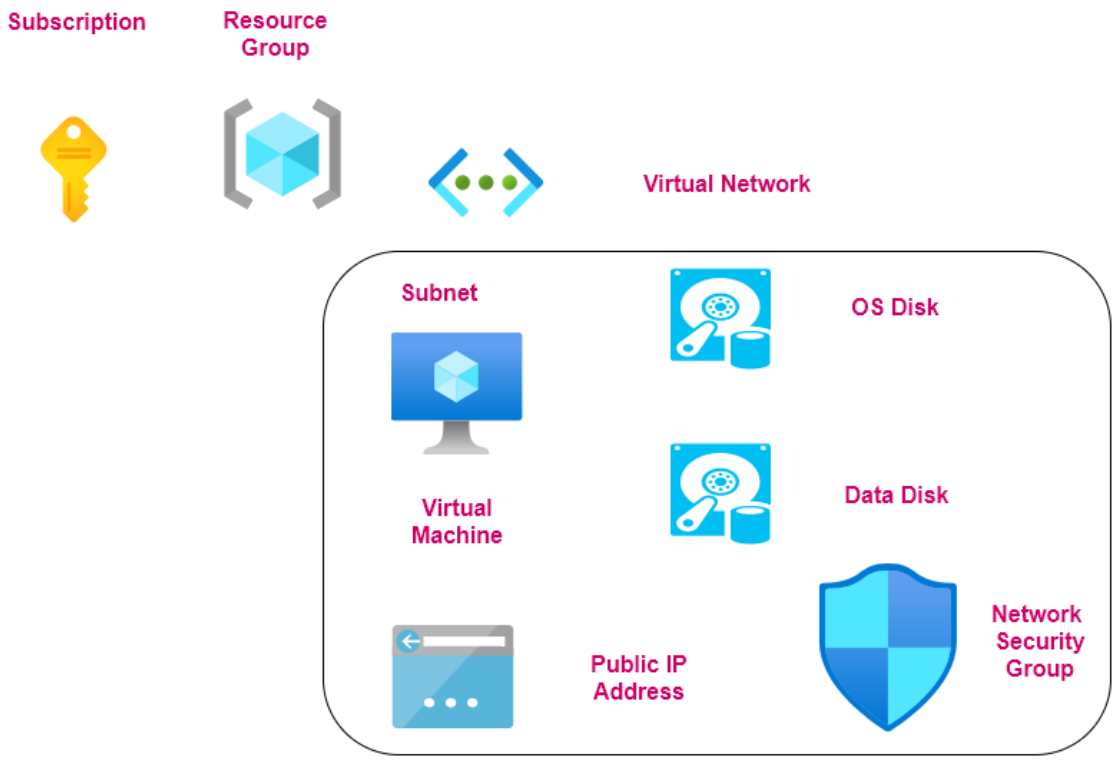
Deploy and Manage Azure compute resources

Deploying a virtual machine



State of the Virtual Machine

Disks

OS Disk - 127 GB

Managed Disk - Designed for high availability

Temporary disk - size varies depending on the instance size

Data on the temporary disk is lost during a maintenance event

Data is lost when you redeploy the VM

Restart / Stoping the VM

1. If you restart the VM, the public IP address will remain as it is. Also the data on the temporary disk remains as it is.

2. If you Stop/Deallocate the VM, the public IP address will be lost. The data on the temporary disk also gets erased.

Physical server

Physical server

Lab - Deploying a Linux machine - SSH keys

Azure Virtual Machine

Linux OS

SSH is an encrypted connection protocol

You can use SSH keys for a more secure connection

This is based on public-private key pair

The public key is stored on the VM itself

You get the private key which is then used to authenticate onto the Linux VM

Server-side encryption - Azure Disk Storage

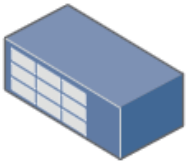
Server-side Disk Encryption

Here your data is automatically encrypted using 256-bit AES Encryption

This protects the data at rest

This is done for Managed disks - OS and data disks

Storage Unit - Azure Data Center



Disks - Understanding IOPS and Throughput

IOPS - This setting defines the number of Input/Output operations per second

Disk SKU ⓘ

Premium SSD

Size	Disk tier	Provisioned IOPS	Provisioned thro...
4 GiB	P1	120	25
8 GiB	P2	120	25
16 GiB	P3	120	25
32 GiB	P4	120	25
64 GiB	P6	240	50

