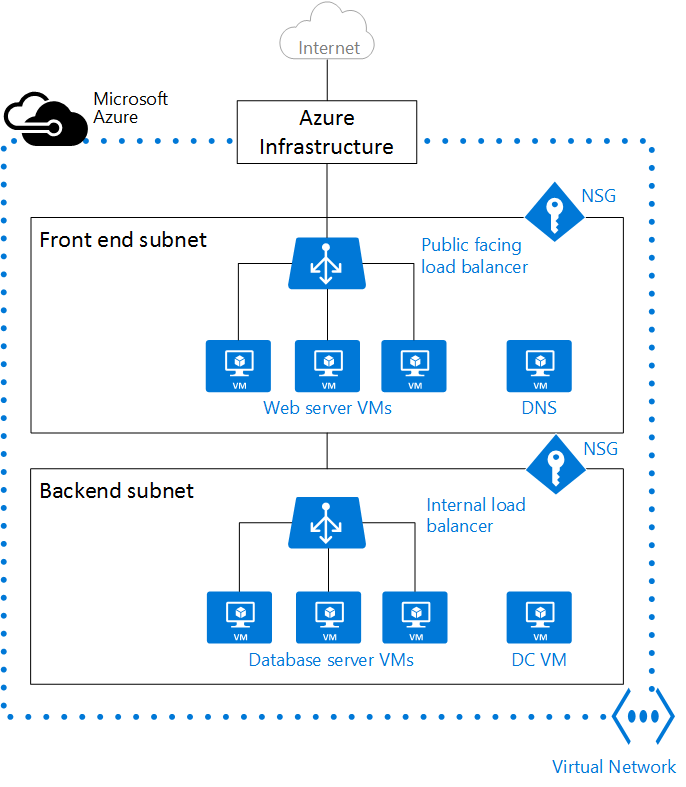
Virtual networks and virtual machines in Azure

an Azure virtual machine (VM), you must create a [virtual network](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview) (VNet) or use an existing VNet. You also need to decide how your VMs are intended to be accessed on the VNet. It is important to [plan before creating resources](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-vnet-plan-design-arm) and make sure that you understand the [limits of networking resources](https://docs.microsoft.com/en-us/azure/azure-subscription-service-limits#networking-limits).

In the following figure, VMs are represented as web servers and database servers. Each set of VMs are assigned to separate subnets in the VNet.



You can create a VNet before you create a VM or you can as you create a VM. You create these resources to support communication with a VM:

* Network interfaces
* IP addresses
* Virtual network and subnets

In addition to those basic resources, you should also consider these optional resources:

* Network security groups
* Load balancers

Network interfaces

A [network interface (NIC)](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-network-interface) is the interconnection between a VM and a virtual network (VNet). A VM must have at least one NIC, but can have more than one, depending on the size of the VM you create. Learn about how many NICs each VM size supports for [Windows](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/sizes) or [Linux](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/sizes).

You can create a VM with multiple NICs, and add or remove NICs through the lifecycle of a VM. Multiple NICs allow a VM to connect to different subnets and send or receive traffic over the most appropriate interface.

If the VM is added to an availability set, all VMs within the availability set must have one or multiple NICs. VMs with more than one NIC aren’t required to have the same number of NICs, but they must all have at least two.

Each NIC attached to a VM must exist in the same location and subscription as the VM. Each NIC must be connected to a VNet that exists in the same Azure location and subscription as the NIC. You can change the subnet a VM is connected to after it's created, but you cannot change the VNet. Each NIC attached to a VM is assigned a MAC address that doesn’t change until the VM is deleted.

