

## **Microsoft Azure Cloud Overview**

Azure is Microsoft's public cloud platform. It Provides:

- On demand delivery of IT resources over internet
- You just pay for what you use
- Azure offers a large collection of services, which includes platform as a service (PaaS), infrastructure as a service (IaaS), and managed database service capabilities.

## **Cloud Compute Services in Azure**

Applications in Azure run on compute services. As part of Microsoft Azure services, the following services are available:

- Azure Virtual Machine
- Azure Virtual Machine Scale Sets
- Azure App Services
- Azure Container Instances
- Azure Kubernetes Services
- Azure Functions
- Azure Virtual Desktops

## **Azure Virtual Machine**

- Azure virtual machines are one of several types of on-demand, scalable computing resources that Azure offers.
- Typically, you choose a virtual machine when you need more control over the computing environment than the other choices offer.
- An Azure virtual machine gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs it.
- However, you still need to maintain the virtual machine by performing tasks, such as configuring, patching, and installing the software that runs on it.
- Azure Virtual machine will let us create and use virtual machines in the cloud as Infrastructure as a Service.
- We can use an image provided by Azure, or partner, or we can use our own to create the virtual machine.
- Using Azure virtual machine, we can able to deploy different services such as Windows, Linux within the Azure cloud.
- Virtual machines can be created and managed using:
  - Azure Portal
  - Azure PowerShell and ARM templates
  - Azure CLI
  - Client SDK's
  - REST APIs
- Following are the configuration choices that Azure offers while creating a Virtual Machine.
  - Operating system (Windows and Linux)

- VM size, which determines factors such as processing power, how many disks we attach etc.
- The region where VM will be hosted
- VM extension, which gives additional capabilities such as running anti-virus etc.
- Compute, Networking, and Storage elements will be created during the provisioning of the virtual machine.

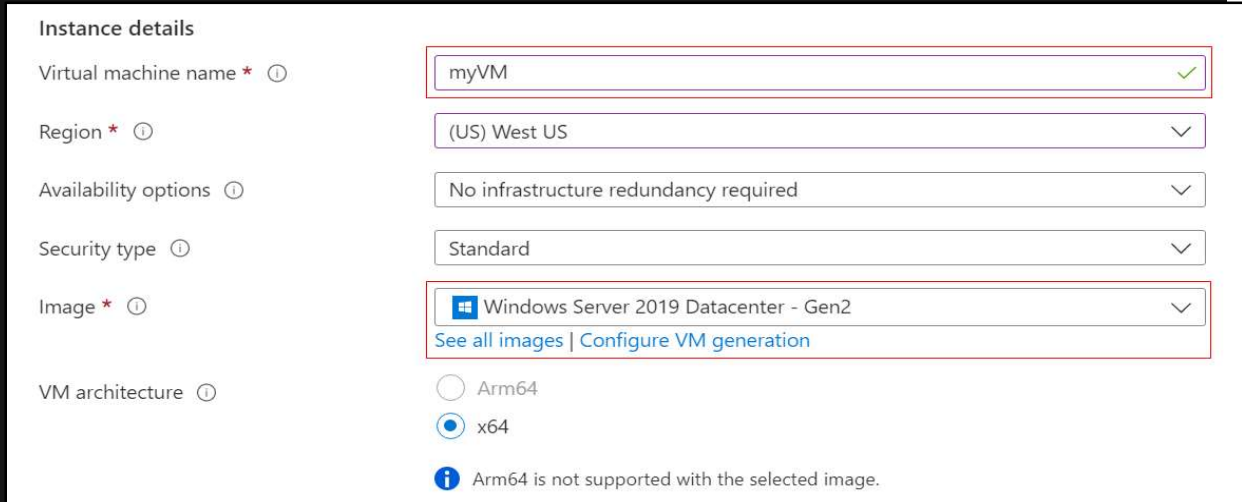
## Deploying a Virtual Machine

- Building and Deploying Windows Virtual Machine
- Building and Deploying linux Virtual Machine

## Building a Windows Virtual Machine

**Following steps are involved in creating and deploying a windows virtual machine:**

1. Enter virtual machines in the search.
2. Under Services, select Virtual machines.
3. In the Virtual machines page, select Create and then Azure virtual machine. The Create a virtual machine page opens.
4. Under Instance details, enter myVM for the Virtual machine name and choose *Windows Server 2019 Datacenter - Gen 2* for the Image. Leave the other defaults.