Throughput - Amount of data that is being sent to the storage disk at a specified interval

Videos are larger in size

Measured in MB per second

Disk SKU ⓘ

Premium SSD

Size	Disk tier	Provisioned IOPS	Provisioned thro...
4 GiB	P1	120	25
8 GiB	P2	120	25
16 GiB	P3	120	25
32 GiB	P4	120	25
64 GiB	P6	240	50
128 GiB	P10	500	100

Azure Shared Disks

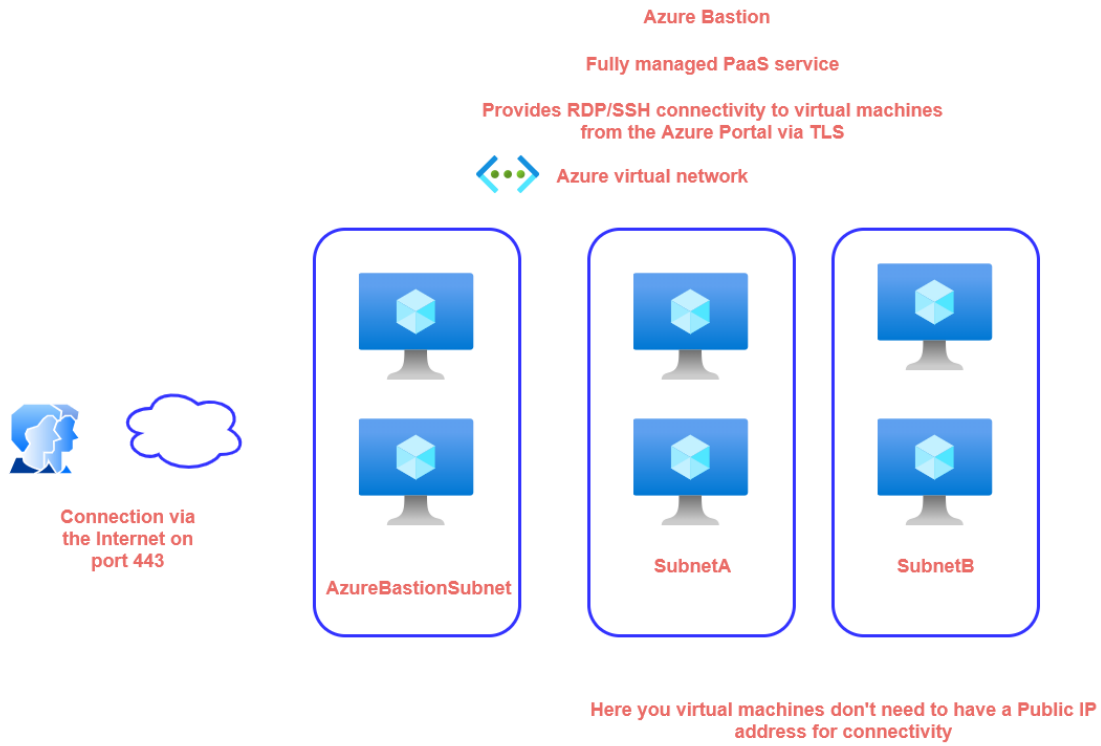
Azure share disks - This allows a managed disk to be attached to multiple virtual machines

