

Microsoft AZ-104
Azure Administrator Associate
Quick Reference Guide



A Microsoft Azure Administrator course you will help you learn how to manage, control, and oversee Azure subscriptions, secure identities, administer the infrastructure, configure virtual networking, connect Azure and on-premises sites, manage network traffic, implement storage solutions, create, and scale virtual machines, implement web apps and containers, back up and share data, and monitor your solution, and much more.

Skill Covered:

- Manage Azure Identities and Governance (15-20%)
- Implement and Manage Storage (15-20%)
- Deploy and Manage Azure Compute Resources (20-25%)
- Configure and Manage Virtual Networking (25-30%)
- Monitor and Back up Azure Resources (10-15%)

Certification Name & Exam Code:

Microsoft Certified: Azure Administrator Associate

[Microsoft Azure Administrator AZ-104](#)

Prepared By: Deepanshu Sood
Connect At: [LinkedIn](#)

Disclaimer

This document is produced by Deepanshu Sood for the sole of purpose of making the quick study notes while studying Microsoft Azure Administrator Associate course. All the notes have been in reference to multiple resources available on internet, like: Microsoft Azure website, Alan Rodrigues course notes on Udemy.com, etc. I do not take any responsibility if the topics mentioned in this document turns to be different or updated or changed from Microsoft for Azure. Always refer to Microsoft website for the updated notes.

Intent

The only intention behind creating this document is to do a quick reference check related Azure Administrator topic. There is no intent or intention to make this document available for any commercial purposes. This document is openly available to use, share, distribute, and share.

Credits

Alan Rodrigues

Microsoft website

Contents

Azure Basics	4
Azure Dedicated Hosts.....	6
Azure Backup Service	7
Azure Redeploy	10
Availability Set.....	10
Update Domain	10
Fault Domain.....	10
Azure Virtual Machine Scale Set.....	11
Availability Zones.....	11
Virtual Machine Image	11
Proximity Placement Groups	12
Azure Web App.....	12
Containers	13
What is Kubernetes?	15
Azure Virtual Networks.....	19
Network Security Groups	20
Azure Resource Manager Templates	22
Azure Load Balancer.....	22
Virtual Network Peering	29
Point to Site VPN Connection	29
Point to Site VPN Connection – Lab/Simulation	31
Site to Site VPN Connection.....	33
Azure ExpressRoute.....	36
Azure Network Watcher	38
Traffic Analytics	40
Azure Network Performance Monitor.....	40
Azure Custom Routes	41
Azure Jump Server or Bastion Host.....	42
Azure Firewall.....	43
Azure DNS.....	45
Azure Storage Accounts	45
Azure – File Share	52
Azure Service Endpoint.....	53
Azure Private Endpoint.....	54

Azure Basics

Difference between Gen 1 vs Gen 2 Virtual Machine

<https://docs.microsoft.com/en-us/azure/virtual-machines/generation-2>

Temporary Disk

Do not store your important data on temporary disk, save it on a permanent drive, i.e., C:\ drive

Work on Azure resources through Commands

If you want to work with resources in Azure from the command line, there are two options:

Azure CLI

Azure CLI is meant only for Azure, it only works with Azure based services itself











Azure PowerShell

Azure PowerShell can be used for other products as well, like it can be used for Windows or for Linux

Azure Cloud Shell (CLI & PowerShell can be used on Cloud Shell)

Azure Cloud Shell is an interactive, authenticated, browser-accessible shell for managing Azure resources. It provides the flexibility of choosing the shell experience that best suits the way you work, either Bash or PowerShell

Custom Script Extensions for Windows

-  This extension is useful for post deployment configuration, software installation, or any other configuration or management tasks.
-  This tool can be used on Azure virtual machines to download and execute scripts
-  This is ideal when you want to deploy any custom configuration of any software installation on virtual machine
-  The scripts can be located in Azure storage account or even in GitHub
-  A time duration of 90 minutes is allowed for the script to run. Any longer and the result will be failed extension provision
-  It is ideal to not place reboots inside the scripts, because the script will not continue after the reboot
-  If your script does need a reboot, then maybe you can look at other tools such as Desired State config, Chef or puppet
-  The script only runs once
-  The custom script will run under the impersonation of the localsystem account
-  The storage account must be in the same location, as the virtual machine, like North-Europe or Central India, etc.

- + Upload the script in Containers under storage account, in this you have to create a container
- + Go to extensions in virtual machine, and select the storage > containers > and select the custom script
- + The same way scripts under extensions can be run on Linux machines too, for e.g., to install a rpm or package file

Cloud init file

- + Cloud init file only works for Linux virtual machine
- + This is another way in which you can actually pre-install the packages on a new Linux virtual machine
- + The config file for the installation of packages, the file format should be *.yaml
- + Under the *.yaml files, the script, or commands to execute any particular function would be inside the file
- + While creating new Linux virtual machine, in Advanced section, in it you have to select Extensions, and “select an extension to install” or you can choose “Cloud init” also to add your commands
- + Once the Linux virtual machine will be ready, the mentioned package in the “cloud init” will be pre-installed on the host

Boot Diagnostics

Boot diagnostics is a debugging feature for Azure virtual machines (VM) that allows diagnosis of VM boot failures. Boot diagnostics enables a user to observe the state of their VM as it is booting up by collecting serial log information and screenshots.

- + It is in virtual machine > Support + Troubleshooting > Boot Diagnostics
- + It takes the screenshot of the virtual machine at the time of booting and also captures the log files
- + You can select the boot diagnostics option while creating the virtual machine
- + Boot diagnostics options work for both Linux and Windows operating system
- + The data for the boot diagnostics stores in Azure storage account
- + You can choose managed storage account, or you can create your own storage account, to store log files

Serial Console

- + Pre-requisites

You should have your custom boot diagnostics storage account, NOT the managed storage account

Once the custom storage account gets setup, then you would be able to use serial console

- + Serial console can be used for sending commands onto your virtual machine

- ✚ It opens the SAC Console (Special Administrative Console)
- ✚ You have to change the channel to particular command prompt

Commands:

1. Cmd
2. ch -si 1
3. Login credentials
4. Now you get the access to virtual machine, by cmd
5. Now you can run commands

Run Command

Run Command can run a PowerShell or shell script within an Azure VM remotely by using the VM agent. This scenario is especially useful when you need to troubleshoot operating system network configurations or user access configuration.

You can run multiple commands under run command, for e.g., for installing IIS through PowerShell or disabling a particular group access or granting access.

There are many by default options you can get to choose to run commands, based on different-different actions.

Confidential Computing

- ✚ This is a feature that allows you to isolate sensitive data when it is being processed in the cloud.
- ✚ This feature is available for your virtual machines. In Confidential computing , a part of the CPU's hardware is reserved for the portion of code and data in your application. This portion is known as an enclave.
- ✚ There is a special series of virtual machines which support confidential computing. This is the DCsv2-Series.
- ✚ To actually ensure that your code or application runs inside the enclave, you will have to program it accordingly.

For this you need to use two open-source frameworks

a) Open Enclave Software Development Kit

<https://github.com/openenclave/openenclave>

b) Confidential Consortium Framework

<https://github.com/Microsoft/CCF>

Azure Dedicated Hosts

- ✚ This service provides physical servers to host virtual machines. The physical server is dedicated to the Azure subscription.

- ✚ The benefits of Azure Dedicated Hosts are that no other virtual machines from any other customers would be placed on the physical server.
- ✚ You can also control the maintenance events that are initiated on the Azure platform.
- ✚ Here the users are charged per dedicated host. This is irrespective of the number of virtual machines running on the physical server.

Azure Backup Service

- ✚ It is a service to take backup of your Azure virtual machines. You can restore the virtual machine using the Azure backup service.
- ✚ There are recovery points being created every time the backup happens, like today recovery point, tmrw recovery point, last week recovery point, etc.
- ✚ When you choose recovery point, you can decide what kind of data you want to recover, like:
 - Individual Files – you can choose particular files which you want to recover
 - VM Recovery – you can recover whole VM and create a duplicate VM
 - Disk Recovery – you can recover a whole disk and save it separately
- ✚ When you are recovering data, at no point in time you are actually connected to the virtual machine, whose data got backed up. The VM will be running separately without any impact on it.
- ✚ At the time of creation of virtual machine, you can select if you want to enable backup for the virtual machine and select and configure the backup policy as well
- ✚ There are two major separate services which are a part of Azure Backup service:
 - Azure Recovery Services Vault
 - Backup Policy

Note: When you take backup, the backup data is being stored in “Azure Recovery Services Vault”. It is a separate resource in Azure.

a. Azure Recovery Services Vault

- The “Azure Recovery Services Vault” should be in the same region as the Azure virtual machine
- During the first backup, all the data from the underlying disk will be taken as backup onto “Recovery Services Vault”
- The next backup will be subsequent in nature, and only the changes or new data will be backed up

b. Backup Policy

- Backup policy is to configure to schedule the backup process
- You can mention the retention period of the backup data as well

Few more important points:

- ✚ During the first backup, an extension gets installed on the virtual machine

- ✚ The type of extension depends upon the type of virtual machine operating system, like for Windows or for Linux
- ✚ This extension is used to take a snapshot of the disk attached to the virtual machine
- ✚ For Windows based VM's, the backup service works with the "Windows Volume Shadow Copy Service" that can be used to take an application consistent snapshot of the virtual machine
- ✚ For Linux based VM's, the service takes a file-consistent backup

Types of Snapshots are:

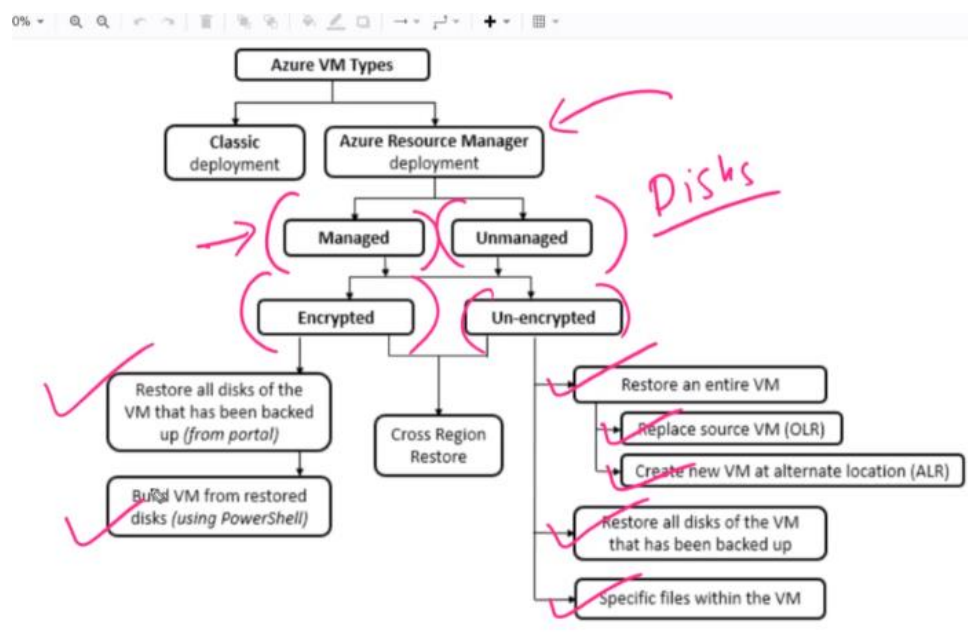
- ✚ Application Consistent
 - It captures the memory content, pending I/O operations
 - It ensures that whatever is the state of the application at that point in time when the backup is being taken is consistent when a restore is taken from the particular backup
- ✚ File System Consistent
 - It takes a snapshot of all the files at the same time
- ✚ Crash Consistent
 - This happens when the virtual machine shuts down at the time of backup process

Instant Recovery Feature

Snapshots taken as a part of the backup job are stored along with the disk and are available for recovery instantly. Once the snapshot phase is done, users can go ahead and use the local snapshot to restore if the patch goes bad.

The instant recovery feature basically goes out and takes a snapshot of the VM itself and stores it locally within the virtual machine itself.

Restore Options



Restore individual files:

- + The particular drive gets created on your local machine, and from that you can take the files.
- + The *.exe file will be created, which will run on PowerShell on local system to make new drives on your host from the restore point
- + Once the activity done, you can unmount those drive on the Azure portal itself

Soft Delete

- + Soft delete protects backup data from accidental deletes
- + Soft delete is a feature which keeps your backup files for 14 days.
- + Even if you stop the backup of a VM, still the backup of a particular VM would be available for 14 days in the recovery services vault
- + Soft delete option has to be disabled to delete the saved backups in the recovery services vault

Steps:

1. Stop the backup of the VM
2. Go to > Recovery Services Vault > Properties > Security Settings > Soft Delete > disable soft delete
3. Even if you stop and delete the backup data, you still won't be able to delete the recovery services vault for 14 days
4. Then delete the backup of all the VM's
5. Then delete the recovery services vault, without disable of soft delete, you wouldn't had been able to delete the recovery services vault.

MARS Agent / Azure Backup Agent / Azure Recovery Services Agent

- + This agent helps you to take backup of particular services/files/folders of on-premises host as well.
- + You have to register your on-prem machine with Azure Recovery Services vault by using a MARS agent.
- + You can also use the 1st on-prem machine backup and restore it onto 2nd on-prem/VM machine as well.

Azure to Azure Site Recovery

- + This service recovers every resource which you choose to a new Azure location, in case of a primary site goes down.
- + This requires a Cache storage for keeping all the recovery in it, and once you do a failover, then everything will be copied from Cache storage, and will be restored to a new Azure site.

Azure Redeploy

When you redeploy a VM, it moves the VM to a new node within the Azure infrastructure and then powers it back on. All your configuration options and associated resources are retained. After you redeploy a VM, the temporary disk is lost, and dynamic IP addresses associated with virtual network interface are updated.

Availability Set

An availability set is a logical grouping of VMs that allows Azure to understand how your application is built to provide for redundancy and availability. We recommended that two or more VMs are created within an availability set to provide for a highly available application and to meet the 99.95% Azure SLA.

Availability Set

- ✚ Availability Sets ensure that the Azure virtual machines are deployed across multiple isolated hardware nodes in a cluster.
- ✚ By deploying your vms across multiple hardware nodes Azure ensures that if hardware or software failure happens within Azure, only a sub-set of your virtual machines are impacted, and your overall solution is safe and in working condition.
- ✚ Availability set provides redundancy for your virtual machines.
- ✚ Availability set spreads your virtual machines across multiple fault domains and update domains.
- ✚ If you want to leverage Microsoft's 99.95% SLA from Microsoft, you must place your VMs inside availability set except your VMs are having premium storage.

Update Domain

- ✚ An update domain is a group of resources that can be updated and rebooted if required at the same time.
- ✚ Virtual machines get update domains automatically once they are put inside availability set.
- ✚ All virtual machines within that update domain will reboot together.
- ✚ Update domains are used for patching of the virtual machines.
- ✚ Only one update domain would be updated at the time

Fault Domain

- ✚ Fault domains define the group of virtual machines that share a common power source and network switch.
- ✚ Each and every fault domain contains some racks, and each rack contains virtual machine.
- ✚ Each of these Fault domain shares a power supply and a network switch.
- ✚ If there is a failure in the fault domain then all the resources in the fault domain become unavailable.

- ✚ You should place your vms such a way that each fault domain gets one web server, one database server and like that.

Azure Virtual Machine Scale Set

Azure virtual machine scale sets let you create and manage a group of loads balanced VMs. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs.

With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.

- ✚ This service allows you to create and manage a group of identical virtual machines
- ✚ You can place the scale set behind the load balancer to distribute the traffic
- ✚ The virtual machines instances automatically increase, or decreases based on the demand of the virtual machine scale set
- ✚ The scale sets help provide better redundancy and improved performance of your applications

Availability Zones

Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking.

- ✚ Using Availability Zones, you can be guaranteed an availability of 99.99% for your virtual machines. You need to ensure that you have 2 or more virtual machines running across multiple availability zones.
- ✚ These features help provides better availability for your application by protecting them from datacenter failures.
- ✚ Each Availability zone is a unique physical location in an Azure region.
- ✚ Each zone comprises of one or more data centers that has independent power, cooling, and networking
- ✚ Hence the physical separation of the Availability Zones helps protect applications against data center failures

Virtual Machine Image

It captures the disk properties (such as host caching) you need in order to deploy a VM in a reusable unit. Similar to OS Images, a VM Image is a collection of metadata and pointers to a set of VHDs (one VHD per disk) stored as page blobs in Azure Storage.

- ✚ This helps you to create an image of a virtual machine, which later can be used to create new virtual machines
- ✚ The virtual machine from which the image has been created, cannot be used and has to be stopped.

Proximity Placement Groups

A proximity placement group is a logical grouping used to make sure that Azure compute resources are physically located close to each other. Proximity placement groups are useful for workloads where low latency is a requirement. Proximity placement groups cannot be used with dedicated hosts.

- ✚ If you want to ensure that the virtual machine is placed closer to each other in the same data center, then make ensure the virtual machines are all part of the same proximity group
- ✚ Placing the virtual machines as a part of a proximity group, the virtual machines will be physically located closed to each other
- ✚ While using proximity placement groups, ensure the virtual machine have accelerated networking enabled. This improves the network performance

Azure Web App

Azure Web Apps is a cloud computing-based platform for hosting websites, created and operated by Microsoft. It is a platform as a service which allows publishing Web apps running on multiple frameworks and written in different programming languages.