**Instance details**

Virtual machine name \* ⓘ  ✓

Region \* ⓘ  ▼

Availability options ⓘ  ▼

Security type ⓘ  ▼

Image \* ⓘ  ▼  
[See all images](#) | [Configure VM generation](#)

VM architecture ⓘ

☐ Arm64

☒ x64

**i** Arm64 is not supported with the selected image.

5. Under **Administrator account**, provide a username, such as *azureuser* and a password. The password must be at least 12 characters long and meet the defined complexity requirements.

**Administrator account**

Username \* ⓘ  ✓

Password \* ⓘ  ✓

Confirm password \* ⓘ  ✓

- Under **Inbound port rules**, choose **Allow selected ports** and then select **RDP (3389)** and **HTTP (80)** from the drop-down.

**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 \*  ▼

**⚠ 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.

- Leave the remaining defaults and then select the **Review + create** button at the bottom of the page.

**Licensing**

Save up to 49% 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 >

- After validation runs, select the **Create** button at the bottom of the page.

Home > Virtual machines >

## Create a virtual machine

Validation passed

**Basics**

Subscription	myAzureSubscription
Resource group	(new) myVM_group_08290738
Virtual machine name	myVM
Region	East US
Availability options	No infrastructure redundancy required
Security type	Standard
Image	Windows Server 2022 Datacenter: Azure Edition - Gen2
VM architecture	x64
Size	Standard D2s v3 (2 vcpus, 8 GiB memory)
Username	azureuser
Public inbound ports	RDP
Already have a Windows license?	No

Create < Previous Next > Download a template for automation

- After deployment is complete, select **Go to resource**.

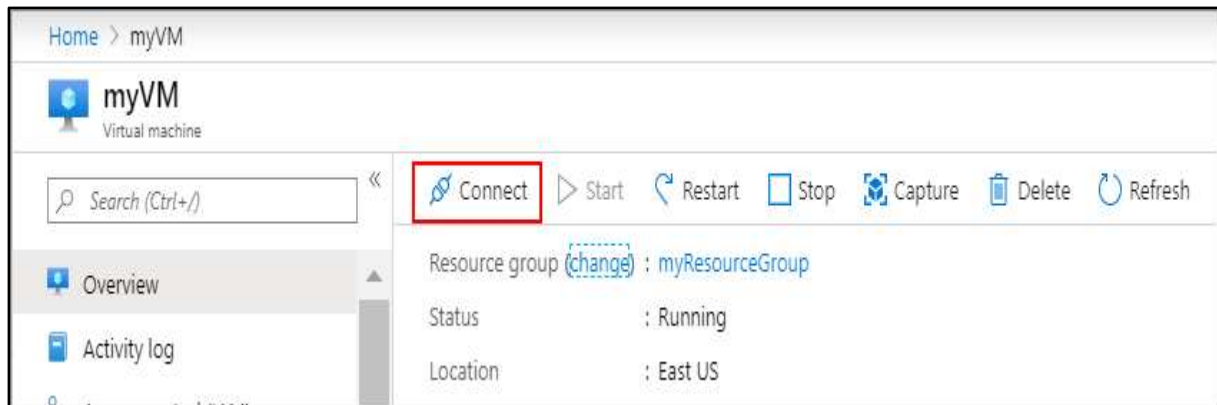
Next steps

- Setup auto-shutdown Recommended
- Monitor VM health, performance and network dependencies Recommended
- Run a script inside the virtual machine Recommended