Clustered SQL Server workload

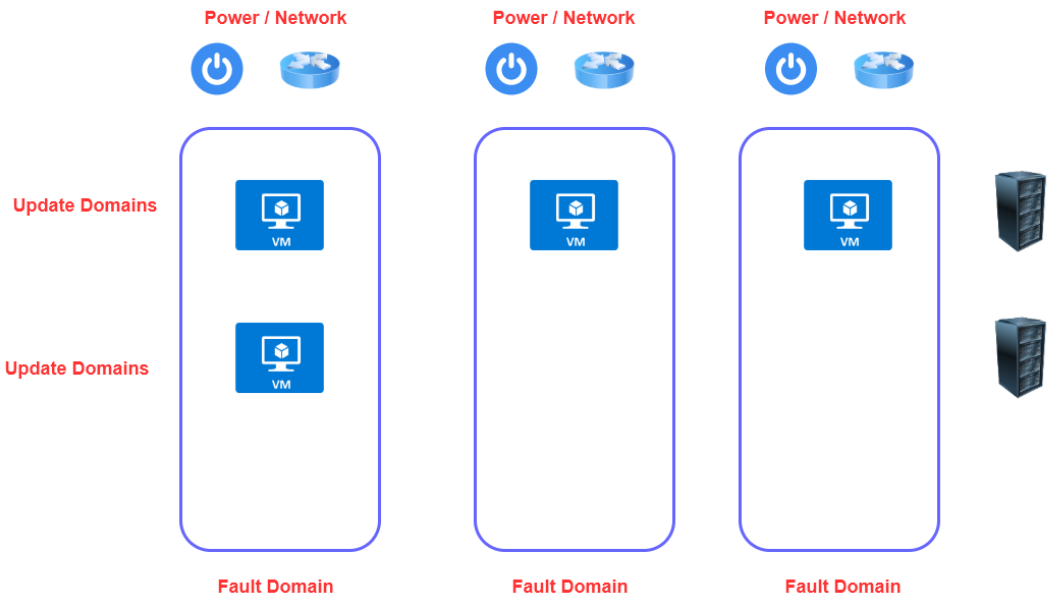
There are restrictions

Can only be enable for Premium and Ultra disks

Azure Bastion Service



Availability Sets



If you have two or more instances deployed in the same Availability Set , you will get an SLA of 99.95% for Virtual Machine Connectivity to at least one instance

Use case scenario - Availability sets

You have to move an on-premises application onto an Azure subscription.

The application will be hosted on several Azure virtual machines.

You have to ensure that the application will always be running on at least four virtual machines during a planned Azure maintenance period.

Availability Sets vs Availability Zones

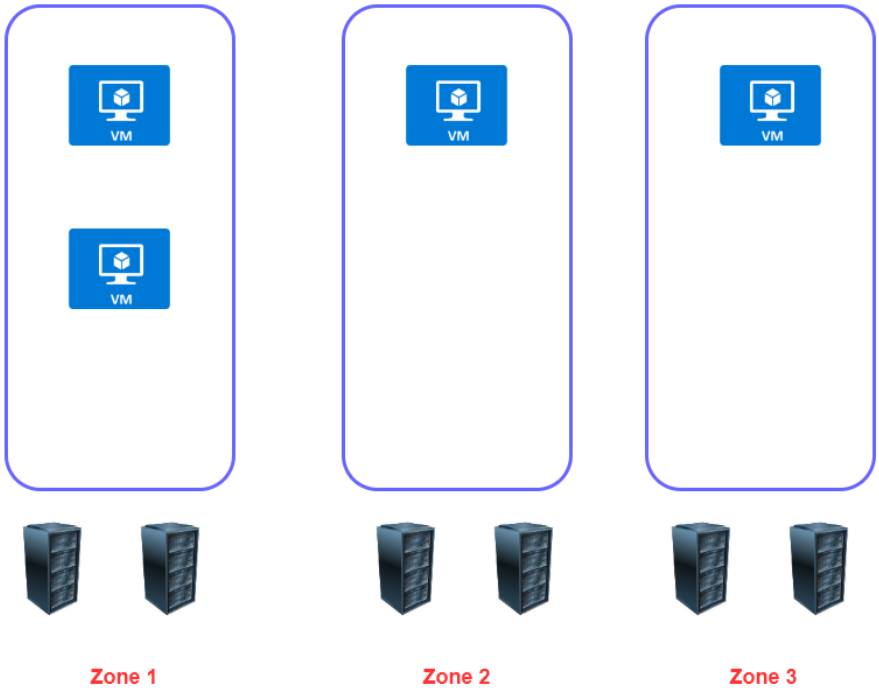
Azure maintenance period - Update domains