This table lists the methods that you can use to create a network interface.

| Method | Description |
| --- | --- |
| Azure portal | When you create a VM in the Azure portal, a network interface is automatically created for you (you cannot use a NIC you create separately). The portal creates a VM with only one NIC. If you want to create a VM with more than one NIC, you must create it with a different method. |
| [Azure PowerShell](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/multiple-nics) | Use [New-AzureRmNetworkInterface](https://docs.microsoft.com/en-us/powershell/module/azurerm.network/new-azurermnetworkinterface) with the **-PublicIpAddressId** parameter to provide the identifer of the public IP address that you previously created. |
| [Azure CLI](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/multiple-nics) | To provide the identifer of the public IP address that you previously created, use [az network nic create](https://docs.microsoft.com/cli/azure/network/nic" \l "create) with the **--public-ip-address** parameter. |
| [Template](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-deploy-multinic-arm-template) | Use [Network Interface in a Virtual Network with Public IP Address](https://github.com/Azure/azure-quickstart-templates/tree/master/101-nic-publicip-dns-vnet) as a guide for deploying a network interface using a template. |

IP addresses

You can assign these types of [IP addresses](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-ip-addresses-overview-arm) to a NIC in Azure:

* **Public IP addresses** - Used to communicate inbound and outbound (without network address translation (NAT)) with the Internet and other Azure resources not connected to a VNet. Assigning a public IP address to a NIC is optional. Public IP addresses have a nominal charge, and there's a maximum number that can be used per subscription.
* **Private IP addresses** - Used for communication within a VNet, your on-premises network, and the Internet (with NAT). You must assign at least one private IP address to a VM. To learn more about NAT in Azure, read [Understanding outbound connections in Azure](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-outbound-connections).

You can assign public IP addresses to VMs or internet-facing load balancers. You can assign private IP addresses to VMs and internal load balancers. You assign IP addresses to a VM using a network interface.

There are two methods in which an IP address is allocated to a resource - dynamic or static. The default allocation method is dynamic, where an IP address is not allocated when it's created. Instead, the IP address is allocated when you create a VM or start a stopped VM. The IP address is released when you stop or delete the VM.

To ensure the IP address for the VM remains the same, you can set the allocation method explicitly to static. In this case, an IP address is assigned immediately. It is released only when you delete the VM or change its allocation method to dynamic.

This table lists the methods that you can use to create an IP address.

| Method | Description |
| --- | --- |
| [Azure portal](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-deploy-static-pip-arm-portal) | By default, public IP addresses are dynamic and the address associated to them may change when the VM is stopped or deleted. To guarantee that the VM always uses the same public IP address, create a static public IP address. By default, the portal assigns a dynamic private IP address to a NIC when creating a VM. You can change this IP address to static after the VM is created. |
| [Azure PowerShell](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-deploy-static-pip-arm-ps) | You use [New-AzureRmPublicIpAddress](https://docs.microsoft.com/en-us/powershell/module/azurerm.network/new-azurermpublicipaddress) with the **-AllocationMethod** parameter as Dynamic or Static. |
| [Azure CLI](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-deploy-static-pip-arm-cli) | You use [az network public-ip create](https://docs.microsoft.com/cli/azure/network/public-ip" \l "create) with the **--allocation-method** parameter as Dynamic or Static. |
| [Template](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-deploy-static-pip-arm-template) | Use [Network Interface in a Virtual Network with Public IP Address](https://github.com/Azure/azure-quickstart-templates/tree/master/101-nic-publicip-dns-vnet) as a guide for deploying a public IP address using a template. |

After you create a public IP address, you can associate it with a VM by assigning it to a NIC.

Virtual network and subnets

A subnet is a range of IP addresses in the VNet. You can divide a VNet into multiple subnets for organization and security. Each NIC in a VM is connected to one subnet in one VNet. NICs connected to subnets (same or different) within a VNet can communicate with each other without any extra configuration.

When you set up a VNet, you specify the topology, including the available address spaces and subnets. If the VNet is to be connected to other VNets or on-premises networks, you must select address ranges that don't overlap. The IP addresses are private and can't be accessed from the Internet, which was true only for the non-routeable IP addresses such as 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16. Now, Azure treats any address range as part of the private VNet IP address space that is only reachable within the VNet, within interconnected VNets, and from your on-premises location.

If you work within an organization in which someone else is responsible for the internal networks, you should talk to that person before selecting your address space. Make sure there is no overlap and let them know the space you want to use so they don’t try to use the same range of IP addresses.

By default, there is no security boundary between subnets, so VMs in each of these subnets can talk to one another. However, 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.