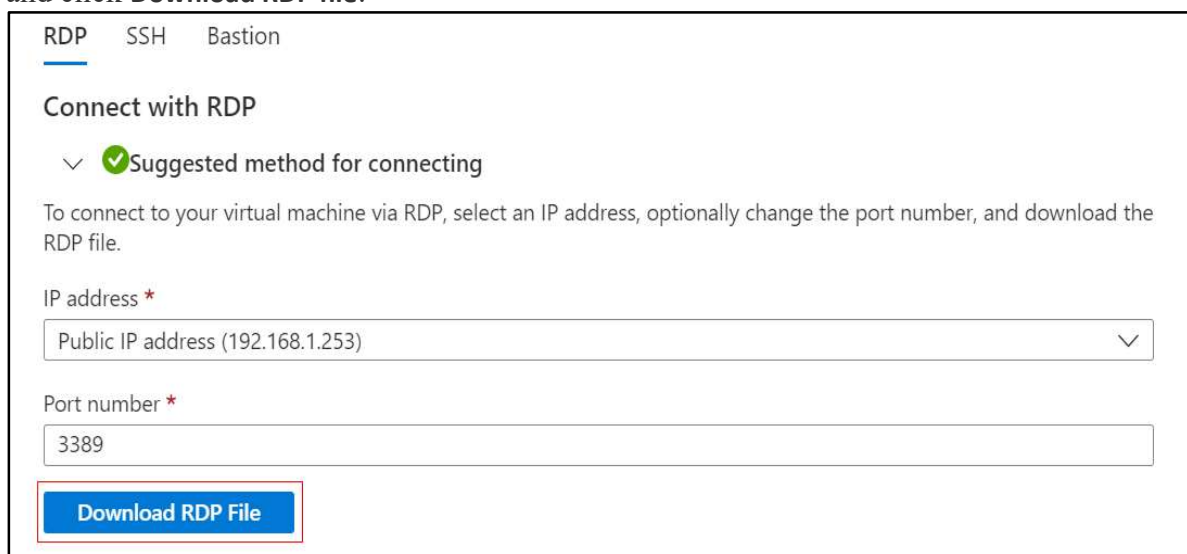
Go to resource Create another VM

## Connecting to the virtual machine

- Create a remote desktop connection to the virtual machine. These directions tell you how to connect to your VM from a Windows computer. On a Mac, you need an RDP client such as this Remote Desktop Client from the Mac App Store.
- On the overview page for your virtual machine, select the **Connect > RDP**.



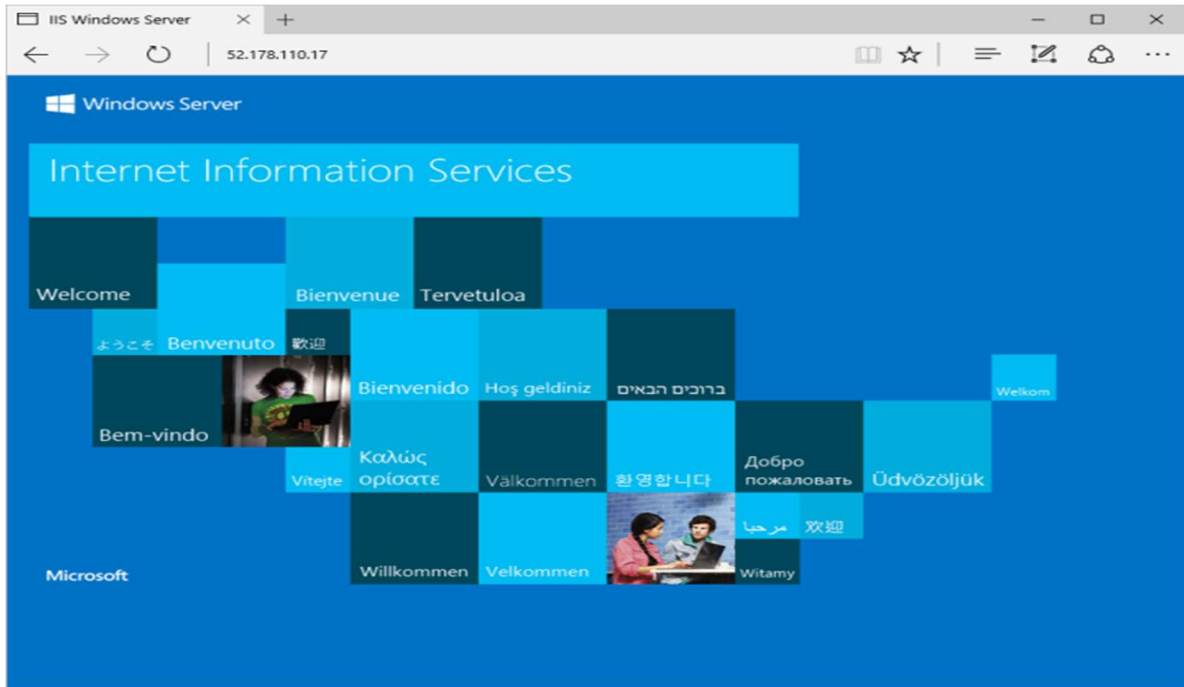
3. In the **Connect with RDP** tab, keep the default options to connect by IP address, over port 3389, and click **Download RDP file**.