Faults to the underlying hardware - Fault domains

Availability Zones

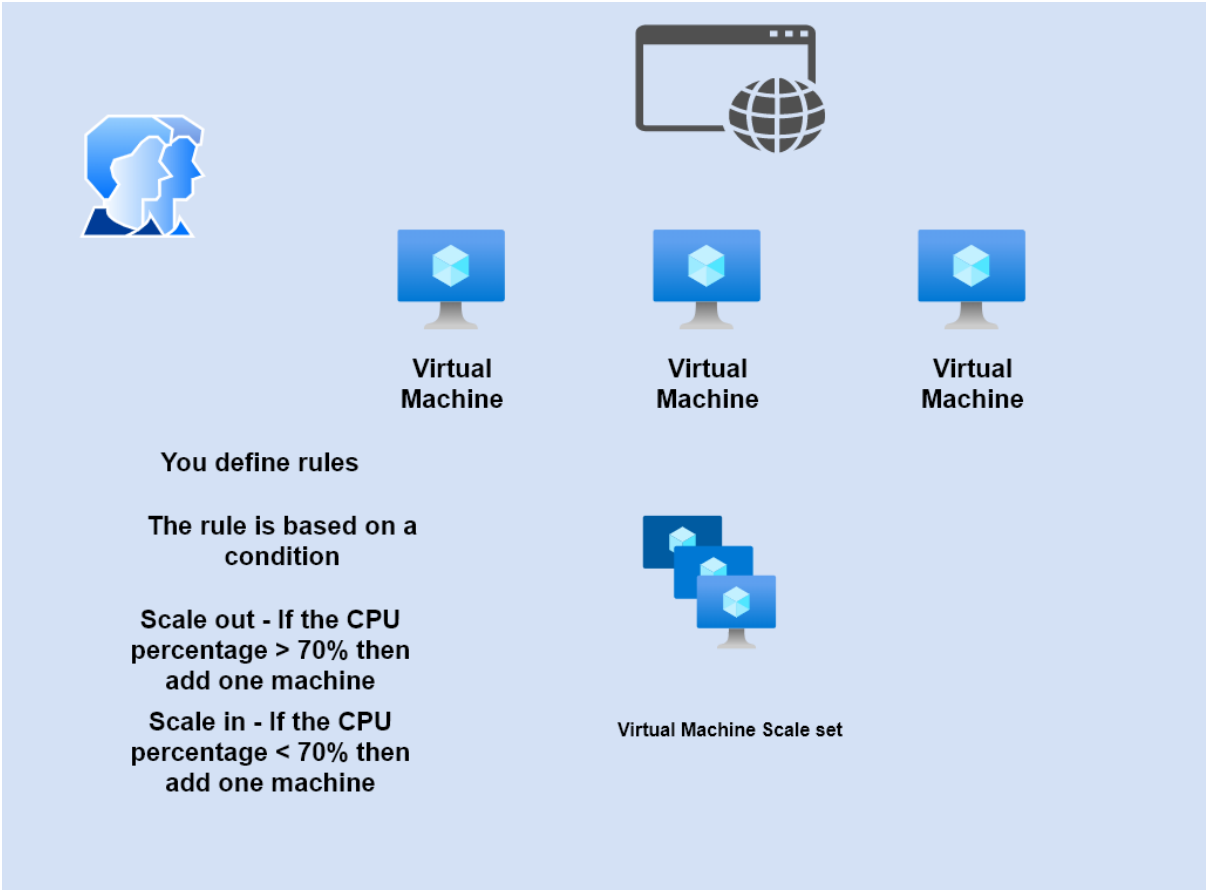
Availability Zones are unique physical locations that are equipped with independent power, cooling and networking.

There are normally three Availability Zones in a region



If you have two or more instances deployed in the same Availability Zone , you will get an SLA of 99.99% for Virtual Machine Connectivity to at least one instance

Azure virtual machine scale sets



Understanding virtual machine images

Image

Data

Application installed

Create an image

Image - This is a copy of the full VM which inlcudes the data disks or just the OS disk

You can create an image and place as part of an Azure compute gallery

You can share the Azure compute gallery across your organization so that other users can create VM's based on the images stored in the gallery