This table lists the methods that you can use to create a VNet and subnets.

| Method | Description |
| --- | --- |
| [Azure portal](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-vnet-arm-pportal) | If you let Azure create a VNet when you create a VM, the name is a combination of the resource group name that contains the VNet and **-vnet**. The address space is 10.0.0.0/24, the required subnet name is **default**, and the subnet address range is 10.0.0.0/24. |
| [Azure PowerShell](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-vnet-arm-ps) | You use [New-AzureRmVirtualNetworkSubnetConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmVirtualNetworkSubnetConfig) and [New-AzureRmVirtualNetwork](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmVirtualNetwork) to create a subnet and a VNet. You can also use [Add-AzureRmVirtualNetworkSubnetConfig](https://docs.microsoft.com/en-us/powershell/module/azurerm.network/add-azurermvirtualnetworksubnetconfig) to add a subnet to an existing VNet. |
| [Azure CLI](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-vnet-arm-cli) | The subnet and the VNet are created at the same time. Provide a **--subnet-name** parameter to [az network vnet create](https://docs.microsoft.com/cli/azure/network/vnet" \l "create) with the subnet name. |
| [Template](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-vnet-arm-template-click) | The easiest way to create a VNet and subnets is to download an existing template, such as [Virtual Network with two Subnets](https://github.com/Azure/azure-quickstart-templates/tree/master/101-vnet-two-subnets), and modify it for your needs. |

Network security groups

A [network security group (NSG)](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg) contains a list of Access Control List (ACL) rules that allow or deny network traffic to subnets, NICs, or both. NSGs can be associated with either subnets or individual NICs connected to a subnet. When an NSG is associated with a subnet, the ACL rules apply to all the VMs in that subnet. In addition, traffic to an individual NIC can be restricted by associating an NSG directly to a NIC.

NSGs contain two sets of rules: inbound and outbound. The priority for a rule must be unique within each set. Each rule has properties of protocol, source and destination port ranges, address prefixes, direction of traffic, priority, and access type.

All NSGs contain a set of default rules. The default rules cannot be deleted, but because they are assigned the lowest priority, they can be overridden by the rules that you create.

When you associate an NSG to a NIC, the network access rules in the NSG are applied only to that NIC. If an NSG is applied to a single NIC on a multi-NIC VM, it does not affect traffic to the other NICs. You can associate different NSGs to a NIC (or VM, depending on the deployment model) and the subnet that a NIC or VM is bound to. Priority is given based on the direction of traffic.

Be sure to [plan](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-nsg#planning) your NSGs when you plan your VMs and VNet.

This table lists the methods that you can use to create a network security group.

| Method | Description |
| --- | --- |
| [Azure portal](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-nsg-arm-pportal) | When you create a VM in the Azure portal, an NSG is automatically created and associated to the NIC the portal creates. The name of the NSG is a combination of the name of the VM and **-nsg**. This NSG contains one inbound rule with a priority of 1000, service set to RDP, the protocol set to TCP, port set to 3389, and action set to Allow. If you want to allow any other inbound traffic to the VM, you must add additional rules to the NSG. |
| [Azure PowerShell](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-nsg-arm-ps) | Use [New-AzureRmNetworkSecurityRuleConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmNetworkSecurityRuleConfig) and provide the required rule information. Use [New-AzureRmNetworkSecurityGroup](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmNetworkSecurityGroup) to create the NSG. Use [Set-AzureRmVirtualNetworkSubnetConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/Set-AzureRmVirtualNetworkSubnetConfig) to configure the NSG for the subnet. Use [Set-AzureRmVirtualNetwork](https://docs.microsoft.com/en-us/powershell/module/azurerm.network/set-azurermvirtualnetwork) to add the NSG to the VNet. |
| [Azure CLI](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-nsg-arm-cli) | Use [az network nsg create](https://docs.microsoft.com/cli/azure/network/nsg" \l "create) to initially create the NSG. Use [az network nsg rule create](https://docs.microsoft.com/cli/azure/network/nsg/rule" \l "create) to add rules to the NSG. Use [az network vnet subnet update](https://docs.microsoft.com/cli/azure/network/vnet/subnet" \l "update) to add the NSG to the subnet. |
| [Template](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-create-nsg-arm-template) | Use [Create a Network Security Group](https://github.com/Azure/azure-quickstart-templates/tree/master/101-security-group-create) as a guide for deploying a network security group using a template. |

Load balancers

[Azure Load Balancer](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview) delivers high availability and network performance to your applications. A load balancer can be configured to [balance incoming Internet traffic](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-internet-overview) to VMs or [balance traffic between VMs in a VNet](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-internal-overview). A load balancer can also balance traffic between on-premises computers and VMs in a cross-premises network, or forward external traffic to a specific VM.