4. Open the downloaded RDP file and click **Connect** when prompted.
5. In the **Windows Security** window, select **More choices** and then **Use a different account**. Type the username as **localhost\username**, enter the password you created for the virtual machine, and then click **OK**.
6. You may receive a certificate warning during the sign-in process. Click **Yes** or **Continue** to create the connection.

## Installing web server (IIS)

1. To see your VM in action, install the IIS web server. Open a PowerShell prompt on the VM and run the following command:  
***Install-WindowsFeature -name Web-Server -IncludeManagementTools***  
 When done, close the RDP connection to the VM.
2. View the IIS welcome page  
 In the portal, select the VM and in the overview of the VM, hover over the IP address to show **Copy to clipboard**. Copy the IP address and paste it into a browser tab. The default IIS welcome page will open, and should look like this:

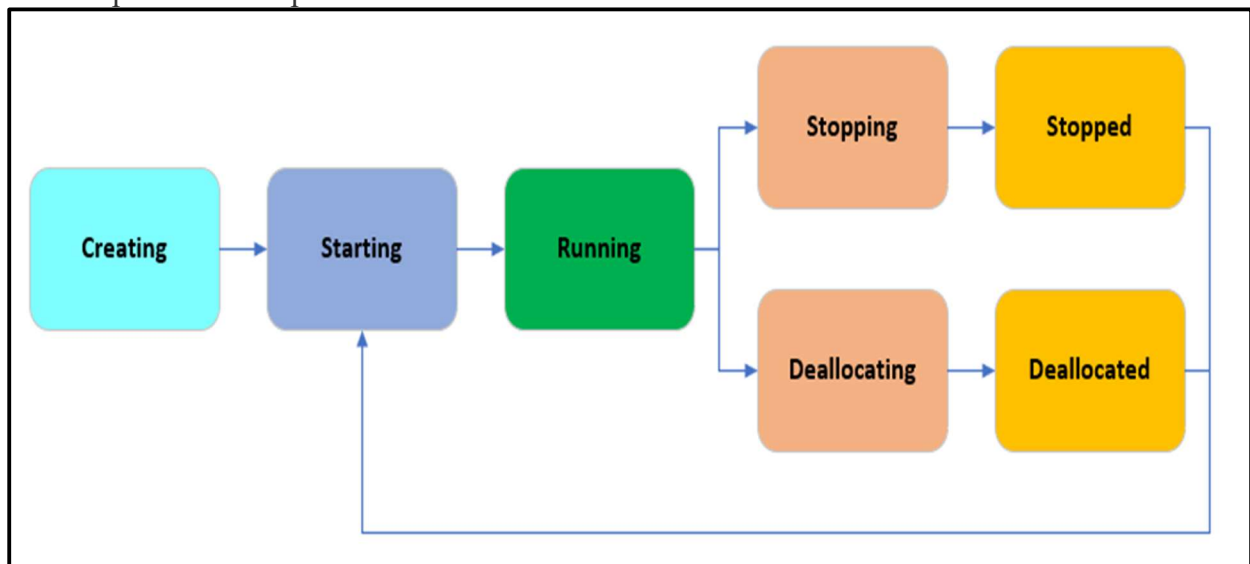


## States of Virtual machine

1. Azure Virtual Machines (VM) instances go through different states. There are *provisioning* and *power* states.

### Power states

2. The power state represents the last known state of the VM.



The following table provides a description of each instance state:

Power state	Description
Creating	Virtual machine is allocating resources.
Starting	Virtual machine is powering up.
Running	Virtual machine is fully up. This state is the standard working state.
Stopping	This state is transitional between running and stopped.
Stopped	The virtual machine is allocated on a host but not running. Also called <i>PoweredOff</i> state or <i>Stopped (Allocated)</i> .
Deallocating	This state is transitional between <i>Running</i> and <i>Deallocated</i> .
Deallocated	The virtual machine has released the lease on the underlying hardware and is powered off. This state is also referred to as <i>Stopped (Deallocated)</i> .

### **Provisioning states**

The provisioning state is the status of a user-initiated, control-plane operation on the VM. These states are separate from the power state of a VM.