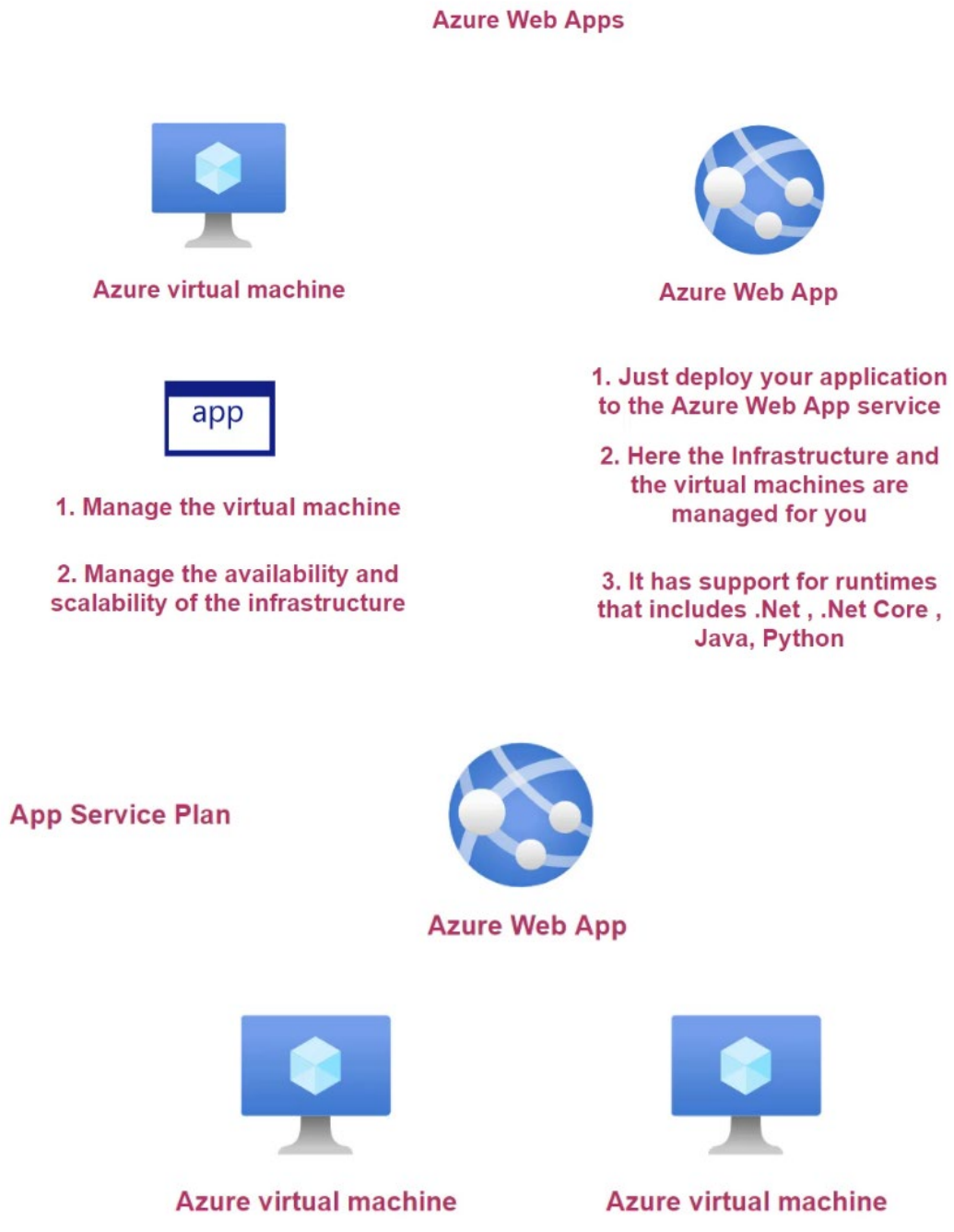
Image Definition - This is a grouping of image versions. Each image definition has information about why the image was created and other information related to the image.

Image Version - This is used to create the VM.