The load balancer maps incoming and outgoing traffic between the public IP address and port on the load balancer and the private IP address and port of the VM.

When you create a load balancer, you must also consider these configuration elements:

* **Front-end IP configuration** – A load balancer can include one or more front-end IP addresses, otherwise known as virtual IPs (VIPs). These IP addresses serve as ingress for the traffic.
* **Back-end address pool** – IP addresses that are associated with the NIC to which load is distributed.
* **NAT rules** - Defines how inbound traffic flows through the front-end IP and distributed to the back-end IP.
* **Load balancer rules** - Maps a given front-end IP and port combination to a set of back-end IP addresses and port combination. A single load balancer can have multiple load balancing rules. Each rule is a combination of a front-end IP and port and back-end IP and port associated with VMs.
* [**Probes**](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-custom-probe-overview) - Monitors the health of VMs. When a probe fails to respond, the load balancer stops sending new connections to the unhealthy VM. The existing connections are not affected, and new connections are sent to healthy VMs.

This table lists the methods that you can use to create an internet-facing load balancer.

| Method | Description |
| --- | --- |
| Azure portal | You can't currently create an internet-facing load balancer using the Azure portal. |
| [Azure PowerShell](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-internet-arm-ps) | To provide the identifer of the public IP address that you previously created, use [New-AzureRmLoadBalancerFrontendIpConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmLoadBalancerFrontendIpConfig) with the **-PublicIpAddress** parameter. Use [New-AzureRmLoadBalancerBackendAddressPoolConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmLoadBalancerBackendAddressPoolConfig) to create the configuration of the back-end address pool. Use [New-AzureRmLoadBalancerInboundNatRuleConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmLoadBalancerInboundNatRuleConfig) to create inbound NAT rules associated with the front-end IP configuration that you created. Use [New-AzureRmLoadBalancerProbeConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmLoadBalancerProbeConfig) to create the probes that you need. Use [New-AzureRmLoadBalancerRuleConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmLoadBalancerRuleConfig) to create the load balancer configuration. Use [New-AzureRmLoadBalancer](https://docs.microsoft.com/en-us/powershell/module/azurerm.network/new-azurermloadbalancer) to create the load balancer. |
| [Azure CLI](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-internet-arm-cli) | Use [az network lb create](https://docs.microsoft.com/cli/azure/network/lb" \l "create) to create the initial load balancer configuration. Use [az network lb frontend-ip create](https://docs.microsoft.com/cli/azure/network/lb/frontend-ip" \l "create) to add the public IP address that you previously created. Use [az network lb address-pool create](https://docs.microsoft.com/cli/azure/network/lb/address-pool" \l "create) to add the configuration of the back-end address pool. Use [az network lb inbound-nat-rule create](https://docs.microsoft.com/cli/azure/network/lb/inbound-nat-rule" \l "create) to add NAT rules. Use [az network lb rule create](https://docs.microsoft.com/cli/azure/network/lb/rule" \l "create) to add the load balancer rules. Use [az network lb probe create](https://docs.microsoft.com/cli/azure/network/lb/probe" \l "create) to add the probes. |
| [Template](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-internet-arm-template) | Use [2 VMs in a Load Balancer and configure NAT rules on the LB](https://github.com/Azure/azure-quickstart-templates/tree/master/201-2-vms-loadbalancer-natrules) as a guide for deploying a load balancer using a template. |

This table lists the methods that you can use to create an internal load balancer.