Provisioning state	Description
Creating	Virtual machine is being created.
Updating	Virtual machine is updating to the latest model. Some non-model changes to a virtual machine such as start and restart fall under the updating state.
Failed	Last operation on the virtual machine resource was unsuccessful.
Succeeded	Last operation on the virtual machine resource was successful.
Deleting	Virtual machine is being deleted.
Migrating	Seen when migrating from Azure Service Manager to Azure Resource Manager.

### **Building a Linux Virtual machine**

**Following steps are involved in creating and deploying a Linux virtual machine:**

- Enter *virtual machines* in the search.
- Under **Services**, select **Virtual machines**.
- In the **Virtual machines** page, select **Create** and then **Virtual machine**. The **Create a virtual machine** page opens.
- In the **Basics** tab, under **Project details**, make sure the correct subscription is selected and then choose to **Create new** resource group. Enter *myResourceGroup* for the name.\*.

**Project details**

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

Subscription \* ⓘ Pay-As-You-Go ✓

Resource group \* ⓘ (New) myResourceGroup ✓

[Create new](#)

- Under **Instance details**, enter *myVM* for the **Virtual machine name**, and choose *Ubuntu 18.04 LTS - Gen2* for your **Image**. Leave the other defaults. The default size and pricing is only shown as an example. Size availability and pricing are dependent on your region and subscription.


**Instance details**

Virtual machine name \* ⓘ myVM ✓

Region \* ⓘ (US) East US ✓

Availability options ⓘ No infrastructure redundancy required ✓

Security type ⓘ Standard ✓

Image \* ⓘ  Ubuntu Server 18.04 LTS - Gen2 ✓

[See all images](#) | [Configure VM generation](#)

Azure Spot instance ⓘ ☐

Size \* ⓘ Standard\_DS1\_v2 - 1 vcpu, 3.5 GiB memory ✓

[See all sizes](#)

- Under Administrator account, select SSH public key.
- In Username enter azureuser.
- For SSH public key source, leave the default of Generate new key pair, and then enter myKey for the Key pair name.



**Administrator account**

Authentication type <sup>①</sup> ☒ SSH public key ☐ Password

Username \* <sup>①</sup>  ✓

SSH public key source  ▼

Key pair name \*  ✓


- Under Inbound port rules > Public inbound ports, choose Allow selected ports and then select SSH (22) and HTTP (80) from the drop-down.

**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 \* <sup>①</sup> ☐ None ☒ Allow selected ports

Select inbound ports \*  ▼

 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.

- Leave the remaining defaults and then select the Review + create button at the bottom of the page.
- On the Create a virtual machine page, you can see the details about the VM you are about to create. When you are ready, select Create.
- When the Generate new key pair window opens, select Download private key and create resource. Your key file will be download as myKey.pem. Make sure you know where the .pem file was downloaded; you will need the path to it in the next step.
- When the deployment is finished, select Go to resource.
- On the page for your new VM, select the public IP address and copy it to your clipboard.

Operating system	: Linux (ubuntu 18.04 LTS)
Size	: Standard D2s v3 (2 vCPUs, 8 GB memory)
Public IP address	: 10.111.12.123 

**Copy to clipboard**

## Connect to virtual machine

1. Create an SSH connection with the VM.
2. If you are on a Windows machine, open a PowerShell prompt.
3. At your prompt, open an SSH connection to your virtual machine. Replace the IP address with the one from your VM, and replace the path to the .pem with the path to where the key file was downloaded.

```
ssh -i ~/Downloads/myKey.pem azureuser@10.111.12.123
```

## Install web server

1. To see your VM in action, install the NGINX web server. From your SSH session, update your package sources and then install the latest NGINX package.

```
sudo apt-get -y update
```

```
sudo apt-get -y install nginx
```

2. When done, type exit to leave the SSH session.
3. View the web server in action
4. Use a web browser of your choice to view the default NGINX welcome page. Type the public IP address of the VM as the web address. The public IP address can be found on the VM overview page or as part of the SSH connection string you used earlier.



## Cloud Networking Services in Azure

The networking services in Azure provide a variety of networking capabilities that can be used together or separately.

- **Connectivity services:** Connect Azure resources and on-premises resources using any or a combination of these networking services in Azure - Virtual Network (VNet), Virtual

WAN, ExpressRoute, VPN Gateway, Virtual network NAT Gateway, Azure DNS, Peering service, and Azure Bastion.