- ✚ You can deploy your applications on the Azure Web App, without manually installing a virtual machine.
- ✚ All the infrastructure related requirements would automatically be created when you deploy your application on Azure Web App
- ✚ Azure web app is a part of your App Service Plan and app service plan hosts your application on an underlying instance or a virtual machine
- ✚ When you create a web app in Azure, you also need to create a “App Service Plan”
- ✚ The web app needs to be linked to “App Service Plan”

App Service Plan

An App Service plan defines a set of compute resources for a web app to run. These compute resources are analogous to the server farm in conventional web hosting. One or more apps can be configured to run on the same computing resources (or in the same App Service plan).

Deployment Slots

Deployment slots allow your function app to run different instances called "slots". Slots are different environments exposed via a publicly available endpoint. One app instance is always mapped to the production slot, and you can swap instances assigned to a slot on demand.

This only works with Standard or higher app service plan only, NOT with free tier.

- You can actually go ahead and publish different versions of your applications onto the same Azure web app.

Auto-Scaling Web Apps

If you have standard or higher app service plan, you get a feature known as auto-scaling, which can add more compute instances to the running application, if the load gets higher.

NOTE: Your app service plan is what is responsible for creating the underlying compute infrastructure

But it is not necessary that you only have to base your scaling based on the metrics of the app service plan

Cool Down

Let's say that the rule has been triggered and now based on the load, it goes ahead and adds another machine. But obviously it will take time for the load to be distributed across the 2 machines, and that period is called cool down period.

During this time the scaling process should not take into account any metrics or thresholds that get breached or reaches its limit, because during the cool down period you are actually allowing the load to be distributed across both the old and new virtual machine

Integration of Azure Web App with Azure Virtual Network

You have to first create a new virtual network, and then add that virtual network into web app, under networking option

Azure Web App – Backup

- Backup feature is available with Azure Web App can be used to create backups of your web app
- The backups are stored in an Azure storage account, backup of the app + database can be up to maximum of 10 GB
- Here the App configuration, the file content and the database connected to the application get backed up
- The app service plan needs to be in Standard or Premium tier to avail the backup & restore feature

Containers

How do containers run on a virtual machine?

You have to install container tool set to run on the virtual machine, the most popular tool set is: Docker. Then the docker engine is then responsible for running your containers on the virtual machine.

How to run & install containers (Docker) on a Linux VM?

1. Update the package index
sudo apt-get update

2. Install packages to allow apt to use the repository over HTTPS
`sudo apt install apt-transport-https ca-certificates curl software-properties-common`
3. Add Docker's official GPG key
`curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -`
4. Setup a stable repository
`sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu bionic stable"`
5. Update the package index
`sudo apt-get update`
6. Install docker, containerd
`sudo apt-get install docker-ce`
7. Pull the nginx image
`sudo docker pull nginx:1.17.0`
8. Create a container out of the image
`sudo docker run --name sampleapp -p 80:80 -d nginx:1.17.0`

Container Instances

Azure Container Instances is a service that enables a developer to deploy containers on the Microsoft Azure public cloud without having to provision or manage any underlying infrastructure. ACI reduces management overhead, so a developer can deploy a container on Azure within seconds.

This service is automatically going to ensure that a virtual machine is in place. That virtual machine will have the docker engine installed and it can go out and create or run containers.

There are three sources to pull the images, from where you can select the docker image

- Quickstart images
- Azure Container Registry
- Docker Hub or other registry

Container Groups

- This is nothing but a collection of containers
- These containers get scheduled on the same host machine
- They share the same lifecycle, resources, local network, and storage volumes
- The deployment can be done via Resource Manager template or a YAML file

- These container groups can also go out and use Azure file share when it comes to the storage of the underlying data for the container itself. So, the container wants to go out and actually mount volumes for storage.

What is Kubernetes?

Kubernetes is a portable, extensible, open-source platform for managing containerized workloads and services, that facilitates both declarative configuration and automation. It has a large, rapidly growing ecosystem. Kubernetes services, support, and tools are widely available.

- + Kubernetes is able to provide a DNS name to your container
- + Kubernetes can load balance and distribute network traffic, if there is a high load on your container
- + Kubernetes can also restart containers that fail
- + It can be used to replace or kill containers
- + It also helps to store and manage sensitive information such as passwords, OAuth tokens, and SSH keys

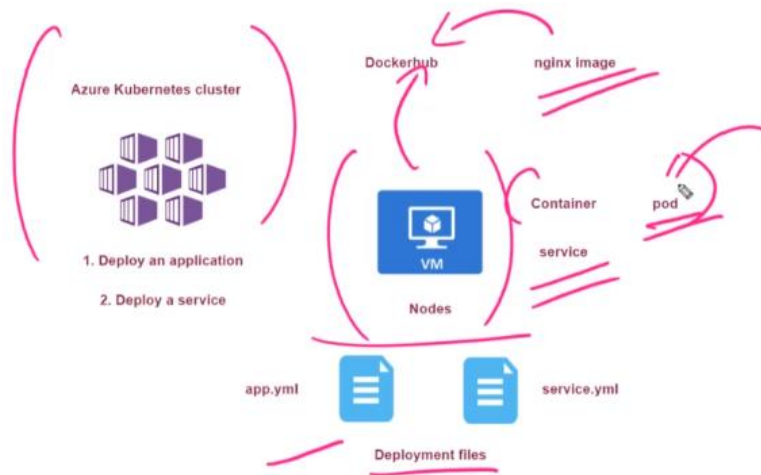
Azure Kubernetes

Deploy and manage containerized applications more easily with a fully managed Kubernetes service. Azure Kubernetes Service (AKS) offers serverless Kubernetes, an integrated continuous integration and continuous delivery (CI/CD) experience and enterprise-grade security and governance. Unite your development and operations teams on a single platform to rapidly build, deliver and scale applications with confidence.

- Fully managed Kubernetes service on Azure
- Makes it easy to deploy and manage containerized applications
- It helps to remove the burden of managing the underlying infrastructure for the Kubernetes deployment

You can deploy a simple container onto the cluster by app.yaml file. The deployment file is going to go ahead and deploy a pod onto a cluster, that is basically a container. It's used for deploying the pods or containers.

So, the service.yaml file will go out and use a load balancer and it allows to go ahead and actually access that nginx container via a public IP address. It is used for deploying the services.



Deploying Azure Kubernetes - via Azure Cloud Shell

1. Create a new resource group
`az group create --name kubernetes --location eastus`
2. Create a new Kubernetes cluster
`az aks create --resource-group kubernetes --name companycluster --node-count 1 --enable-addons monitoring --generate-ssh-keys`
3. Get the credentials of the cluster
`az aks get-credentials --resource-group kubernetes --name companycluster`
4. Get the nodes running in the cluster
`kubectl get nodes`
5. Apply the application configuration file
`kubectl apply -f app.yml`
6. Apply the service configuration file
`kubectl apply -f service.yml`
7. Get the list of services running in Kubernetes
`kubectl get services`

Kubernetes Networking

In Azure Kubernetes when you go ahead and deploy your containers so they are deployed onto individual pods, and these pods would reside on the nodes, so the nodes basically are your compute infrastructure that is required for hosting the pods, which in turns holds your containers.

Now when it comes to the IP addresses that can be assigned onto the pods, so there are two ways that can be achieved.



Pods receive an IP address from a logically different address space to the Azure virtual network subnet

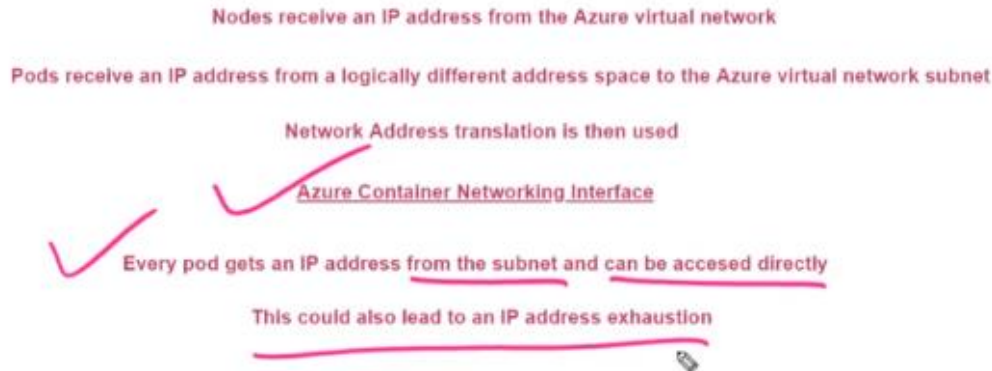
Network Address translation is then used

Azure Container Networking Interface

When you use Kubenet:

- ## 2. Azure Container Network Interface

- Every pod gets an IP address from the subnet directly and can be accessed directly as well, but this could go and lead onto IP address exhaustion, so the IP addresses in your subnet may not be enough to go out and cover all the pods on the different nodes



[Dashboard](#) > [All resources](#) > [New](#) > [Kubernetes Service](#) >

Create Kubernetes cluster ...

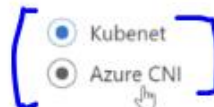
Basics Node pools Authentication **Networking** Integrations Tags Review + create

You can change networking settings for your cluster, including enabling HTTP application routing and configuring your network using either the 'Kubenet' or 'Azure CNI' options:

- The **kubenet** networking plug-in creates a new VNet for your cluster using default values.
- The **Azure CNI** networking plug-in allows clusters to use a new or existing VNet with customizable addresses. Application pods are connected directly to the VNet, which allows for native integration with VNet features.

[Learn more about networking in Azure Kubernetes Service](#)

Network configuration ⓘ



DNS name prefix * ⓘ

democluster-dns ✓

Azure Kubernetes Storage

When you deploy your Kubernetes cluster, make sure that it is not a part of any availability zone.

1. Azure Disks

Use Azure Disks to create a Kubernetes DataDisk resource. Disks can use:

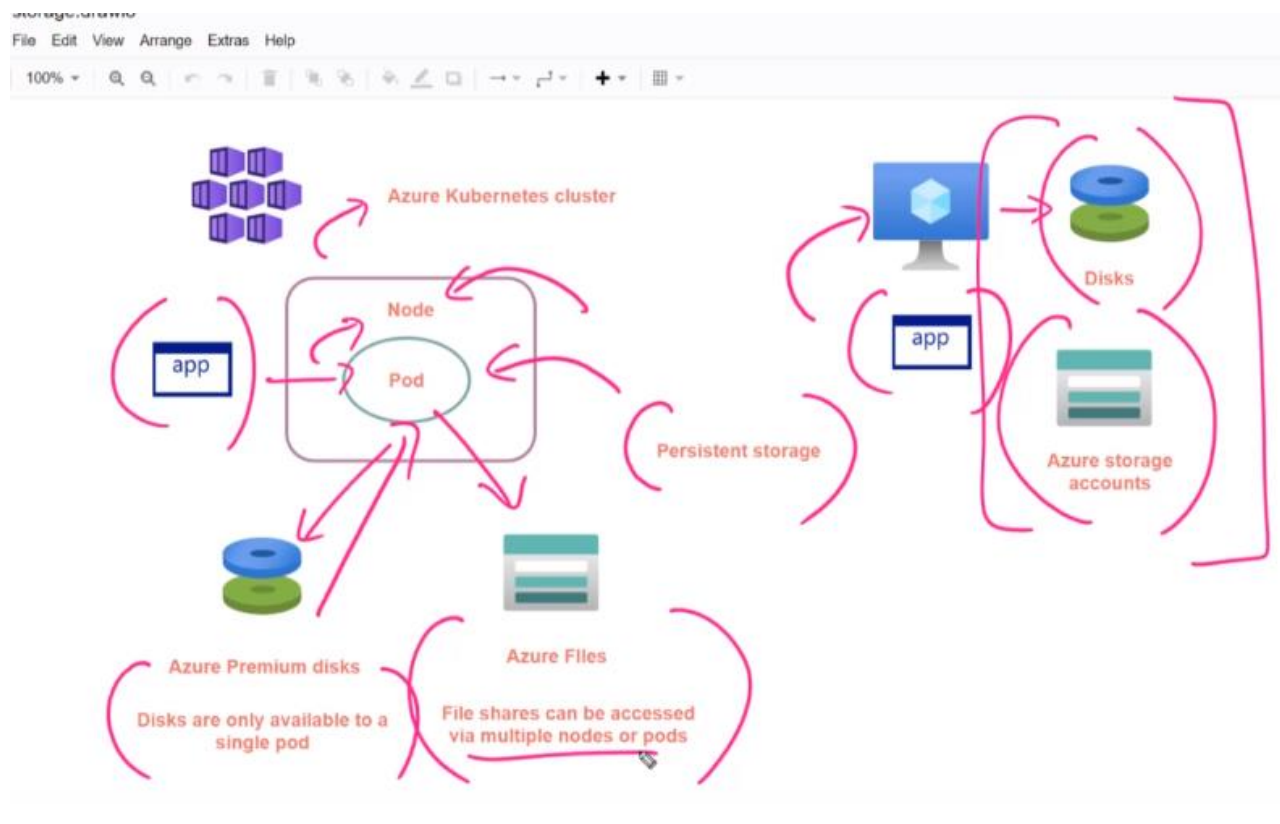
- Azure Premium storage, backed by high-performance SSDs, or
- Azure Standard storage, backed by regular HDDs.

2. Azure Files

Use Azure Files to mount an SMB 3.0 share backed by an Azure Storage account to pods.

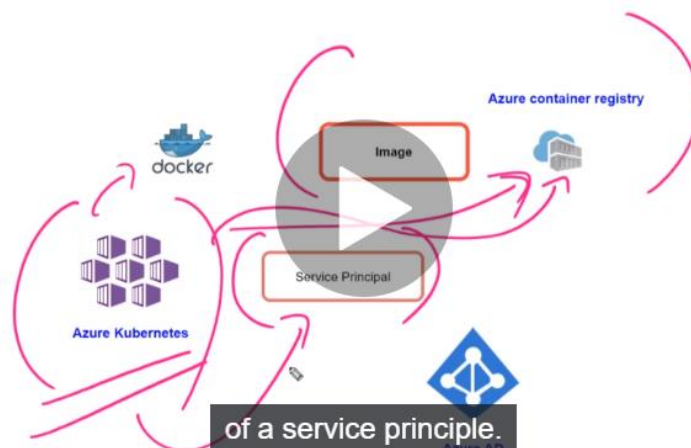
Files let you share data across multiple nodes and pods and can use:

- Azure Premium storage, backed by high-performance SSDs, or
- Azure Standard storage backed by regular HDDs.



Azure Container Registry

Azure Container registry allows you to build, store, and manage container images and artifacts in a private registry for all types of container deployments

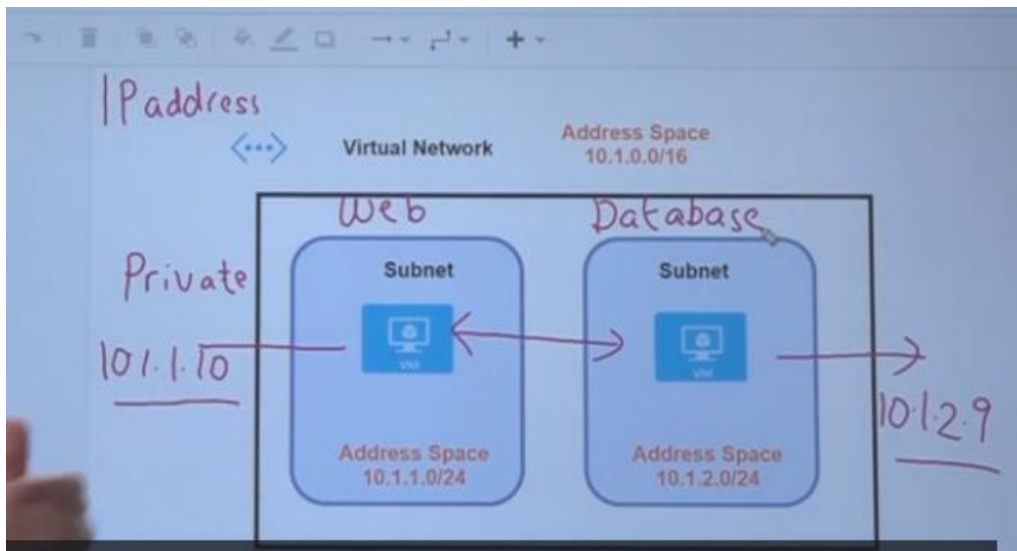


Azure Virtual Networks

An Azure Virtual Network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription. When you create a VNet, your services and VMs within your VNet can communicate directly and securely with each other in the cloud.

Azure Virtual Network gives you an isolated and highly secure environment to run your virtual machines and applications. Use your private IP addresses and define subnets, access control

policies and more. Use Virtual Network to treat Azure in the same way as you would treat your own datacenter.