| Method | Description |
| --- | --- |
| Azure portal | You can't currently create an internal load balancer using the Azure portal. |
| [Azure PowerShell](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-ilb-arm-ps) | To provide a private IP address in the network subnet, use [New-AzureRmLoadBalancerFrontendIpConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmLoadBalancerFrontendIpConfig) with the **-PrivateIpAddress** parameter. Use [New-AzureRmLoadBalancerBackendAddressPoolConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmLoadBalancerBackendAddressPoolConfig) to create the configuration of the back-end address pool. Use [New-AzureRmLoadBalancerInboundNatRuleConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmLoadBalancerInboundNatRuleConfig) to create inbound NAT rules associated with the front-end IP configuration that you created. Use [New-AzureRmLoadBalancerProbeConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmLoadBalancerProbeConfig) to create the probes that you need. Use [New-AzureRmLoadBalancerRuleConfig](https://docs.microsoft.com/powershell/resourcemanager/AzureRM.Network/v1.0.13/New-AzureRmLoadBalancerRuleConfig) to create the load balancer configuration. Use [New-AzureRmLoadBalancer](https://docs.microsoft.com/en-us/powershell/module/azurerm.network/new-azurermloadbalancer) to create the load balancer. |
| [Azure CLI](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-ilb-arm-cli) | Use the [az network lb create](https://docs.microsoft.com/cli/azure/network/lb" \l "create) command to create the initial load balancer configuration. To define the private IP address, use [az network lb frontend-ip create](https://docs.microsoft.com/cli/azure/network/lb/frontend-ip" \l "create) with the **--private-ip-address** parameter. Use [az network lb address-pool create](https://docs.microsoft.com/cli/azure/network/lb/address-pool" \l "create) to add the configuration of the back-end address pool. Use [az network lb inbound-nat-rule create](https://docs.microsoft.com/cli/azure/network/lb/inbound-nat-rule" \l "create) to add NAT rules. Use [az network lb rule create](https://docs.microsoft.com/cli/azure/network/lb/rule" \l "create) to add the load balancer rules. Use [az network lb probe create](https://docs.microsoft.com/cli/azure/network/lb/probe" \l "create) to add the probes. |
| [Template](https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-get-started-ilb-arm-template) | Use [2 VMs in a Load Balancer and configure NAT rules on the LB](https://github.com/Azure/azure-quickstart-templates/tree/master/201-2-vms-internal-load-balancer) as a guide for deploying a load balancer using a template. |

VMs

VMs can be created in the same VNet and they can connect to each other using private IP addresses. They can connect even if they are in different subnets without the need to configure a gateway or use public IP addresses. To put VMs into a VNet, you create the VNet and then as you create each VM, you assign it to the VNet and subnet. VMs acquire their network settings during deployment or startup.

VMs are assigned an IP address when they are deployed. If you deploy multiple VMs into a VNet or subnet, they are assigned IP addresses as they boot up. A dynamic IP address (DIP) is the internal IP address associated with a VM. You can allocate a static DIP to a VM. If you allocate a static DIP, you should consider using a specific subnet to avoid accidentally reusing a static DIP for another VM.

If you create a VM and later want to migrate it into a VNet, it is not a simple configuration change. You must redeploy the VM into the VNet. The easiest way to redeploy is to delete the VM, but not any disks attached to it, and then re-create the VM using the original disks in the VNet.

This table lists the methods that you can use to create a VM in a VNet.

| Method | Description |
| --- | --- |
| [Azure portal](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/quick-create-portal) | Uses the default network settings that were previously mentioned to create a VM with a single NIC. To create a VM with multiple NICs, you must use a different method. |
| [Azure PowerShell](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/tutorial-manage-vm) | Includes the use of [Add-AzureRmVMNetworkInterface](https://docs.microsoft.com/en-us/powershell/module/azurerm.compute/add-azurermvmnetworkinterface) to add the NIC that you previously created to the VM configuration. |
| [Azure CLI](https://docs.microsoft.com/en-us/azure/virtual-machines/linux/create-cli-complete) | Create and connect a VM to a Vnet, subnet, and NIC that build as individual steps. |
| [Template](https://docs.microsoft.com/en-us/azure/virtual-machines/windows/ps-template) | Use [Very simple deployment of a Windows VM](https://github.com/Azure/azure-quickstart-templates/tree/master/101-vm-simple-windows) as a guide for deploying a VM using a template. |