Two types of images that you can create

Specialized VM Images	Generalized VM Images
Here information about specific users and machine information is retained	Here information about specific users and machine information is removed
So new VM's created out of the image will have the same computer name and admin user information	Here you have to perform the process of generalization. The original VM is unusable after you perform this process

Azure Web App



Azure Web Apps - Deployment Slots

Deployment Slots

Staging Environments for App Service Plans

Version 1

Version 2

Production Slot

Staging slot

Standard , Premium and Isolated App Service Plan

Applications in deployment slots have their own host names

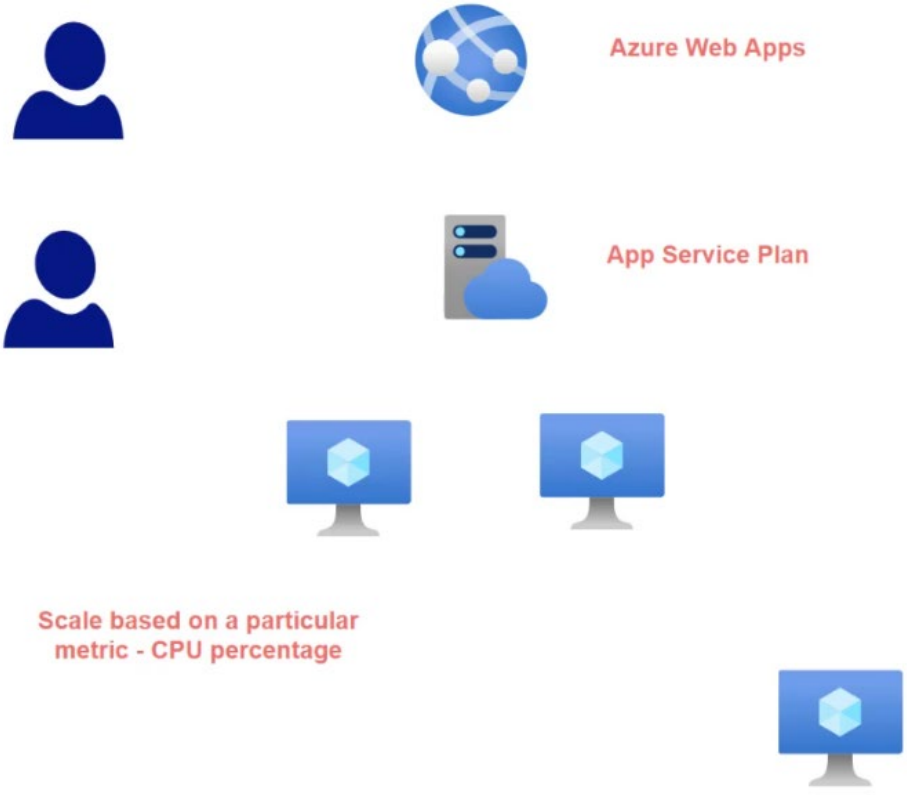
1. You have the chance to validate all application changes in the staging deployment slot

2. You can then swap the staging slot with the production slot

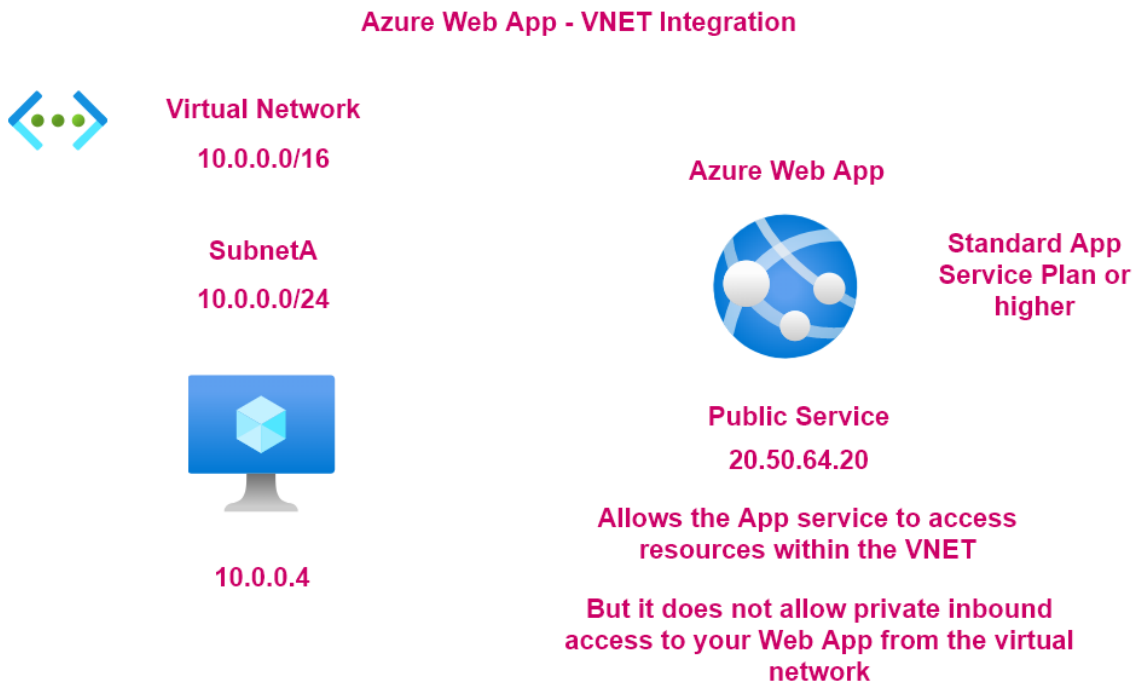
3. This helps eliminate the downtime for your application when new changes are deployed