Notes:

- ✚ Azure virtual network allows resources such as Azure virtual machines to securely communicate with each other
- ✚ You define subnets in an Azure virtual network. This helps segment the network into one or more sub-networks
- ✚ A virtual network is scoped to a single region
- ✚ Public IP address – This is used for communications with the internet
- ✚ Private IP address – This is used for communications within an Azure virtual network or with an on-premises network

Public IP Address few points:

- ✚ There are 2 SKU's when it comes to public IP address
- ✚ Basic SKU – Here you can assign either a static or dynamic IP address
- ✚ Network security groups can optionally be used to restricting traffic via the public IP address
- ✚ There is no support for availability zones
- ✚ Standard SKU – Here the IP address needs to be static IP address
- ✚ Network security groups need to be used to restrict traffic
- ✚ They are zone redundant by default

If you want to keep your public IP address unchanged even after restart or stopping your virtual machine, mark the IP address as static.

Network Security Groups

Network security groups are used to control the flow of traffic into and out of your virtual machine. So, it is kind of a firewall that presents for the traffic that enters or goes out of your virtual machine

- + Network security group is a separate resource that is defined on Azure platform and NSG gets attached to the network interface that is attached to your virtual machine
- + NSG can be attached either to the network interface or it could be linked to the entire subnet. So, if it will be linked to the entire subnet it will affect all of the virtual machines which are a part of that subnet
- + NSG consists of inbound and outbound security rules
- + Inbound security rule is used to control the flow of traffic that flows into the virtual machine
- + Outbound security rule is used to control the flow of traffic that flows out of the virtual machine

Imp. : There are some default rules which are already in place.

- + So, when a NSG is created for you, there are some default rules. You can remove these rules or changes these rules
- + One of the rules is to allow traffic within the virtual network itself, so, if you have multiple virtual machines then the NSG would automatically allow the traffic between these virtual machines
- + NSG can be applied for a particular VM also or for against a subnet also, so this way any machine under the same subnet will follow the NSG rules only
- + If you have the NSG at the subnet level, then first the rules on the NSG at the subnet level will be evaluated first
- + Then NSG follows the VM NSG rules
- + If the port 80 is not mentioned in the NSG which is assigned to subnet level, then it is deny, so in this case the request won't go to NSG at the VM level to cross check
- + If you don't have the network security group attached onto a network interface, then any traffic or communication is by default ON
- + If you want to specify the IP address of a VM to access on NSG to be allowed, then you have to add private IP address of the VM in NSG to be allowed, where the network address translation happens, and you can still be able to access the VM by public IP address

By default, rules which are enabled on an NSG:

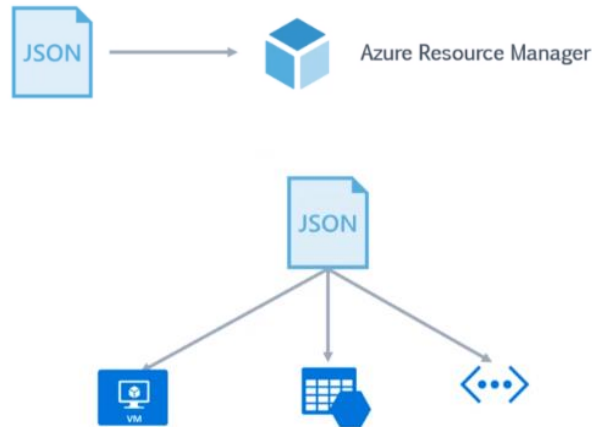
1. First rule is to go ahead and allow all traffic within a virtual network. All virtual machines communicate with each other
2. If Azure VM is placed behind Azure Load Balancer, by default all traffic will be allowed from the load balancer onto the VM itself
3. Third rule, is to deny all other types of traffic



Azure Resource Manager Templates

1. This provides the ability to define your infrastructure-as-a-code (IaC)
2. You create templates using JSON (JavaScript Object Notation)
3. This defines the infrastructure and configuration of the resources that need to deploy

Your JSON file, which is your ARM template, you can then submit it then to the Azure resource manager. That JSON file could be used to create various number of resources.



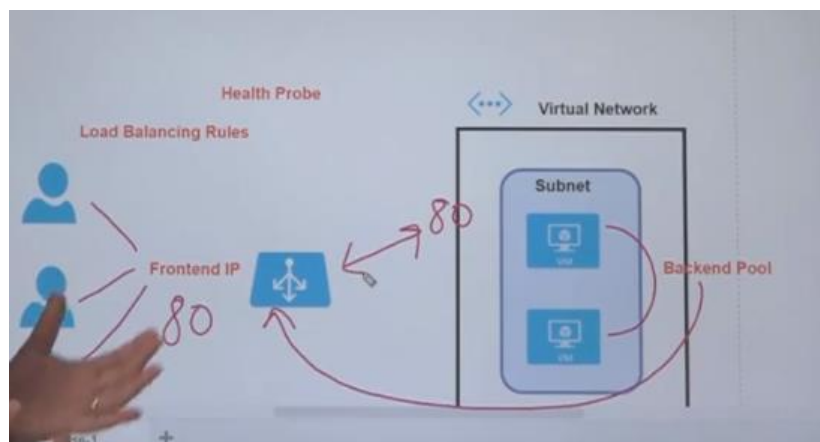
There are different sections of the template:

1. Resources – This is used to specify the resources which needs to be deployed
2. Variables – These are values that can be reused in the template
3. Parameters – This can be used to provide values during the deployment phase
4. Outputs – This returns values from the deployed resources

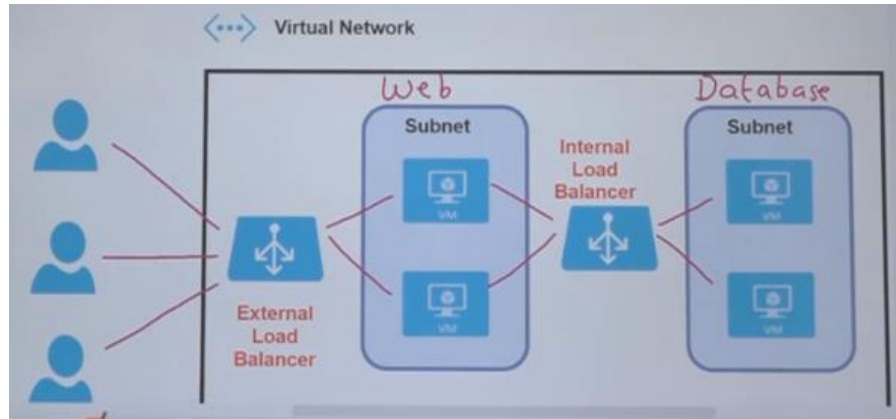
Azure Load Balancer

An Azure load balancer is a Layer-4 (TCP, UDP) load balancer that provides high availability by distributing incoming traffic among healthy VMs. To distribute traffic to the VMs, a back-end address pool contains the IP addresses of the virtual (NICs) connected to the load balancer.

The load balancer is used to distribute the incoming traffic to the pool of virtual machines. It stops routing the traffic to a failed virtual machine in the pool. In this way, we can make our application resilient to any software or hardware failures in that pool of virtual machines.



Difference between External and Internal load balancer



Types of Azure Load Balancer:

There are three load balancers in Azure:

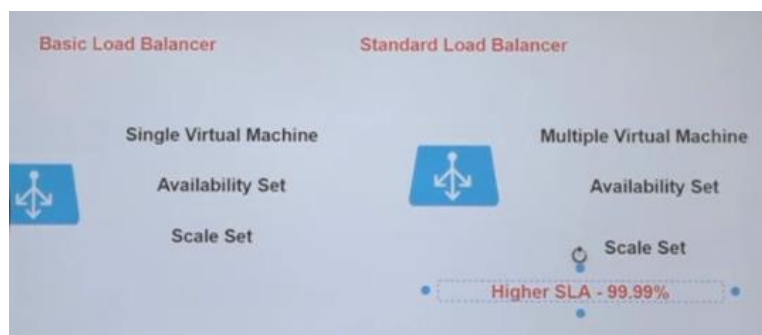
1. Azure Load Balancer
2. Internal Load Balancer (ILB)
3. Traffic Manager

Azure Load Balancer's Offerings:

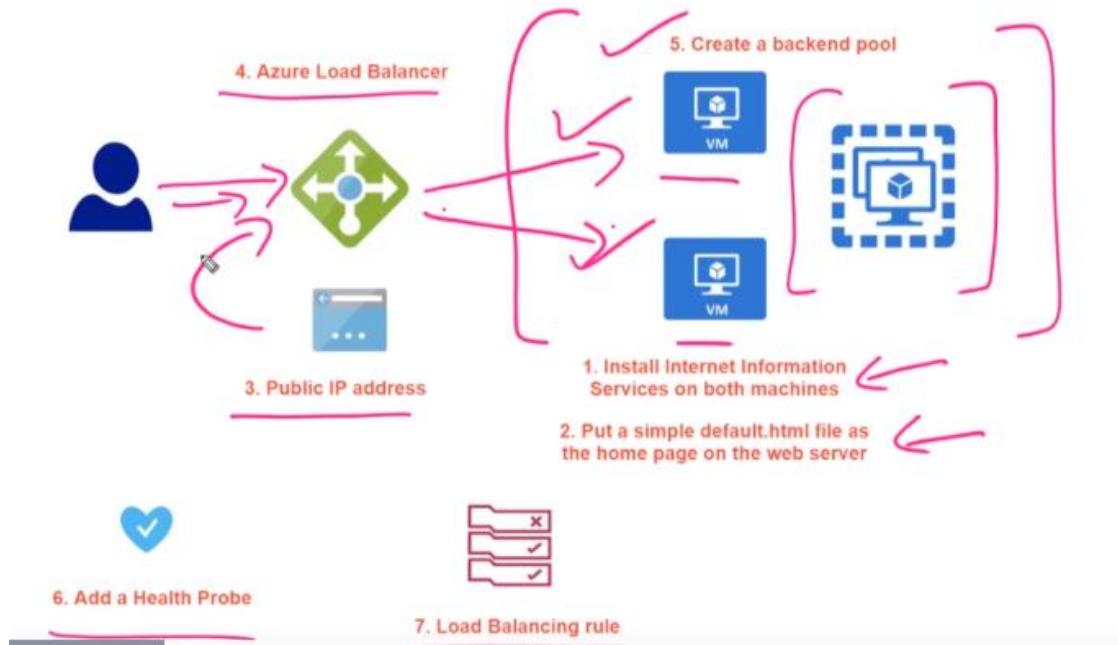
1. Basic Load Balancer
2. Standard Load Balancer

Basic Load Balancer – If you have multiple VM's they have to be a part of either an Availability Set or to be a part of virtual machine scale set

Standard Load Balancer – You can have two independent virtual machines which are neither part of an availability set or not even part of a scale set



1. Basic – Azure Load Balancer Setup

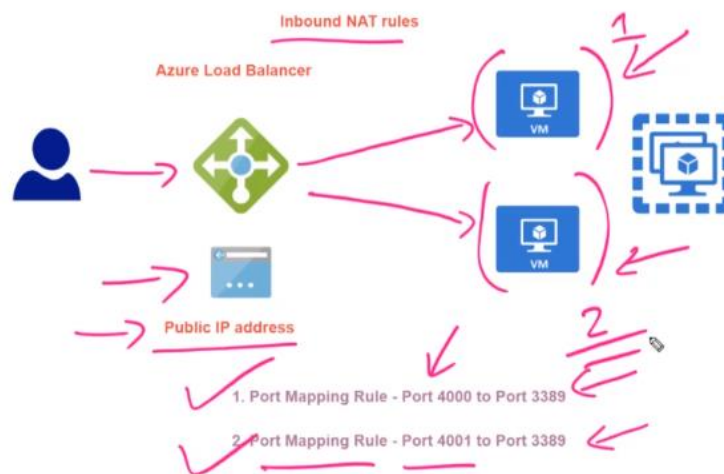


Disassociate or Remove Public IP Address from a Virtual Machine

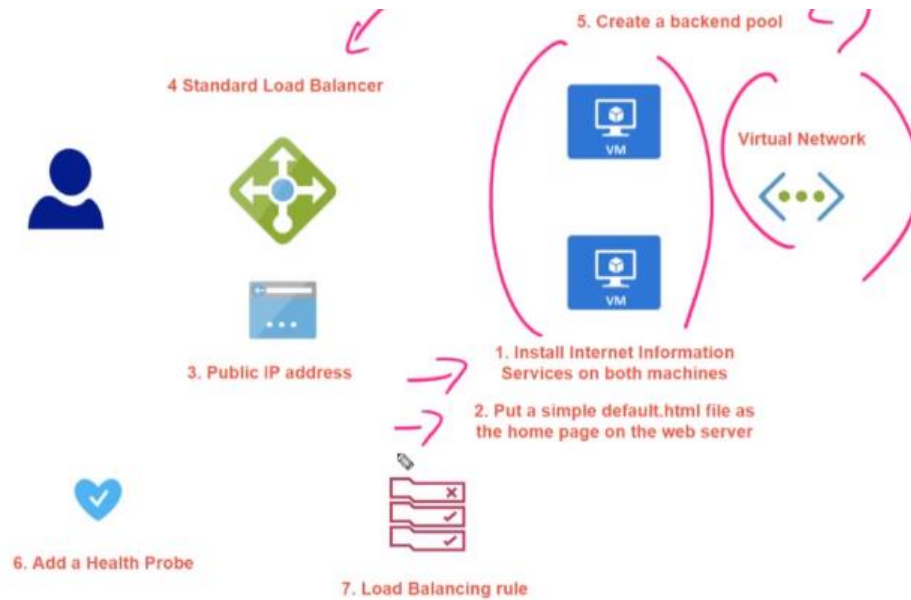
1. Go to virtual machine > Networking
2. Go to Network Interface > IP Configurations
3. IP Config > Disassociate public IP address

Inbound NAT Rules

Inbound NAT rules are an optional setting in the Azure load balancer. These rules essentially create another port mapping from frontend to backend, forwarding traffic over a specific port on the frontend to a specific port in the backend.



2. Standard – Azure Load Balancer Setup



Load Balancing Rule

A load balancing rule distributes incoming traffic that is sent to a selected IP address and port combination across a backend pool combination. Only backend instances that the health probe considers healthy receive new traffic.

Inbound NAT Rules

Inbound NAT rules are an optional setting in the Azure load balancer. These rules essentially create another port mapping from frontend to backend, forwarding traffic over a specific port on the frontend to a specific port in the backend.

Source Network Address Translation (SNAT)

The frontend IPs of an Azure public Load Balancer can be used to provide outbound connectivity to the internet for backend instances. This configuration uses source network address translation (SNAT) as the source or virtual machine's IP is translated to a Public IP address. SNAT maps the IP address of the backend to the public IP address of your load balancer. This prevents outside sources from having a direct address to the backend instances.

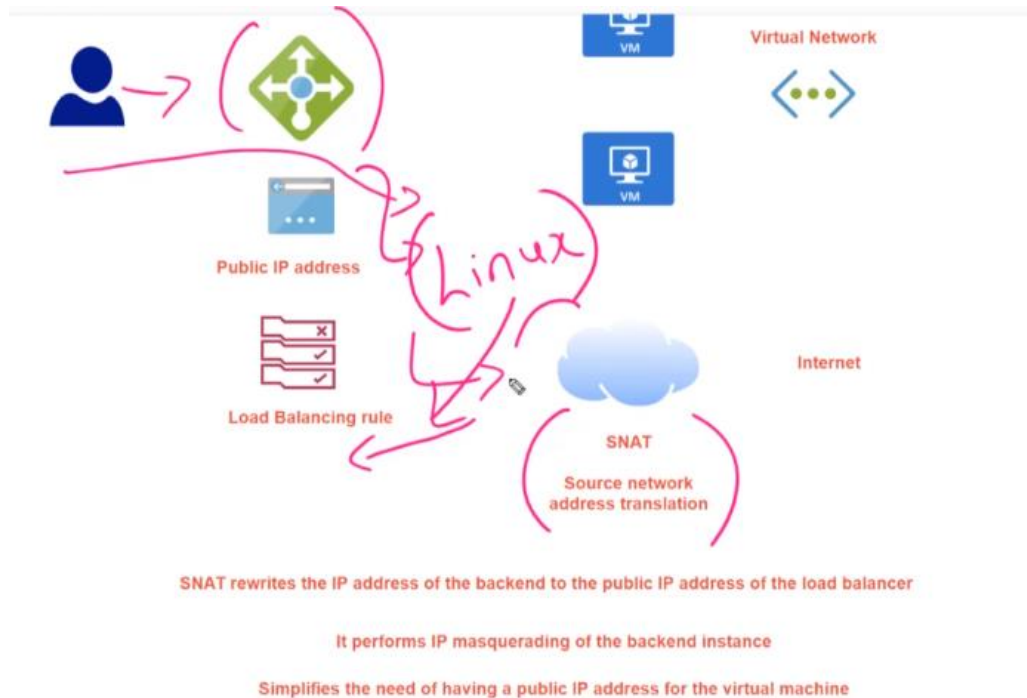
Outbound rules enable you to explicitly define SNAT (source network address translation) for a Standard public load balancer. This configuration allows you to use the public IP(s) of your load balancer to provide outbound internet connectivity for your backend instances.

This configuration enables:

- IP masquerading
- Simplifying your allowlists.
- Reduces the number of public IP resources for deployment

With outbound rules, you have full declarative control over outbound internet connectivity. Outbound rules allow you to scale and tune this ability to your specific needs.