- **Application protection services:** Protect your applications using any or a combination of these networking services in Azure - Load Balancer, Private Link, DDoS protection, Firewall, Network Security Groups, Web Application Firewall, and Virtual Network Endpoints.
- **Application delivery services:** Deliver applications in the Azure network using any or a combination of these networking services in Azure - Content Delivery Network (CDN), Azure Front Door Service, Traffic Manager, Application Gateway, Internet Analyzer, and Load Balancer.
- **Network monitoring:** Monitor your network resources using any or a combination of these networking services in Azure - Network Watcher, ExpressRoute Monitor, Azure Monitor, or VNet Terminal Access Point (TAP).

## **Virtual network**

- 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.
- Why use an Azure Virtual network?
  - Azure virtual network enables Azure resources to securely communicate with each other, the internet, and on-premises networks.
  - Key scenarios that you can accomplish with a virtual network include - communication of Azure resources with the internet, communication between Azure resources, communication with on-premises resources, filtering network traffic, routing network traffic, and integration with Azure services.
- You can use VNets to:
  - **Communicate between Azure resources:** You can deploy VMs, and several other types of Azure resources to a virtual network.
  - **Communicate between each other:** You can connect virtual networks to each other, enabling resources in either virtual network to communicate with each other, using virtual network peering.
  - **Communicate to the internet:** All resources in a VNet can communicate outbound to the internet, by default. You can communicate inbound to a resource by assigning a public IP address or a public Load Balancer. You can also use [Public IP addresses](#) or public [Load Balancer](#) to manage your outbound connections.
  - **Communicate with on-premises networks:** You can connect your on-premises computers and networks to a virtual network

## **Network Security Groups**

- You can use an Azure network security group to filter network traffic between Azure resources in an Azure virtual network.

- A network security group contains [security rules](#) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.
- For each rule, you can specify source and destination, port, and protocol.
- A network security group contains zero, or as many rules as desired.
- Each rule specifies the following properties: source, source port, destination, destination port, and protocol.
- Security rules are evaluated and applied based on the five-tuple (source, source port, destination, destination port, and protocol) information. You can't create two security rules with the same priority and direction.
- Default security rules: Azure creates the following default rules in each network security group that you create:

#### *Inbound*

##### AllowVNetInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

##### AllowAzureLoadBalancerInBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	AzureLoadBalancer	0-65535	0.0.0.0/0	0-65535	Any	Allow

##### DenyAllInbound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

#### *Outbound*

##### AllowVnetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65000	VirtualNetwork	0-65535	VirtualNetwork	0-65535	Any	Allow

##### AllowInternetOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65001	0.0.0.0/0	0-65535	Internet	0-65535	Any	Allow

##### DenyAllOutBound

Priority	Source	Source ports	Destination	Destination ports	Protocol	Access
65500	0.0.0.0/0	0-65535	0.0.0.0/0	0-65535	Any	Deny

## Virtual Network Peering

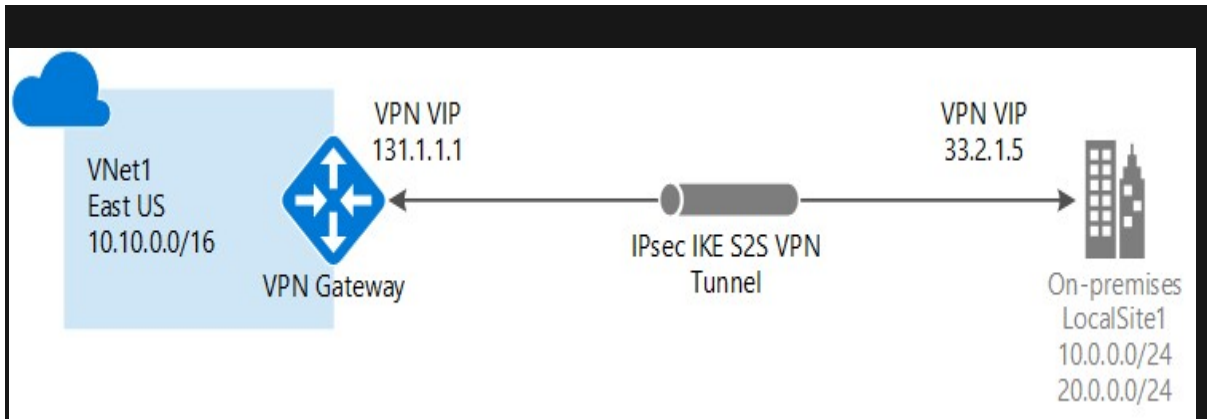
- Virtual network peering enables you to seamlessly connect two or more [Virtual Networks](#) in Azure.
- The traffic between virtual machines in peered virtual networks uses the Microsoft backbone infrastructure.
- Like traffic between virtual machines in the same network, traffic is routed through Microsoft's *private* network only.
- Azure supports the following types of peering:
  - **Virtual network peering:** Connecting virtual networks within the same Azure region.
  - **Global virtual network peering:** Connecting virtual networks across Azure regions.
- The benefits of using virtual network peering, whether local or global, include:
  - A low-latency, high-bandwidth connection between resources in different virtual networks.
  - The ability for resources in one virtual network to communicate with resources in a different virtual network.
  - The ability to transfer data between virtual networks across Azure subscriptions, Azure Active Directory tenants, deployment models, and Azure regions.
  - The ability to peer virtual networks created through the Azure Resource Manager.
  - The ability to peer a virtual network created through Resource Manager to one created through the classic deployment model.
  - No downtime to resources in either virtual network when creating the peering, or after the peering is created.
- Network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft backbone network.
- No public Internet, gateways, or encryption is required in the communication between the virtual networks.