4. You can also easily roll back the changes

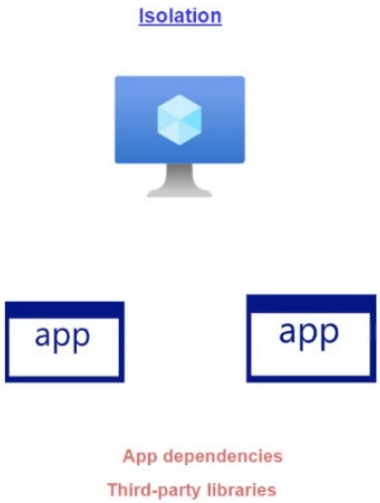
Azure Web Apps - Autoscaling



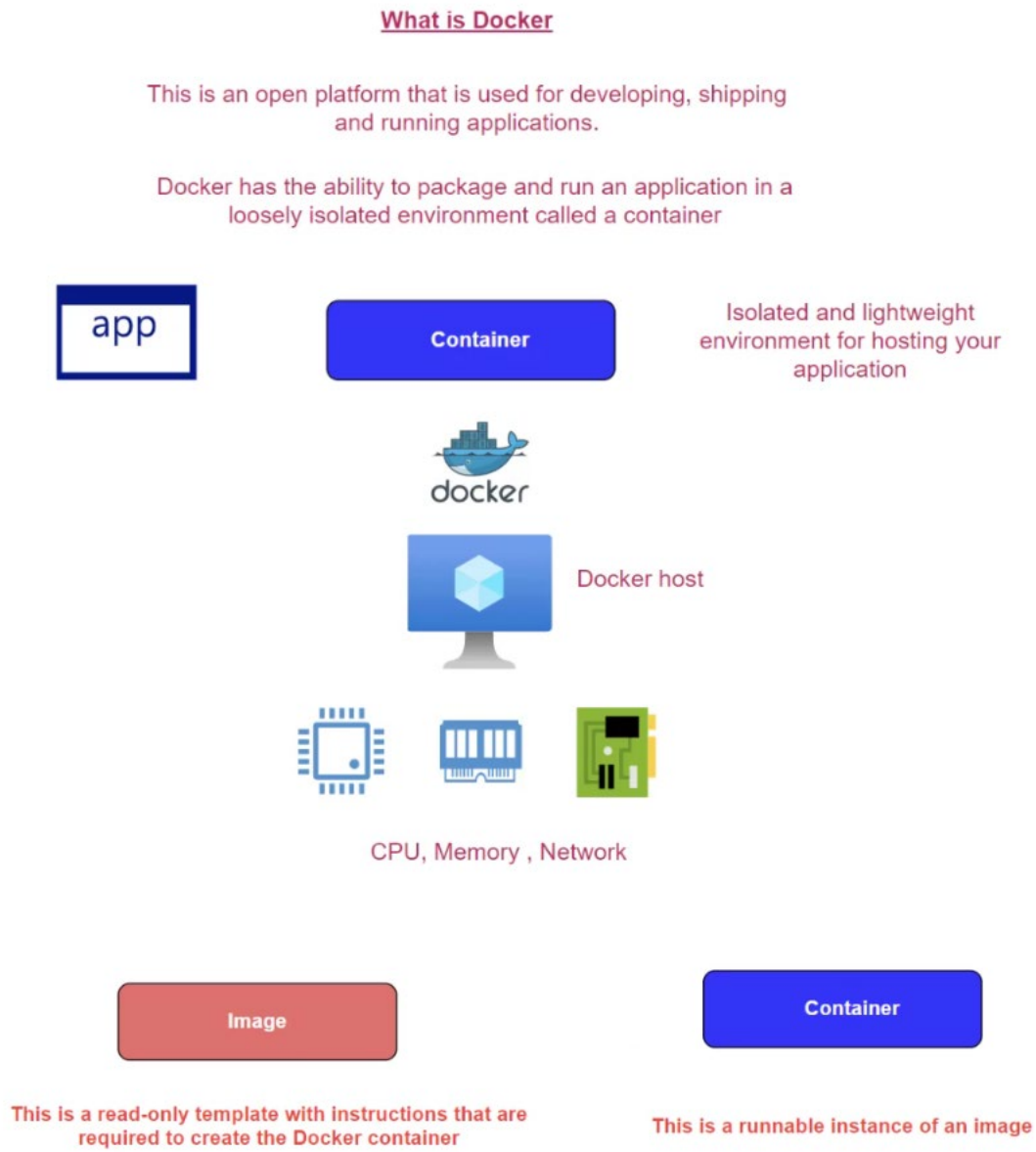
Azure Web App - Virtual Network Integration



