the VM.
4. Click **OK** to initialize the disk. It will then show up in the list of volumes where you can format it and assign a drive letter.
5. Open File Explorer and you should now see your data drive.
6. Go ahead and close the RDP client to sign out of the VM. The server will continue to run.