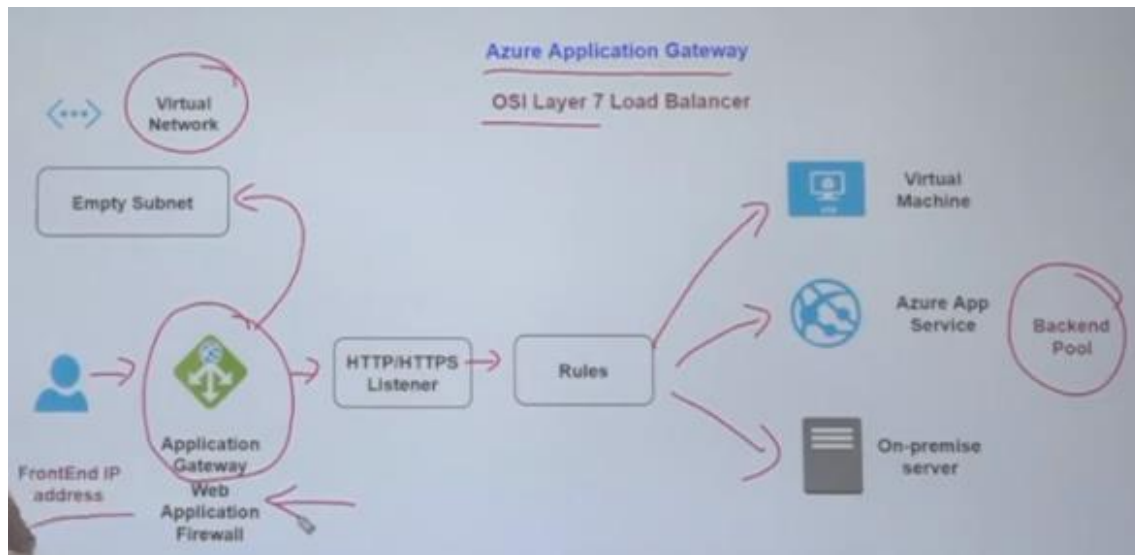
So if you want to go and have specific rules in place just for allowing outbound traffic from your backend VM's, that are part of the load balancer backend pool, you can go ahead and define your outbound rules.



Azure Application Gateway

1. This service is web traffic load balancer that is used to distribute traffic to web applications
2. The web application can reside on virtual machines, virtual machine scale sets or even on on-premises servers
3. The application gateway is an OSI Layer 7 load balancer
4. It provides Secure Sockets Layer (SSL) termination
5. Here request for the Application Gateway can be secured, and then the requests to the backend pool resources can be go unencrypted
6. This can lift the burden of the backend pool for decrypting traffic
7. The decryption of the requests can be left to the Application Gateway resource
8. You can enable auto-scaling for your application gateway resource
9. This allows the application gateway to scale up or down based on traffic load patterns
10. You can also enable the Web Application Firewall for the Application Gateway resource
11. You can also enable session affinity which allows a user session to directed to the same server for processing. If the state of the user session is stored on the server, then this can be a useful feature

When you are deploying an Application Gateway, it is important to have an empty subnet as a part of your virtual network

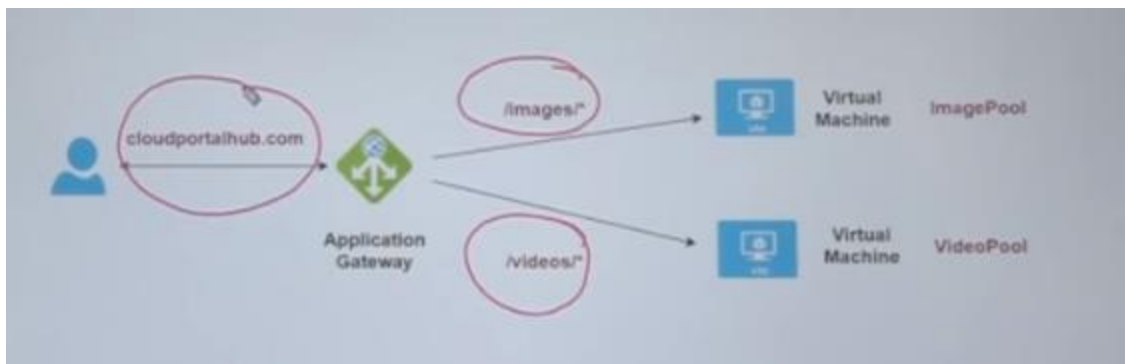


Components of the Application Gateway

1. **Frontend IP address** – Users will hit the Application Gateway via the frontend IP address
2. **Listener** – This is a logical entity that checks for incoming connection requests. There can be multiple listeners attached to an application gateway
Two types of listeners configurations:
 - **Basic** – Here the listener listens to single domain site
 - **Multi-site** – Here the listeners maps to multiple domain sites
3. **Routing Rules** – This is used to route the traffic from the listener to the backend pool
Two types of routing rules:
 - **Basic** – Here all requests are routed to backend pool directly
 - **Path-based** – Here are requests are routed to the backend pool based on the URL in request
4. **Backend Pools** – These can be network interfaces cards, virtual machine scale sets, Public or internal IP addresses, FQDN or backends such as App service
5. **Health Probes** – This defines how the application gateway will monitor the health of the resources in the backend pool

Application Gateway has an ability to route traffic based on what is the URL of the request itself. You can actually look at the request itself and direct the traffic based on the application type of request, as Application Gateway is a Layer 7, i.e., Application Layer service.

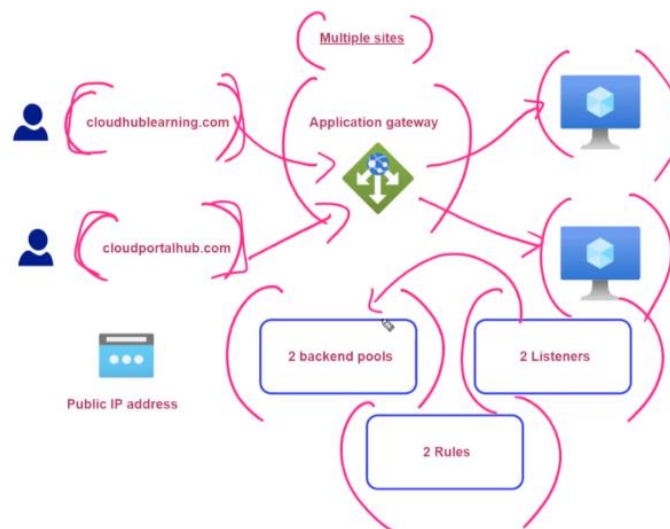
Because the application gateway works at a application layer it has this added advantage of routing requests based on the URL.



Difference between Azure Load Balancer Vs. Application Gateway

- Azure Load Balancer is used to load balance your traffic at layer Four (Transport Layer)
- Azure Application Gateway is used to load balance your traffic at layer Seven (Application Layer)

Azure Application Gateway – Multiple Sites



Important Note:

In virtual network we have to keep one empty subnet in place, that is an application subnet.

Application gateway service, it will go and create that compute infrastructure in that application subnet and that compute infrastructure will be responsible for routing the traffic onto virtual machines.

Application Gateway – Auto Scale

The compute infrastructure that is going to be created by the application gateway also has this feature of auto-scaling, because if the number of users requests which are hitting the application gateway increases then the compute resources of the application gateway has to be increased to manage the load, NOTE: this auto scale is not for the backend pool resources

Virtual Network Peering

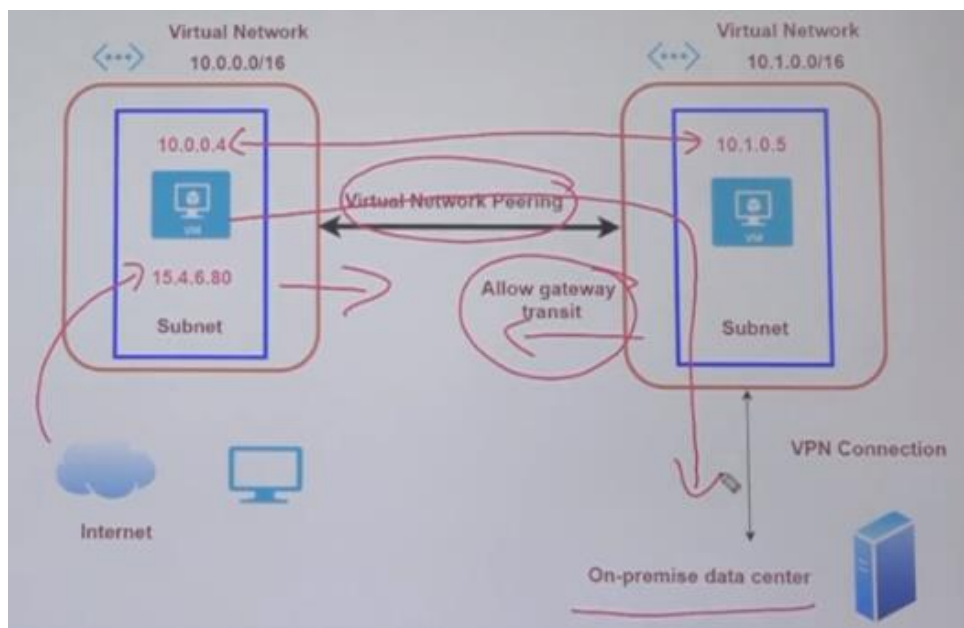
VNet Peering allows two VNets in the same region to connect with each other without having to set up the VPN Gateways.

Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure. The virtual networks appear as one for connectivity purposes. 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.

- Virtual Network Peering is used to connect two Azure virtual networks together via backbone network
- Azure supports connecting two virtual networks located in the same region or networks located across regions
- Once you enable virtual network peering between two virtual networks, virtual machine can then communicate via their IP addresses across the peering connection
- You can also peer virtual networks that are located across different subscriptions
- The virtual networks cannot have overlapping CIDR blocks

Azure supports the following types of peering:

- **Virtual network peering:** Connect virtual networks within the same Azure region
- **Global virtual network peering:** Connecting virtual networks across Azure regions



Point to Site VPN Connection

Let's say that if you want a client machine or workstation in your on-premises environment to go ahead and access the virtual machine via its private IP address, NOT public IP address

If you want a secure connection over the internet between your on-premises workstation and a virtual machine over a private IP address, then you need to establish a **virtual private network connection**

So, what it goes into establishing a point to site VPN connection

On Azure Side

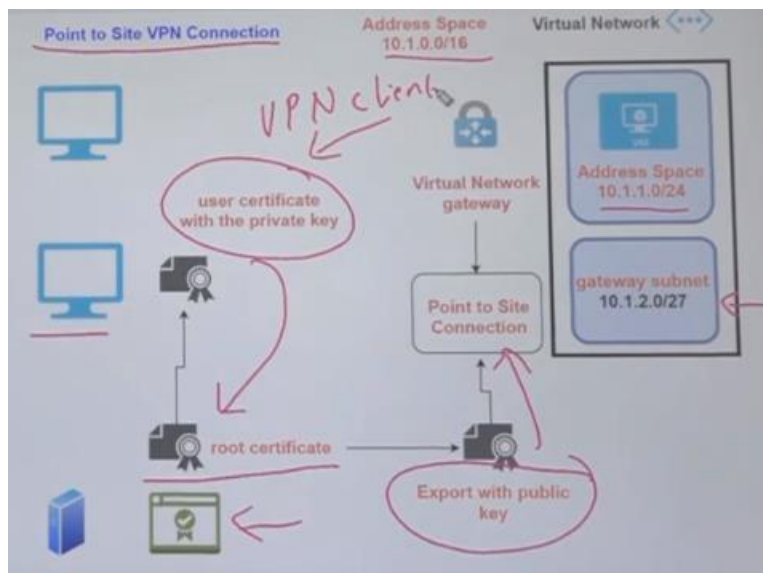
1. As part of your virtual network, you have to create a “Gateway Subnet”. This Gateway Subnet will be used as a gateway between your workstation and a virtual network
2. Once the “Gateway Subnet” is created, you have to create “Virtual Network Gateway”, it is a separate resource available in Azure
3. You can only create the Virtual Network Gateway and attach it your virtual network, if you have the gateway subnet in place
4. Once the “Virtual Network Gateway” is ready then you can go ahead and configure a **Point to Site VPN connection**

On workstation/on-premises Side

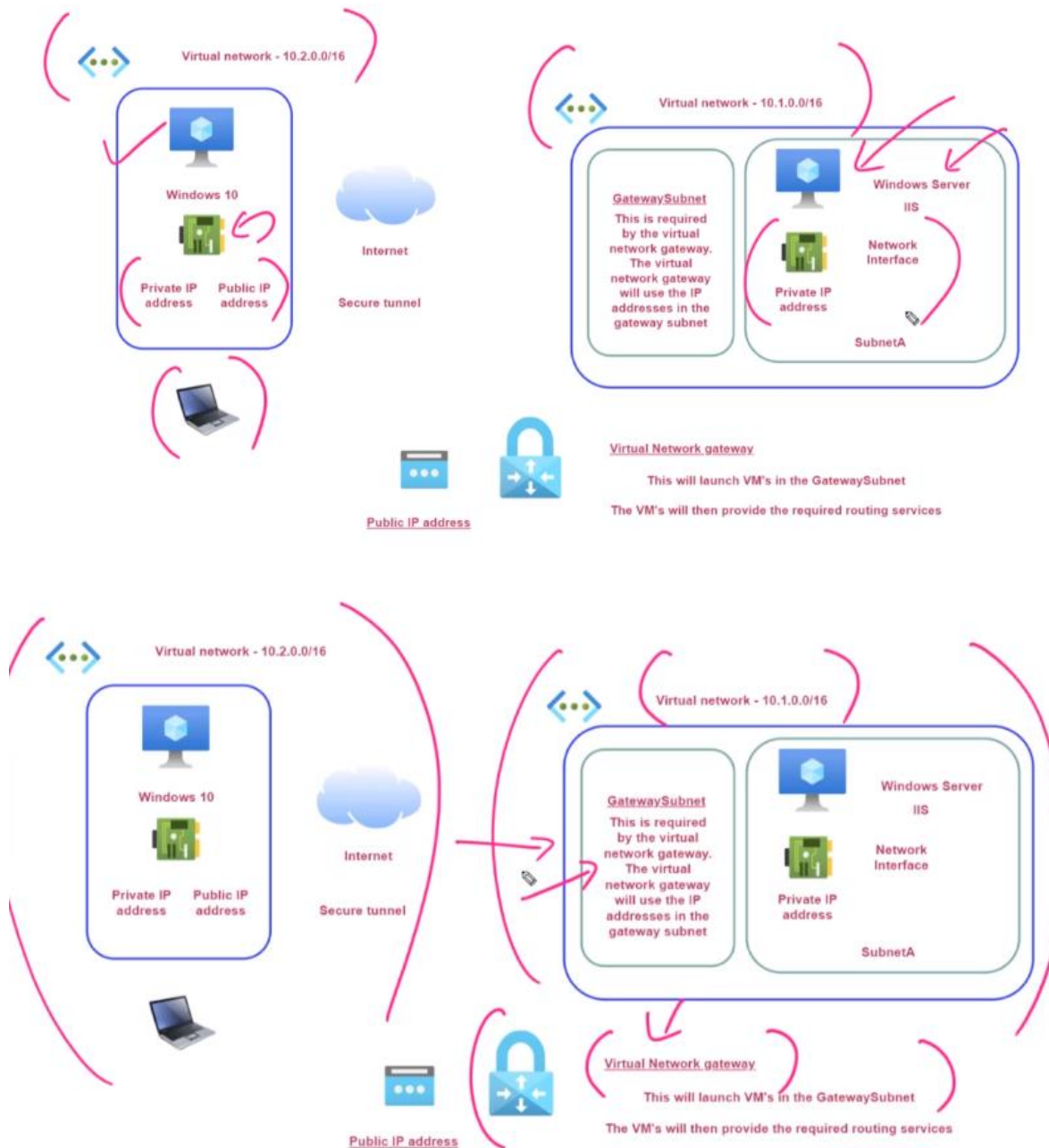
1. In order to go ahead and connect securely using the Point to site VPN connection, you have to go ahead and have certificates in place
2. You could go ahead and create your own self signed certificate, or your company might already have a private certificate provider
3. Your private certificate provider could go ahead and generate a root certificate, this generation of certificate on the certificate provider can be done by you itself on their portal
4. Once you have the root certificate, you have to go ahead and export the certificate with the Public Key and then upload it to the Point to Site connection
5. On Azure end, Azure has to authenticate the connection based on the certificate
6. Now you want to ensure a workstation can connect using the Point to site connection on the client/workstation machine you have to have a “user certificate” with a “private key” in place that user certificate is generated from the root certificate

Now from Azure you can download the VPN client and then the VPN client can be used to establish a point to site connection

Now if you want another workstation to also establish a point to site connection make sure the VPN client is also on that workstation and ensure that the same user certificate is also available on the client workstation



Point to Site VPN Connection – Lab/Simulation



The virtual network gateway has to have a Public IP address, because the traffic from the client workstation when it establishes a point to site VPN connection.

The traffic from workstation will flow from the internet then will hit the public IP address of the virtual network gateway, and the virtual network gateway will route the traffic via gateway subnet on to your Azure virtual network resources.