## Azure VPN

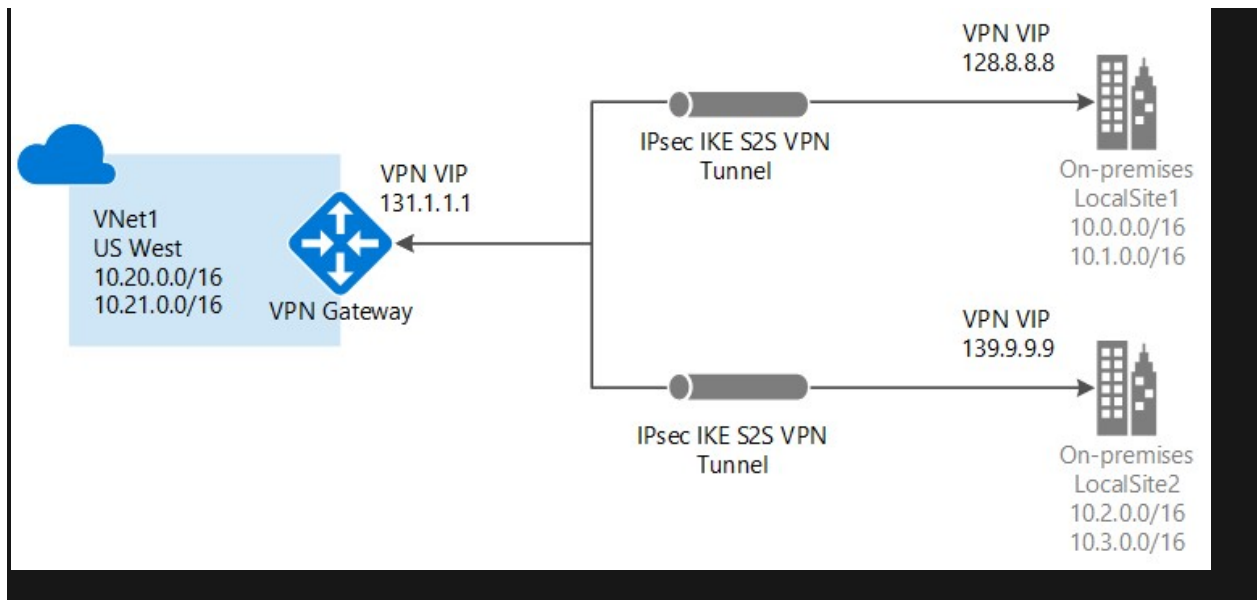
- Azure VPN Gateway is a service that uses a specific type of virtual network gateway to send encrypted traffic between an Azure virtual network and on-premises locations over the public Internet.
- You can also use VPN Gateway to send encrypted traffic between Azure virtual networks over the Microsoft network.
- In Azure , we have following options to connect azure virtual network to on-premise network (Remote Network).
  - Site-to-Site VPN connections
  - Point-to-Site VPN connections
  - VNet-to-VNet VPN connections

## Site-to-Site VPN connections

- A Site-to-Site (S2S) VPN gateway connection is a connection over IPsec/IKE (IKEv1 or IKEv2) VPN tunnel.
- S2S connections can be used for cross-premises and hybrid configurations.
- A S2S connection requires a VPN device located on-premises that has a public IP address assigned to it.