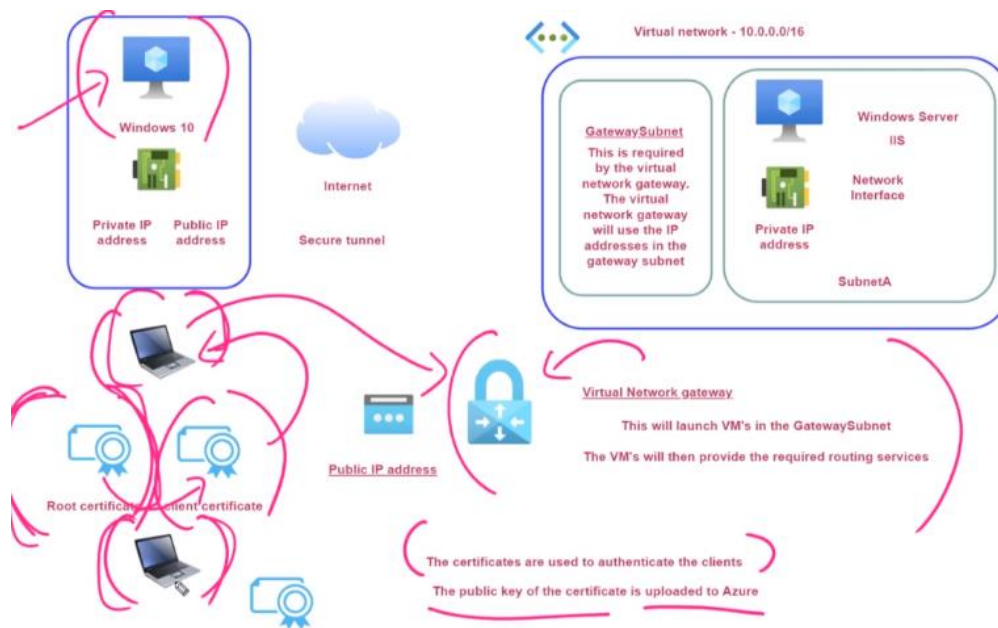
The virtual network gateway takes about 30-45 minutes to get functional ready after creation of it.

VPN Gateway Type

There are multiple options to choose which version/kind of VPN to select in Virtual Network Gateway, and generations as well. Versions are different with pricing and offering the speed of the VPN.

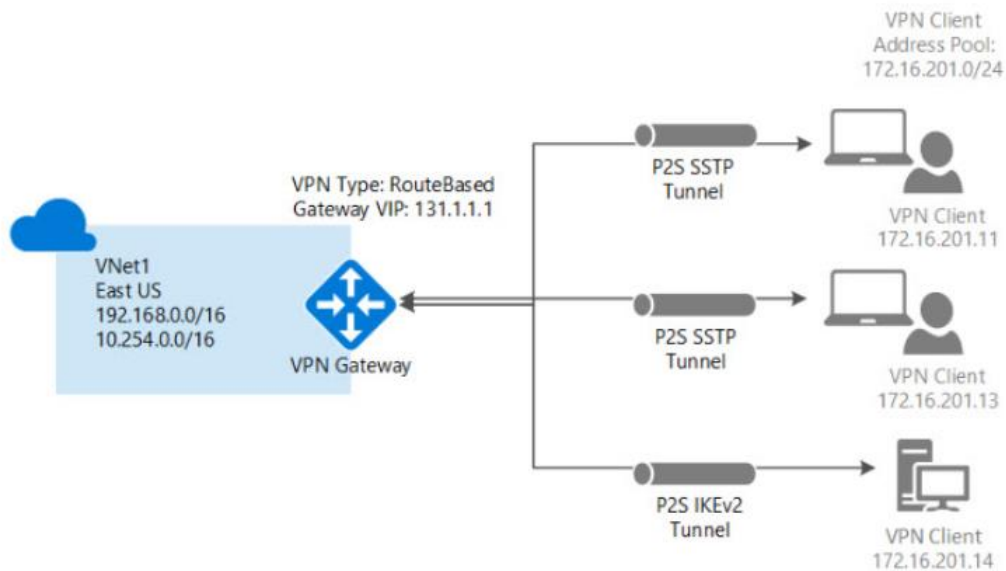
If there are so many workstations who are trying to connect to virtual machines once at a time, then you need a higher version of VPN to support many connections and bandwidth at a time, the lowest version of VPN gateway type is BASIC.

The simulation example:



A Point-to-Site VPN connection is used to establish a secure connection between multiple client machines an Azure virtual network via the Internet.

Below is a diagram from the Microsoft documentation on a sample scenario:



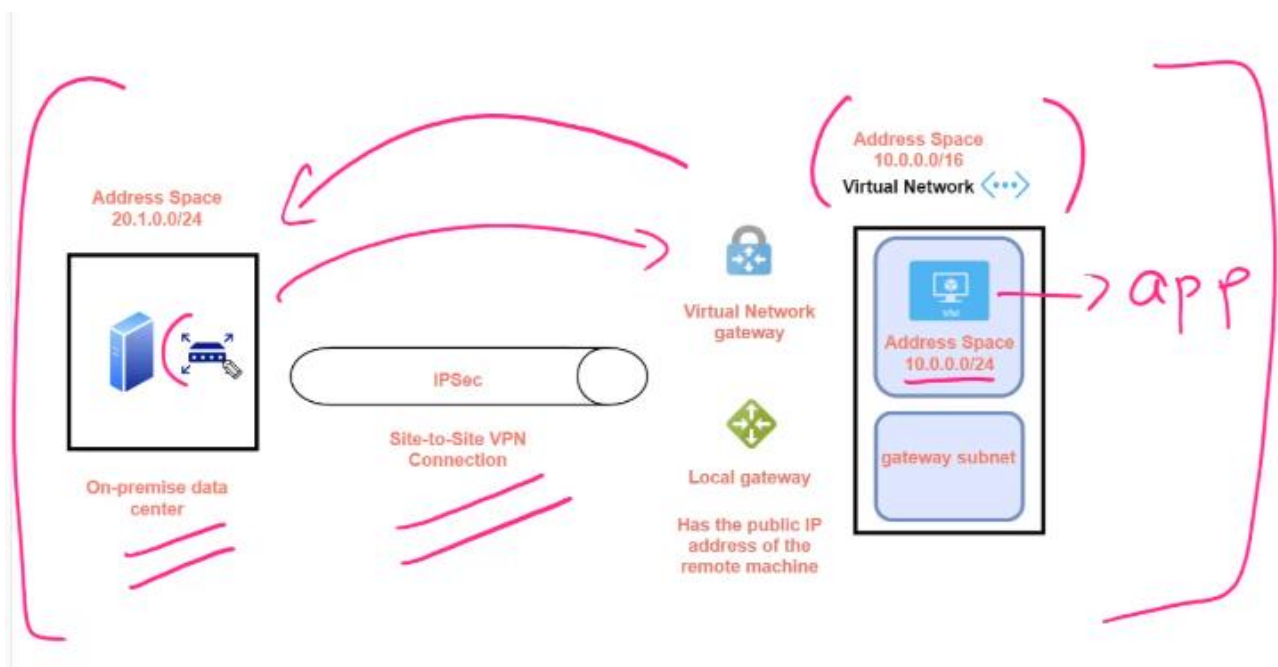
Site to Site VPN Connection

Azure VPN gateways provide cross-premises connectivity between customer premises and Azure.

In Azure environment if you want to connect your virtual machine to your on-premises data center. So instead of exposing public IP address for the Azure virtual machine and allow your employees in the company to access the applications running on the virtual machines via their public IP address.

You can have a connection between your on-premises data center and the Azure virtual network, in such a way that the communications happen via the private IP address of the virtual network, it's a more secure way to accessing your VM's.

So, connecting your entire data center onto the Azure virtual network is to go out and create a Site-to-Site VPN connection.



On the Azure end, you need to have the below configurations and services:

1. Gateway subnet
2. Local gateway
3. Virtual network gateway
4. Then site-to-site VPN connection will be established

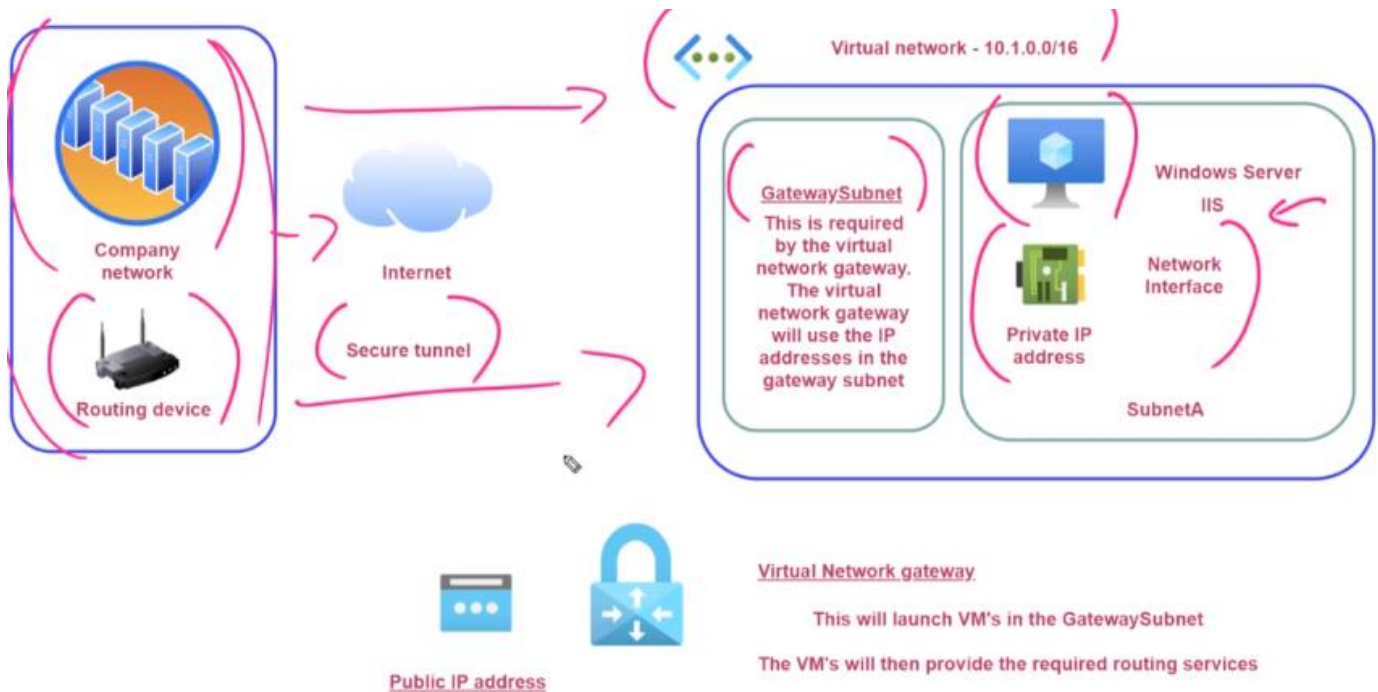
Gateway subnet – This is required by the virtual network gateway

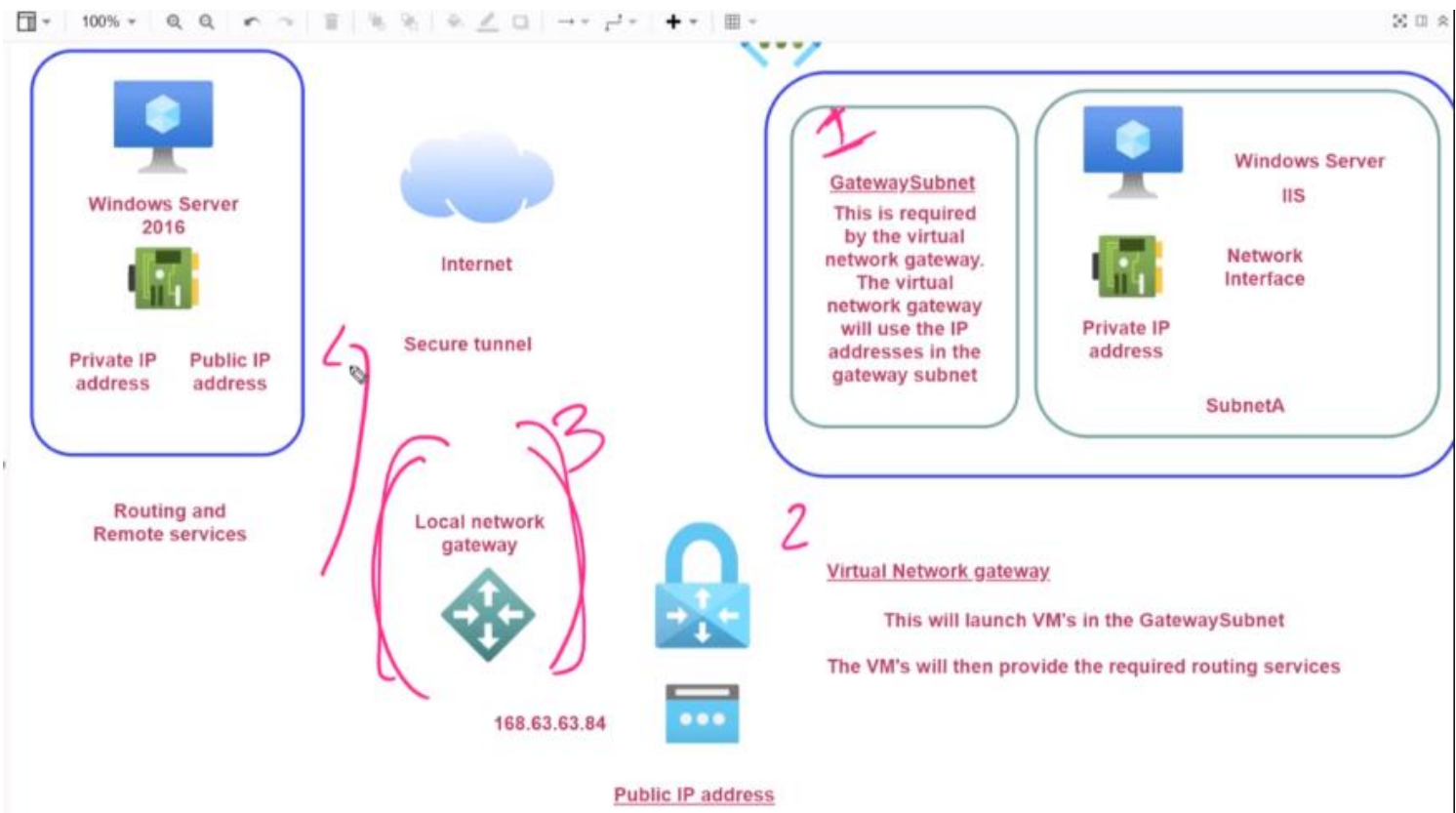
Virtual Network gateway – This will use the IP address in the gateway subnet.

On the On-premises data center, you need to have below requirements:

1. A routing device – it could be a physical device, like Cisco router.
2. A software based routing solution can also work.

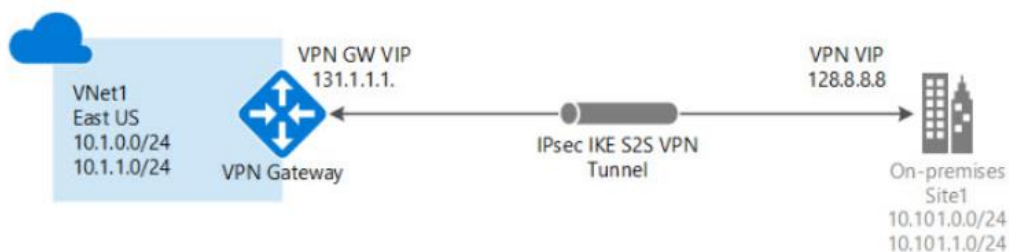
The routing device should have a capability of routing the traffic from the company network onto the virtual network in Azure.





A Site-to-Site VPN connection is used to establish a secure connection between an on-premises network and an Azure network via the Internet.

Below is a diagram from the Microsoft documentation on a sample scenario.



On the on-premises side, you need to have a VPN device that can route traffic via the Internet onto the VPN gateway in Azure. The VPN device can be a hardware device like a Cisco router or a software device (e.g Windows Server 2016 running Routing and Remote services). The VPN device needs to have a publicly routable IP address.

The subnets in your on-premises network must not overlap with the subnets in your Azure virtual network

The Site-to-Site VPN connection uses an IPsec tunnel to encrypt the traffic.

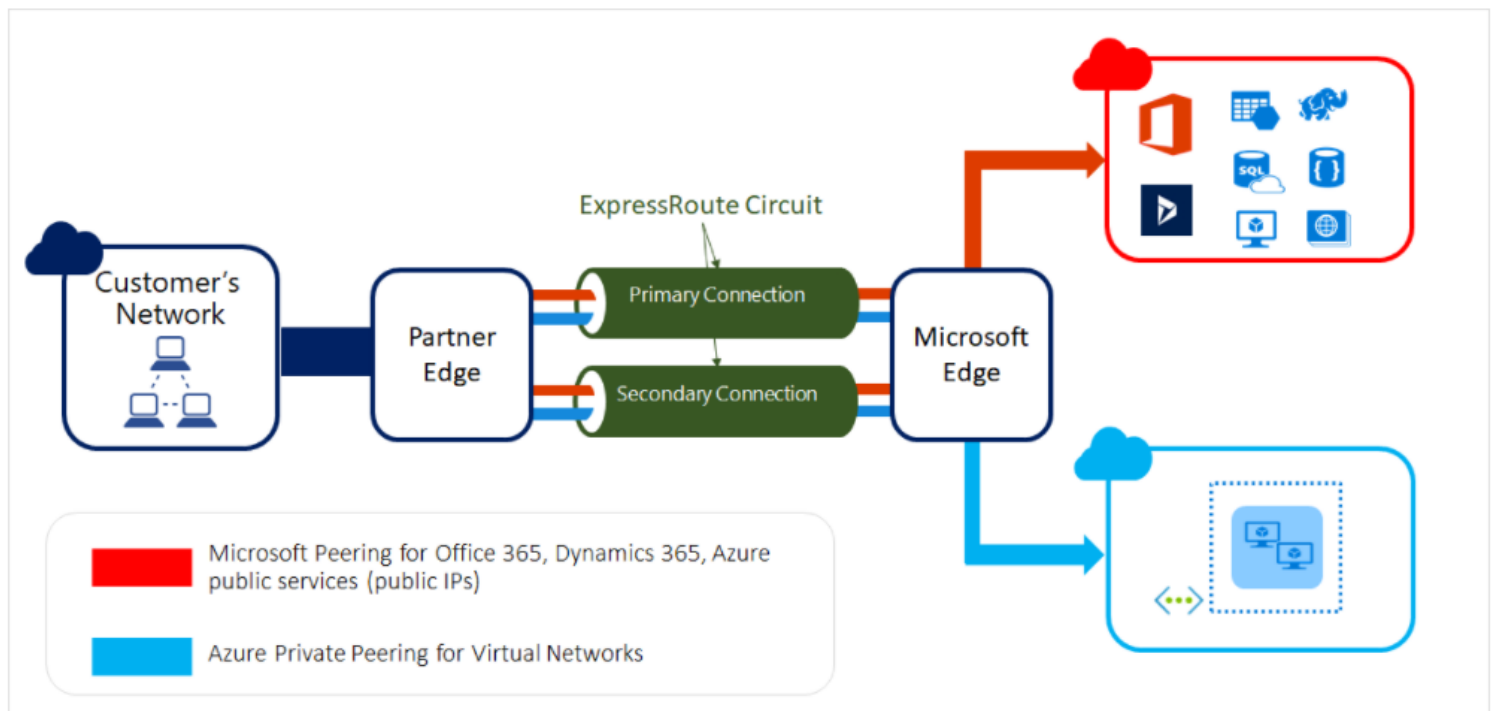
The VPN gateway resource you create in Azure is used to route encrypted traffic between your on-premises data center and your Azure virtual network.

There are different SKU's for the Azure VPN gateway service. Each SKU has a different pricing and attributes associated with it - Reference - <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpn-gateway-settings>

Azure ExpressRoute

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. ExpressRoute connections don't go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet. For information on how to connect your network to Microsoft using ExpressRoute.



My notes:

This is one of the services that allows you to connect your on-premises data center onto your Azure virtual network. In my making a dedicated connection, you can use Azure ExpressRoute circuit.

When you connect your customer network onto let's say an Azure virtual network using express route all the traffic flows via the entire Microsoft backbone network. This makes it much faster when it comes to the data transfer between the customer network and Azure virtual network.

You can also connect your customer network onto PaaS services such as Azure storage account, Azure SQL database and even MS Office 365.

In this case your connection is not going over the internet.

In Azure ExpressRoute, you create something known as Express Route Circuit, in that circuit you create something known as peering connections onto either private services such as Azure virtual network or onto public services such as Azure storage account, Azure SQL or MS Office 365.

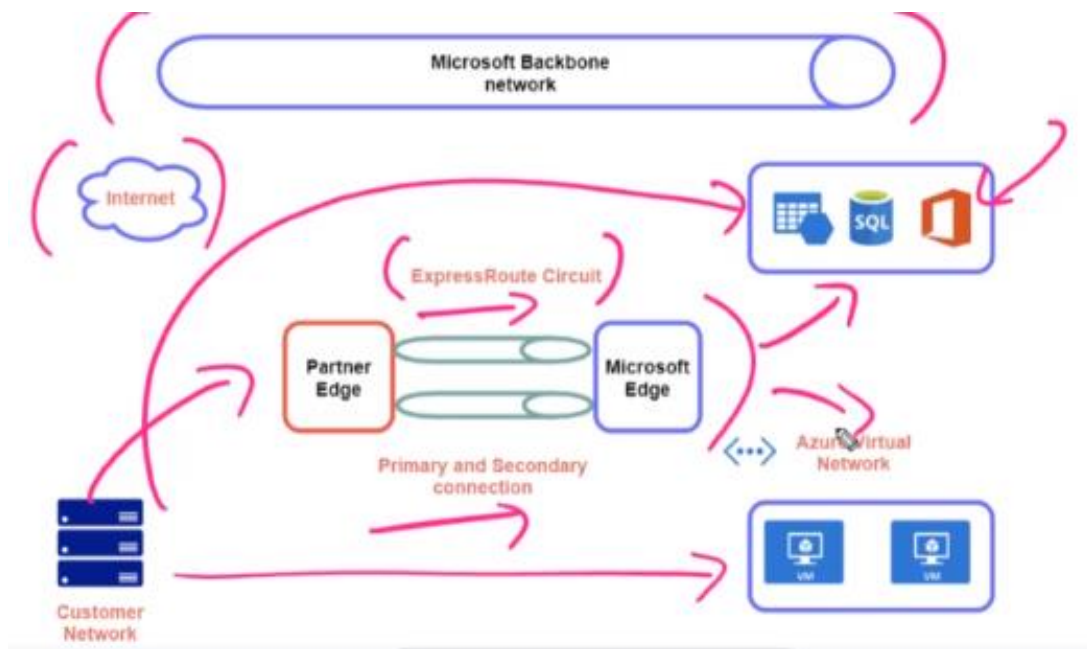
When you want to set up an Azure ExpressRoute circuit, you can create either a dedicated connection or you can create a connection via the third-party provider.

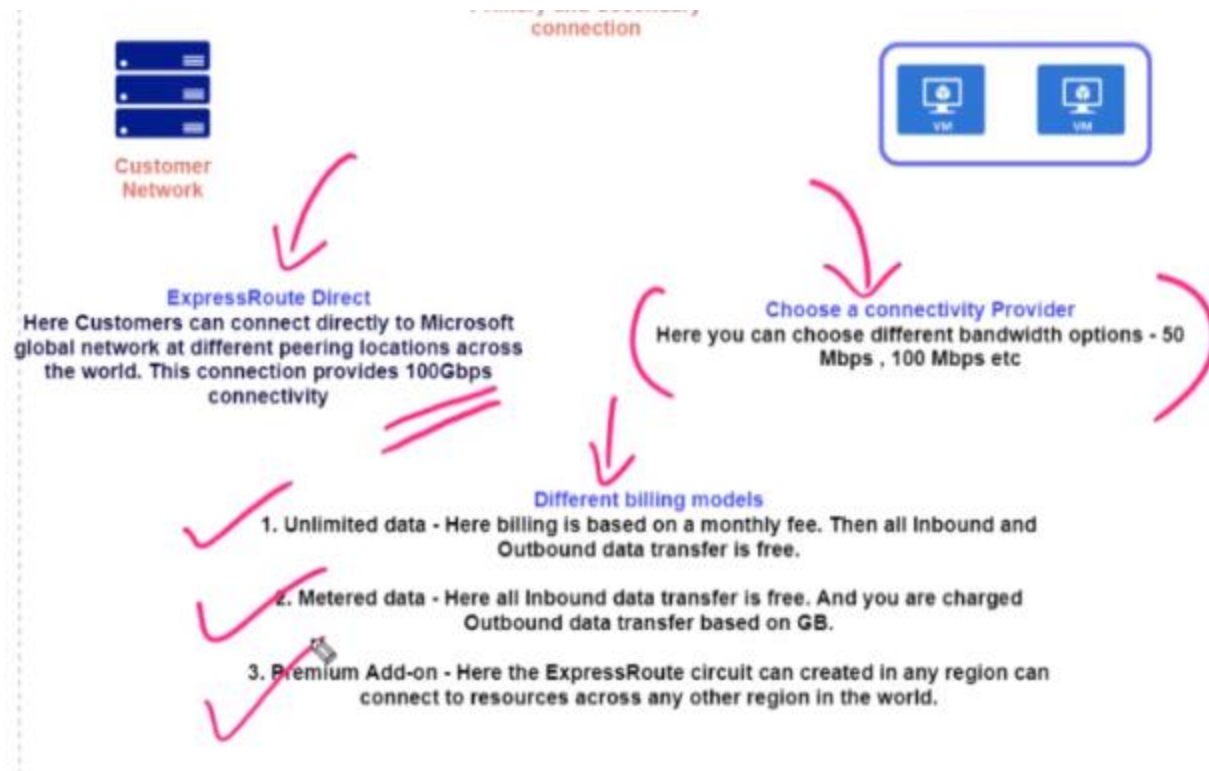
ExpressRoute are used by large organizations that need to have the dedicated line. This is for those organizations that want to have a large bandwidth pipe between their customer network and Azure.

Your connection can flow through internet service provider or a third-party provider, it's actually known as a partner edge. You then have connections on to Microsoft Edge.

So, when you create an ExpressRoute circuit connection, there are two connections in place, a primary and a secondary connection. This is used for high availability.

This connects on to Microsoft Edge network, we then have connections on to Azure services.





Azure Network Watcher

Azure Network Watcher allows you to monitor, diagnose, and gain insight into your network performance between various points in the network infrastructure. Here's a breakdown of some of the elements.

- ✚ This service provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in Azure virtual network
- ✚ It is used to monitor the network for your Infrastructure-as-a-service (IaaS)
- ✚ This tool is not intended for monitoring your PaaS solutions or for Web Analytics

1. The Monitoring Element
2. The Network Performance Monitor
3. Diagnostics Tool
 - IP Flow
 - The Connection Troubleshooting Tool
 - The Packet Capture Tool
4. Metrics Tool
5. Logging

Connection Monitor

- ✚ This provides a unified end-to-end connection monitoring in Azure Network Watcher
- ✚ This supports both Azure and Hybrid setup as well
- ✚ This tool can get you better visibility into network performance
- ✚ It supports connectivity checks based on HTTP, TCP, ICMP

IP Flow Verify – Detecting Traffic Filtering Problems

- ✚ This tool can be used to check if a packet has been allowed or denied access to or from a virtual machine
- ✚ You can choose to check the packet flow based on Protocol (TCP, UDP), Local and Remote IP address and port number
- ✚ This tool basically looks at the rules in the Network Security Groups (NSG) assigned to subnet or the virtual machine INC
- ✚ You can use this tool to confirm whether a rule in a Network Security Groups (NSG) is blocking ingress or egress traffic to or from a virtual machine

Next Hop – Detecting Virtual Machine Routing Problems

- ✚ This tool can be used to check if traffic is being sent to the destination based on the routes associated with the network interface
- ✚ You can get next hop type, IP address, and Route table being used to route traffic
- ✚ You can use this to understand whether traffic is being routed to the intended destination

Connection Troubleshoot – Diagnose Connectivity

- ✚ This tool can be used to check the connection between virtual machines or from a virtual machine to a fully qualified domain name, URL or IPv4 address
- ✚ Since there are many parameters that can hinder network connectivity such as Network Security Groups (NSG) on the virtual machines, this tool can be used to give insights onto any connectivity issues

VPN Troubleshoot

- ✚ This tool can be used to check the connectivity between on-premises resources and other virtual networks in Azure

Packet Capture

- This can be used to capture traffic to and from a virtual machine

Network Security Group Logging

- This tool gives more information on the ingress and egress IP traffic flowing via a Network Security Groups (NSG)
- Here the flow logs are written in JSON format

Traffic Analysis

- This provides visibility into the user and application activity
- This tool analyzes the Network Watcher network security groups flow logs
- It provides more insight into the traffic flow

Traffic Analytics

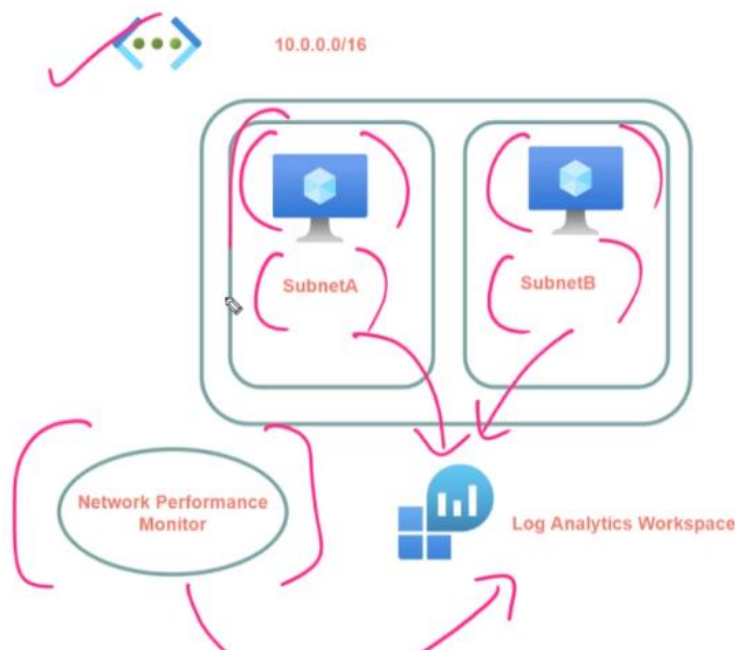
Traffic Analytics is a cloud-based solution that provides visibility into user and application activity in cloud networks. Traffic analytics analyzes Network Watcher network security group (NSG) flow logs to provide insights into traffic

flow in your Azure cloud. With traffic analytics, you can:

1. Visualize network activity across your Azure subscriptions and identify hot spots.
2. Identify security threats to, and secure your network, with information such as open-ports, applications attempting internet access, and virtual machines (VM) connecting to rogue networks.
3. Understand traffic flow patterns across Azure regions and the internet to optimize your network deployment for performance and capacity.
4. Pinpoint network misconfigurations leading to failed connections in your network.

Azure Network Performance Monitor

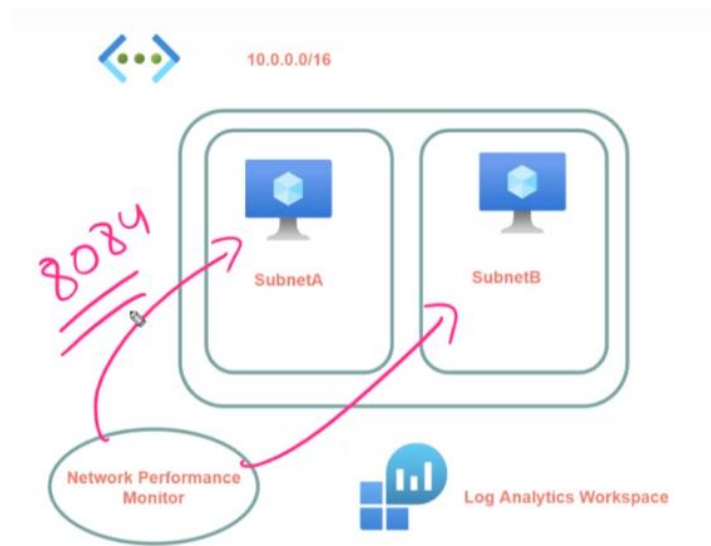
1. This is a network monitoring tool that can help monitor performance between various points in your network infrastructure.
2. It can also be used to monitor network connectivity to service and application endpoints and monitor the performance of Azure ExpressRoute.
3. This tool can be used to detect network issues and also generate alerts based on the issues.
4. **Performance Monitor** – This can be used to monitor network connectivity across cloud deployments and on-premises locations, multiple data centers and branch offices.
5. **Service Connectivity Monitor** – This can be used to monitor connectivity from users to important services. These are tests based on HTTP, HTTPS, TCP, and ICMP to monitor the real time availability and response time of your service.



The network performance monitor solution is going to go ahead and simulate synthetic transactions against both of the VM's in these different subnets to go ahead and understand the network performance.

So based on any sort of latency or any sort of network traffic, it will actually go ahead and take that data and via the log analytics workspace you will see the data within network performance monitor.

Network performance monitor will send synthetic transactions, and this will be done on to the inbound ports of the both the VM's. By default, the ports that will be used is 8084.