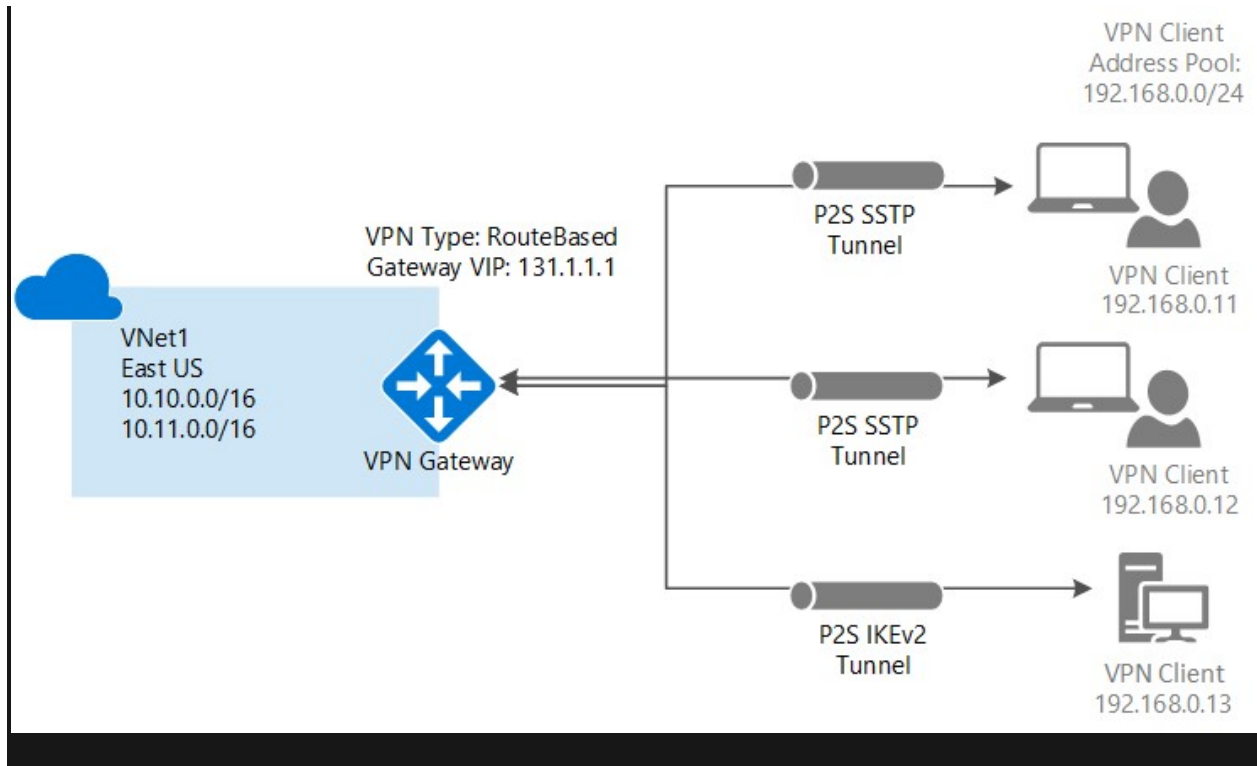
- You can create more than one VPN connection from your virtual network gateway, typically connecting to multiple on-premises sites.



## Point-to-Site VPN

- A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer.
- A P2S connection is established by starting it from the client computer.
- This solution is useful who want to connect to Azure VNets from a remote location, such as from home or a conference.

- Unlike S2S connections, P2S connections do not require an on-premises public-facing IP address or a VPN device.



### VNet-to-VNet connections

- Connecting a virtual network to another virtual network (VNet-to-VNet) is similar to connecting a VNet to an on-premises site location. Both connectivity types use a VPN gateway to provide a secure tunnel using IPsec/IKE. You can even combine VNet-to-VNet communication with multi-site connection configurations.
- the VNets you connect can be:
  - in the same or different regions
  - in the same or different subscriptions
  - in the same or different deployment models