Numbers of Steps to Perform:

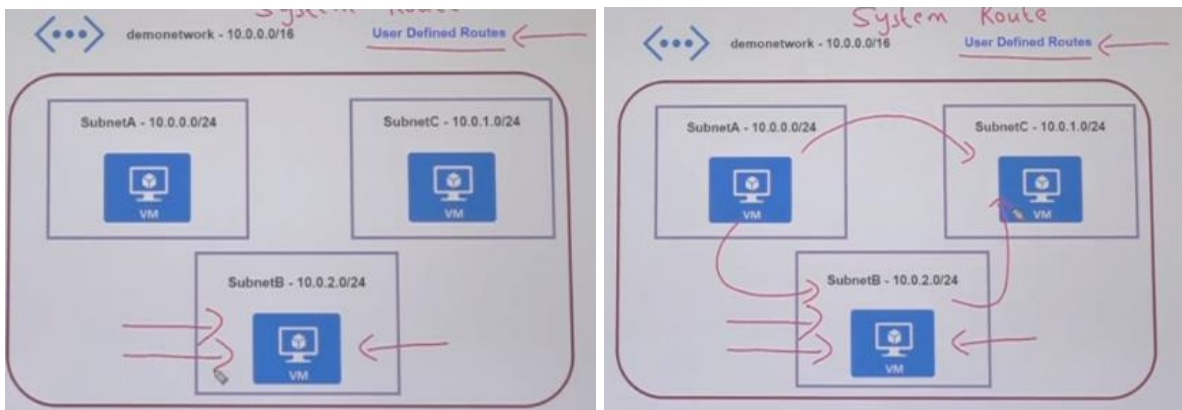
1. Open up the port in NSG
2. Also run a PowerShell script
3. The VM's already have that PowerShell script, and have to execute that script
4. The script will open the ports on Windows firewall, not on NSG, and do number of jobs

Note:

The subnet or the virtual network which you want to monitor, just go out and install agent on one of the VM's in that subnet in that virtual network.

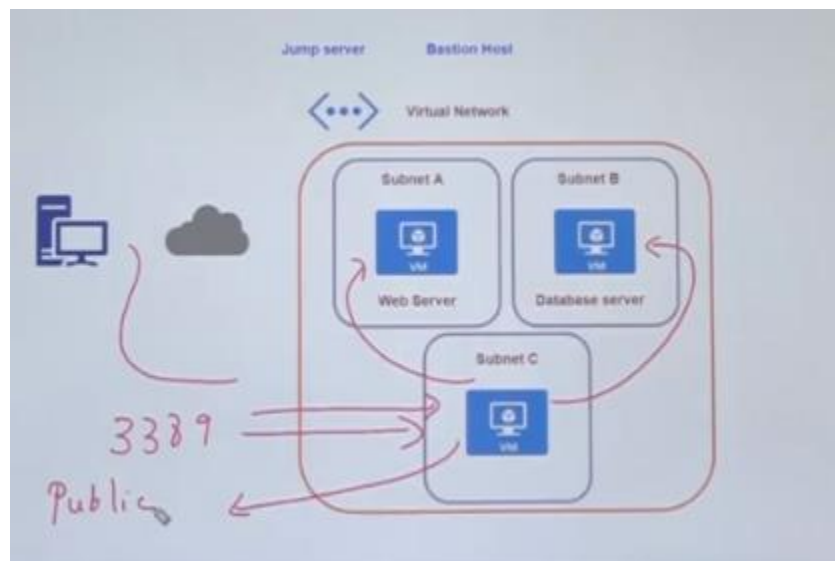
Azure Custom Routes

Azure routes traffic between all subnets within a virtual network, by default. You can create your own routes to override Azure's default routing. Custom routes are helpful when, for example, you want to route traffic between subnets through a network virtual appliance.



Azure Jump Server or Bastion Host

When we create a virtual machine in the Azure cloud. This virtual machine is on the virtual network on the Azure cloud. This VM is called Jumpbox also named as Jump server. Then, by using this VM, we can connect to the other Azure VM's using dynamic IP. Jump box prevents all Azure VM's to expose to the public.



Azure Bastion Service

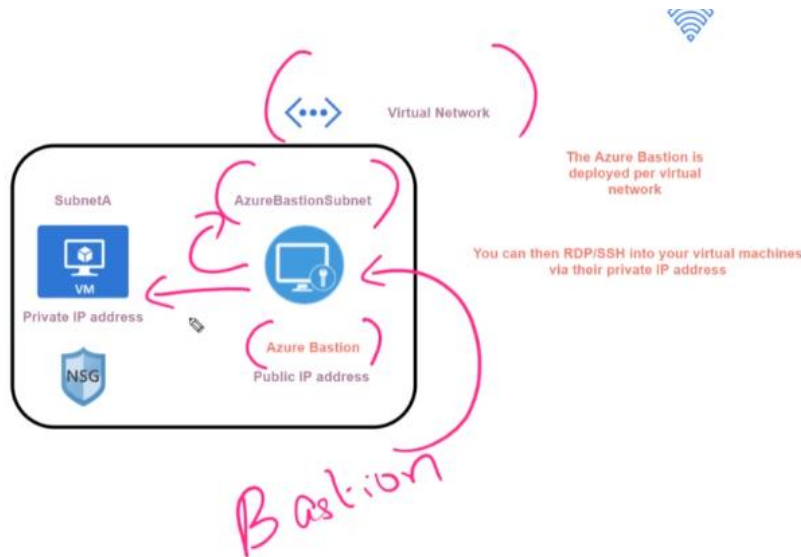
Azure Bastion is a service you deploy that lets you connect to a virtual machine using your browser and the Azure portal. The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly from the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address, agent, or special client software.

Bastion provides secure RDP and SSH connectivity to all of the VMs in the virtual network in which it is provisioned. Using Azure Bastion protects your virtual machines from exposing RDP/SSH ports to the outside world, while still providing secure access using RDP/SSH.

Note:

In order to go ahead and launch the Azure Bastion host in your virtual network, you need to have a subnet known as BastionSubnet.

We are going to go ahead and connect via the bastion host on the public address onto our VM, but this is going to be seamlessly with the help of Bastion service.



Azure Firewall

Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

Azure Firewall uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.

Key Points:

1. Azure Firewall has a built-in availability
2. It can deploy the Azure Firewall instance across two or more Availability Zones – 99.99% SLA
3. You can filter traffic based on fully qualified domain name
4. You can also create network filtering rules – Based on source and destination IP address, port, and protocol
5. It is stateful in nature, so it understands what packets of data to allow
6. It has built-in threat intelligence – Here you can get alerts or deny traffic from/to malicious IP addresses and domain

Notes:

- Azure Firewall service is actually linked with the virtual network

-
- The diagram illustrates the Azure Firewall architecture. At the bottom, an **On-premises** network (represented by a server icon) connects to a **Central VNet** (represented by a cloud icon with a double-headed arrow). This connection is labeled **Azure to on-prem traffic filtering**. The **Central VNet** is connected to two **Spoke VNETs** (labeled **Spoke 1** and **Spoke 2**), each containing two computer icons. The **Central VNet** also connects to the **Azure Firewall** (represented by a cloud icon with a red 'X' and a green checkmark). The **Azure Firewall** is connected to the Internet (represented by a globe icon). The **Azure Firewall** is configured with **User configuration L3-L7 connectivity policies** and **Microsoft Threat Intelligence Known malicious IPs and FQDNs**. The **Azure Firewall** allows inbound/outbound access based on **Threat intel, NAT, network and application traffic filtering rules**. The **Azure Firewall** is also connected to the Internet via a green checkmark and a red 'X', with the text **Traffic is denied by default** indicating that traffic is blocked by default.



Azure DNS

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services. You can't use Azure DNS to buy a domain name.

Azure Private DNS

- A private zone can be linked to one or more virtual networks by the use of virtual networks links
- Auto-registration – This allows VM's to be automatically registered in the private DNS zone

Azure Private DNS provides a reliable and secure DNS service for your virtual network. Azure Private DNS manages and resolves domain names in the virtual network without the need to configure a custom DNS solution. By using private DNS zones, you can use your own custom domain name instead of the Azure-provided names during deployment.

Using a custom domain name helps you tailor your virtual network architecture to best suit your organization's needs. It provides a naming resolution for virtual machines (VMs) within a virtual network and connected virtual networks. Additionally, you can configure zones names with a split-horizon view, which allows a private and a public DNS zone to share the name.

Azure Storage Accounts

An Azure storage account contains all of your Azure Storage data objects: blobs, file shares, queues, tables, and disks. The storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS. Data in your storage account is durable and highly available, secure, and massively scalable.

Storage Data Objects:

- Blobs
- File shares
- Queues
- Tables
- Disks

Azure Storage Explorer

Microsoft Azure Storage Explorer is a standalone app that makes it easy to work with Azure Storage data on Windows, macOS, and Linux. It is a useful GUI tool for inspecting and altering the data in your Windows Azure Storage projects including the logs of your cloud-hosted applications.

All 3 types of cloud storage can be viewed and edited: blobs, queues, and tables.

Access Storage Account Access

There are three ways you give access onto storage account, below are those:

- Access Keys
- Shared Access Signatures
- Azure Active Directory (User defined roles by RBAC)

Storage Account access keys – gives you full authorization over all of the services that are part of your storage account

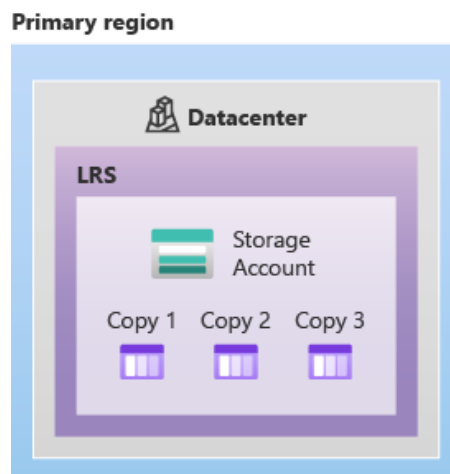
Azure Storage Redundancy / Replication

Azure Storage always stores multiple copies of your data so that it is protected from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters. Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.

1. Locally redundant storage (LRS)

It copies your data synchronously three times within a single physical location in the primary region. LRS is the least expensive replication option but is not recommended for applications requiring high availability or durability.

Note: In LRS case, the data is getting stored on 3 different storage devices within the same data center, so your data remains in the same data center, and do not gets shared into any other zones or geo location.



2. Zone-redundant storage (ZRS)

It copies your data synchronously across three Azure availability zones in the primary region. For applications requiring high availability, Microsoft recommends using ZRS in the primary region, and also replicating to a secondary region.

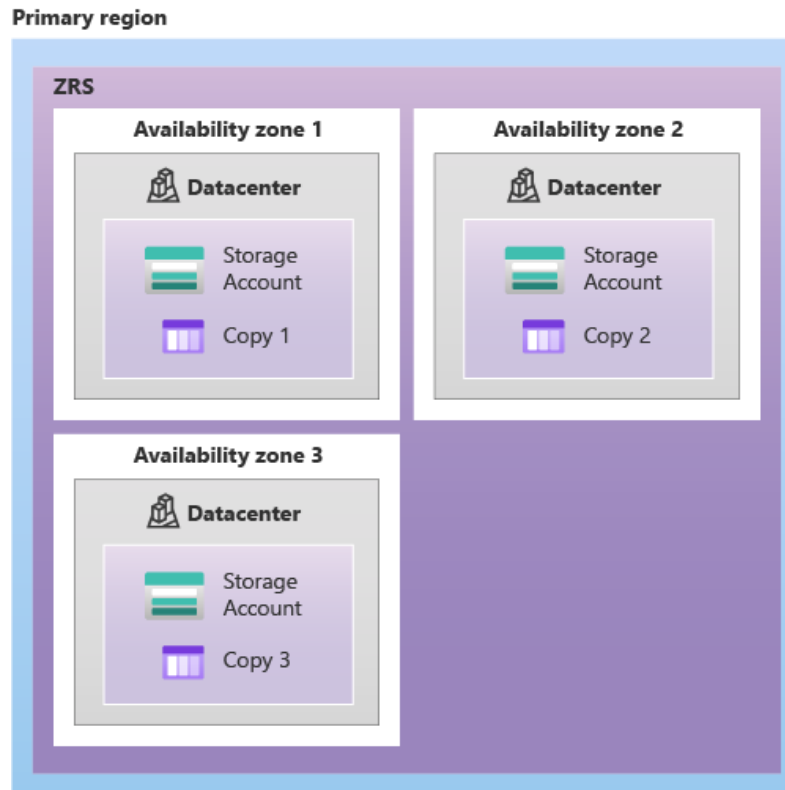
Zone Redundant Storage (ZRS) helps you to protect against data center level failure.

Notes:

In one geo location, there are 3 three availability zones.

Each availability zone is a separate physical location with independent power, cooling, and networking. And each zone is a collection of multiple data centers

In this case the file or data will be copied in another data center in another availability zone, to avoid data center failures



3. Geo-redundant storage (GRS)

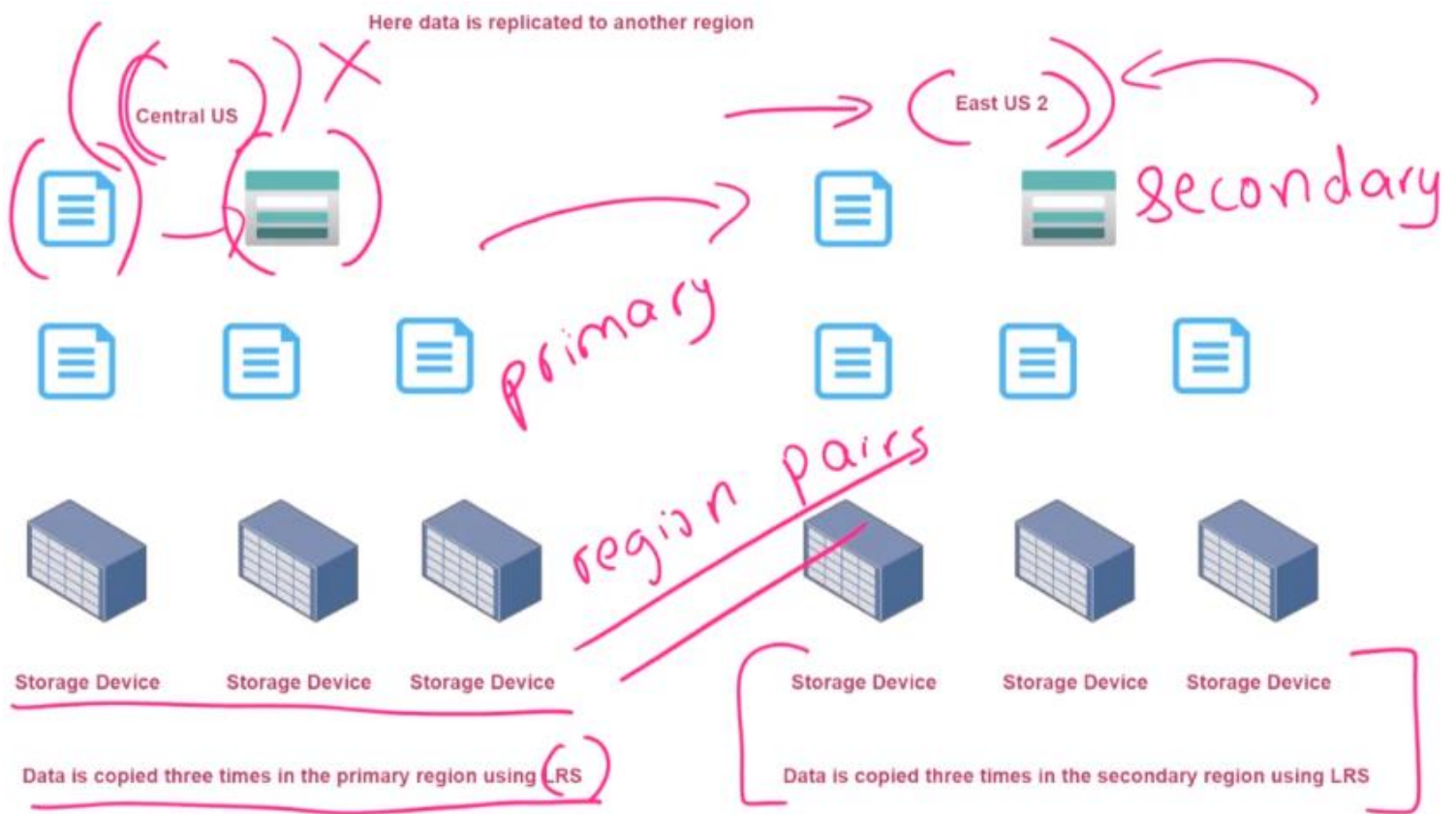
Geo-redundant storage (GRS) copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in a secondary region that is hundreds of miles away from the primary region. GRS offers durability for Azure Storage data objects of at least 99.99999999999999% (16 9's) over a given year.

Notes:

In GRS case, your data will be replicated on to a different region altogether.

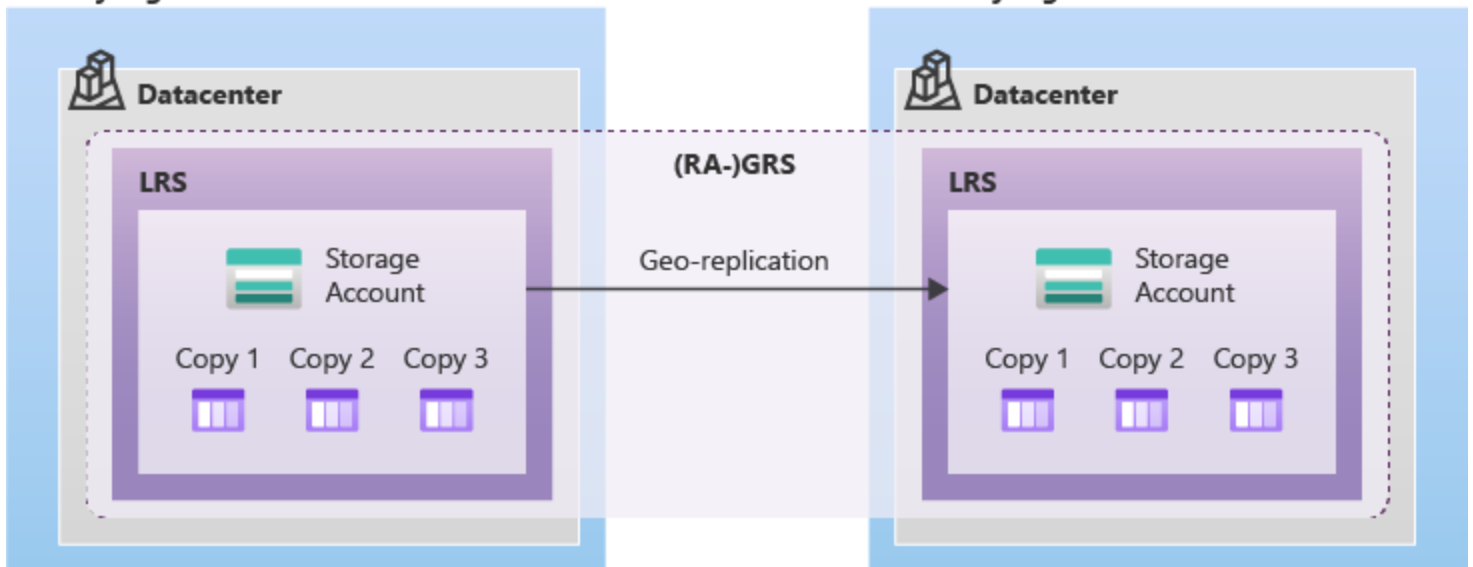
In this scenario Local redundancy storage will also work, and the data will be stored locally on three devices within a data center.

In this case, if entire zone, like Central US goes down, your data will be available in East US 2.



Primary region

Secondary region



4. Read-access Zone Redundant Storage

Read-access zone redundant storage is similar to zone redundant storage, but in this scenario, you would be able to access your data in both the regions at the same time, like: US-East 1 & Central US.

Use Case: So, if your application needs access onto objects in both of the regions, you can choose Read-access zone redundant storage.

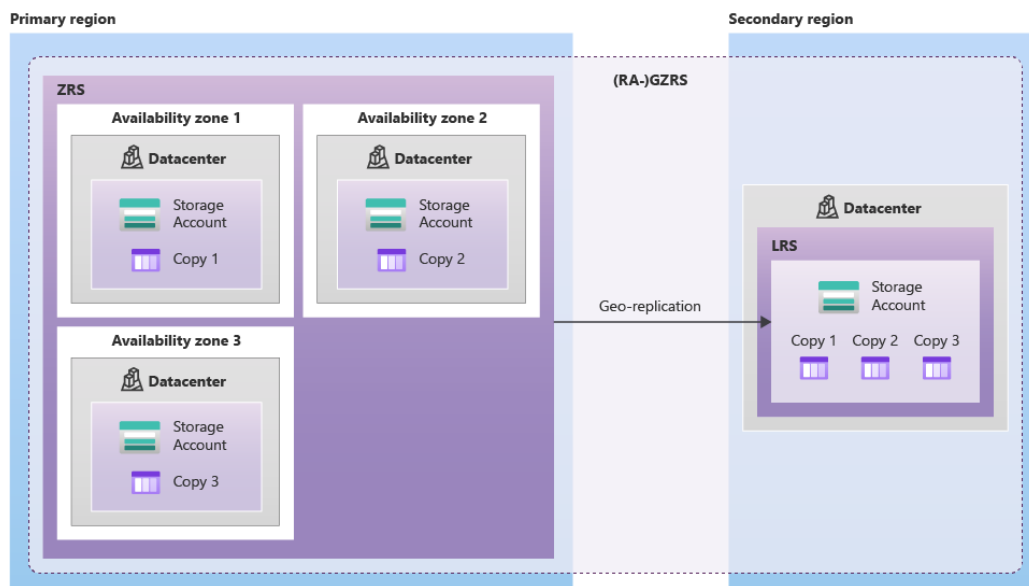
5. Geo-zone-redundant storage

Geo-zone-redundant storage (GZRS) combines the high availability provided by redundancy across availability zones with protection from regional outages provided by geo-replication. Data in a GZRS storage account is copied across three Azure availability zones in the primary region and is also replicated to a secondary geographic region for protection from regional disasters. Microsoft recommends using GZRS for applications requiring maximum consistency, durability, and availability, excellent performance, and resilience for disaster recovery.

With a GZRS storage account, you can continue to read and write data if an availability zone becomes unavailable or is unrecoverable. Additionally, your data is also durable in the case of a complete regional outage or a disaster in which the primary region isn't recoverable. GZRS is designed to provide at least 99.99999999999999% (16 9's) durability of objects over a given year.

Only general-purpose v2 storage accounts support GZRS and RA-GZRS.

Read-Access Geo-Zone-Redundant Storage (RA-GZRS) is also there.



Azure Storage – Access Tiers

There are three access tiers in Azure storage.

1. **Hot Access Tier** – This is used for data that is accessed frequently
2. **Cool Access Tier** – This is used for data that is accessed infrequently and stored for at least 30 days
3. **Archive Access Tier** – This is used for data that is rarely accessed and stored for at least 180 days

Archive can be only enabled on individual Blob level. Hot & Cool can be enabled for any kind of storage, like Blob, files, tables

How to access Archive files

1. You have to rehydrate the file to access the file

2. To rehydrate the file, you have to change the access tier of the file to either Hot or Cool to access the file
3. It takes time to rehydrate and access that object

Rehydration Process

There are two options


1. Standard Priority

The request is processed in the order received and can take up to 15 hours. After this time only you could access the file

2. High Priority

The request is prioritized and could finish in under 1 hour for objects under 10 GB in size

Azure Storage Accounts



Data storage prices pay-as-you-go
All prices are per GB per month.

	PREMIUM	HOT	COOL	ARCHIVE
First 50 terabyte (TB) / month	\$0.15 per GB	\$0.0184 per GB	\$0.01 per GB	\$0.00099 per GB
Next 450 TB / month	\$0.15 per GB	\$0.0177 per GB	\$0.01 per GB	\$0.00099 per GB
Over 500 TB / month	\$0.15 per GB	\$0.0170 per GB	\$0.01 per GB	\$0.00099 per GB

When a company starts storing millions of objects, then the storage price makes a difference

Azure Block Blob Storage

Premium Performance for Block Blob Storage

Block blobs are optimized for uploading large amounts of data efficiently. Block blobs are composed of blocks, each of which is identified by a block ID.

1. Block blobs are basically your objects such as videos and images
2. You can create a **BlockBlobStorage** account of the Premium performance kind
3. Here the data will be stored on solid state drive (SSD). This will give you faster access to your data when compared to let's say using the Blob service in General Purpose v2 storage accounts
4. If you have applications like Artificial Intelligence or Machine Learning applications that require rapid responses to change in data, you can consider this type of storage account

Premium Performance for block blob

› Reference - <https://azure.microsoft.com/en-us/pricing/details/storage/blobs/>

Data storage prices pay-as-you-go

All prices are per GB per month.

	PREMIUM	HOT	COOL	ARCHIVE
First 50 terabyte (TB) / month	\$0.15 per GB	\$0.0184 per GB	\$0.01 per GB	\$0.00099 per GB
Next 450 TB / month	\$0.15 per GB	\$0.0177 per GB	\$0.01 per GB	\$0.00099 per GB
Over 500 TB / month	\$0.15 per GB	\$0.0170 per GB	\$0.01 per GB	\$0.00099 per GB

Premium Performance for page Blob

1. Page blobs are basically used for storing disk files for your virtual machines
2. You can choose Premium SSD to get the best performance for your page Blob
3. This will increase the storage performance for your underlying virtual machines
4. With Azure Management Disks, you can also choose Premium SSD's
5. You can use un-managed disks, where in you manage the disks for your virtual machines
6. You can choose General Purpose V2 or General Purpose V1 storage accounts of the Premium Performance to store page blobs

Azure Storage Account – Change Replication

1. If you want to migrate the storage account from LRS to ZRS in the primary region, then you need to perform either a manual migration or live migration
 - For a manual migration, you basically create another storage account with the ZRS replication type, and then you copy the data from the source onto the destination
 - Now during the manual migration, you might need to ensure that no new objects are being added on to your primary storage accounts because you need to go out and migrate everything at a particular point in time once a migration is complete
 - If you have an application that has been using that storage account that you need to go out and switch onto a new storage account, so there might be a downtime for your application during a manual migration.
2. You can also request Microsoft to perform a live migration. This ensures that you have no application downtime during the migration process. Here you can access the data as the migration is processing
3. To migrate from LRS to GZRS or RA-GZRS, first switch to GRS or RA-GRS and then request a live migration
4. To migrate from GRS or RA-GRS to ZRS, first switch to LRS, then request a live migration

Azure Storage Account – Lifecycle Management Policies

Azure Blob Storage lifecycle management offers a rich, rule-based policy for GPv2 and blob storage accounts. Use the policy to transition your data to the appropriate access tiers or expire at the end of the data's lifecycle. The lifecycle management feature is available in all Azure regions for general purpose v2 (GPv2) accounts, blob storage accounts, premium block blobs storage accounts, and Azure Data Lake Storage Gen2 accounts.

Azure Storage Account – Object Replication

Object replication asynchronously copies block blobs between a source storage account and a destination account.

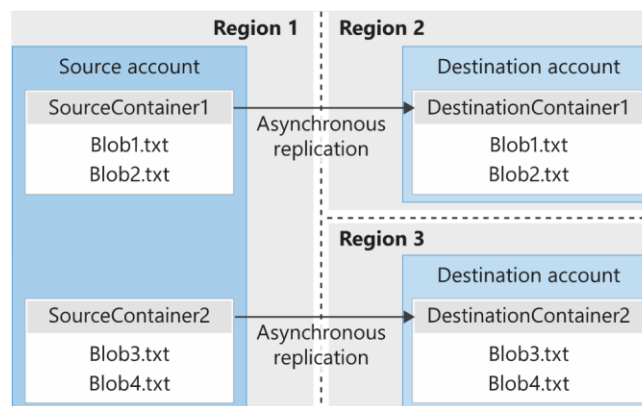
Some benefits and use cases:

- Minimizing latency
- Increase efficiency for compute workloads
- Optimizing data distribution
- Optimizing costs

Notes:

- Object replication works if the blobs are either in the Hot/Cool access tier
- Object replication will fail if the objects are in the archive access tier

The following diagram shows how object replication replicates block blobs from a source storage account in one region to destination accounts in two different regions.



Azure – File Share

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) protocol or Network File System (NFS) protocol. Azure file shares can be mounted concurrently by cloud or on-premises deployments. Azure Files SMB file shares are accessible from Windows, Linux, and macOS clients.

Azure Files NFS file shares are accessible from Linux or macOS clients. Additionally, Azure Files SMB file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

Key benefits of Azure File Share

1. Shared access

Azure file shares support the industry standard SMB and NFS protocols. Being able to share a file system across multiple machines, applications/instances is a significant advantage with Azure Files for applications that need shareability.

2. Fully managed

Azure file shares can be created without the need to manage hardware or an OS. This means you don't have to deal with patching the server OS with critical security upgrades or replacing faulty hard disks.

3. Scripting and tooling

PowerShell cmdlets and Azure CLI can be used to create, mount, and manage Azure file shares as part of the administration of Azure applications. You can create and manage Azure file shares using Azure portal and Azure Storage Explorer.

4. Resiliency

Azure Files has been built from the ground up to be always available. Replacing on-premises file shares with Azure Files means you no longer have to wake up to deal with local power outages or network issues.

5. Familiar programmability

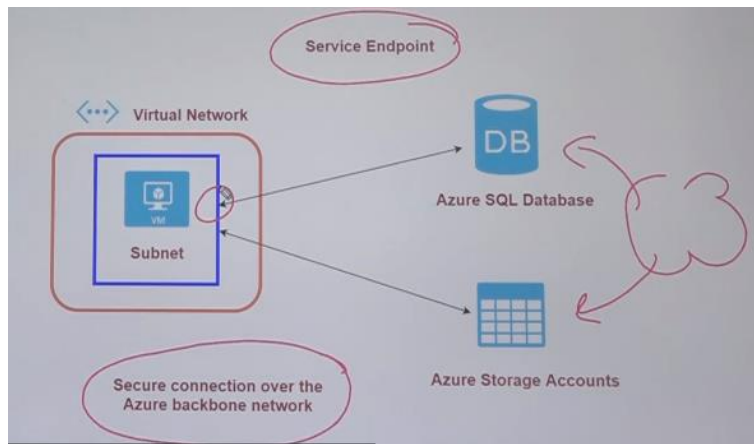
Applications running in Azure can access data in the share via file system I/O APIs. Developers can therefore leverage their existing code and skills to migrate existing applications. In addition to System IO APIs, you can use Azure Storage Client Libraries or the Azure Storage REST API.

Azure Service Endpoint

Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet. This feature is available for the following Azure services and regions.

So, when you establish a service endpoint from your virtual network onto the services all of the traffic goes via the Azure backbone network. So, none of the traffic from the virtual machine onto either the services or resources goes via the internet.

First you have to ensure that you enable a service endpoint for that particular service from within the virtual network and then you can link the service endpoint onto a particular subnet. Once you do from that resource itself, you then have to go ahead and add that virtual network.



Azure Private Endpoint

Azure Private Endpoint is a network interface that connects you privately and securely to a service powered by Azure Private Link. Private Endpoint uses a private IP address from your VNet, effectively bringing the service into your VNet. The service could be an Azure service such as Azure Storage, Azure Cosmos DB, Azure SQL Database, or your own Private Link Service.

- ✚ Azure private endpoint is a network interface that can be provisioned in your virtual network
- ✚ It allows you to connect privately and securely to a service
- ✚ The service can be storage account, Azure Cosmos DB, etc.

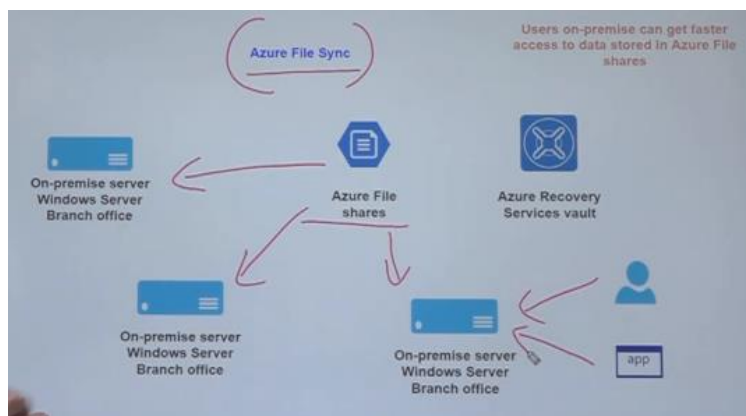
Azure File Sync

Azure File Sync is a service that allows you to cache several Azure file shares on an on-premises Windows Server or cloud VM.

You can use the Azure File Sync service to seek files from your file share onto your on-premises servers. You could use the file share service to actually sync the files from Azure File Share onto multiple servers in your on-premises locations.

Example:

You have multiple branch offices, and you want the file shares to be available locally so they could be accessed faster.



Transferring Data to Azure Storage Accounts

Azure Import/Export Service

- This can be used to securely import large amounts of data to the Azure Blob and Azure File service
- Here you can actually store the data that you want to transfer on your own drives, or you can use disk drives provided by Microsoft
- You can ship the drives to an Azure datacenter
- The data on the drives will be imported to Azure Blob or Azure File storage
- You can also use the service to export data from Azure Blobs

What are general steps involved

1. First you decide the storage account that you're going to import data into
2. What is the type of service you want – Azure Blob or Azure File Share
3. Then, finally you have your disk drives in place on which you're going to have your data
4. Now on your disk drives you need to get your data in a ready state that needs to be imported onto Azure Storage Account. For that you have to download a tool, that's freely available.
5. WAImportExportTool to copy data onto disk drives . The Disk Drives needs to be encrypted with BitLocker
6. You then need to create an import job in Azure. Here you need to associate the job with an Azure storage account. You also need to upload the drive journal files to the job
7. You also need to mention the return address (while physically mailing the drives onto the Azure Datacenters)
8. Then ship the drives to the Azure datacenters

AzCopy Tool

Another tool which is available for transferring data is AzCopy Tool

- This is a command utility that you can use to copy blobs or files to or from a storage account
- This tool works on Windows, Linux, and MacOS

Azure Data Box

This is similar to the Azure Import/Export service, but here the device itself sent to you for storing the data, which is a Microsoft provided appliance

Data Box – 100 TB

Data Box Disk – 8 TB

Data Box Heavy – 1 PB

Azure Data Factory

- This is a cloud service that can be used to perform ETL (Extract-Transform-Load), ELT (Extract-Load-Transform) and data integration projects
- In the Azure Data Factory service, you can author various types of activities

Key Components:

- Data Set

This is the source of your data. It can be an on-premises file server, SQL database server, Azure SQL database server. You define a linked service that is used to connect to the data source.

- Activity

You then define the activity. Examples of activities is ingesting data, cleaning data

- All of these activities then run as part of a pipeline