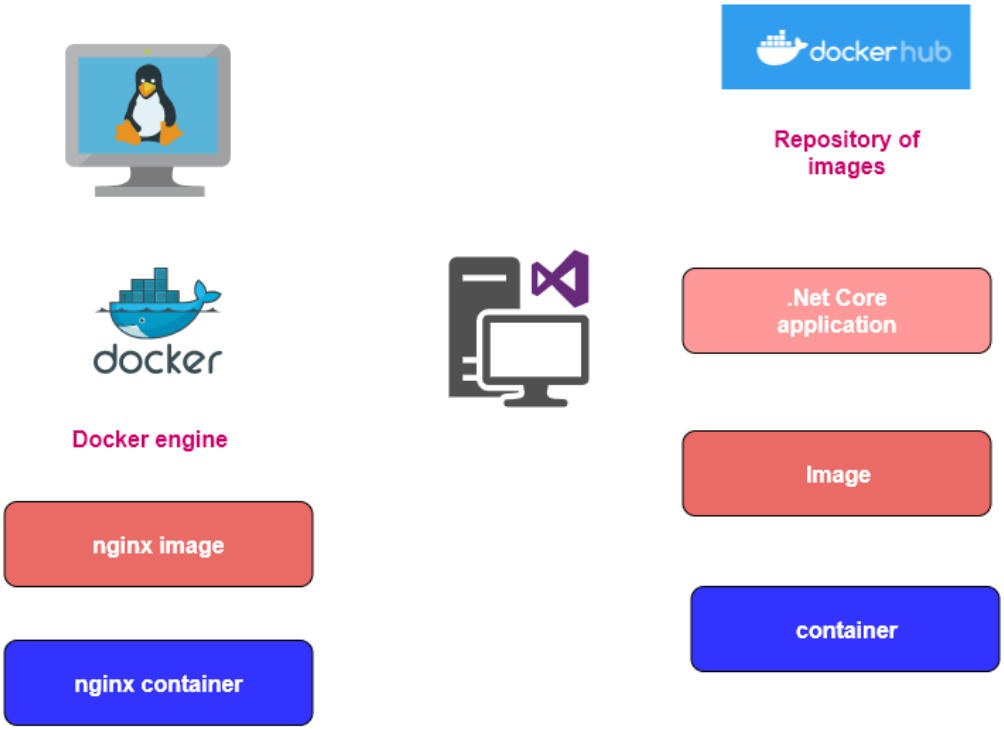
The need for containers



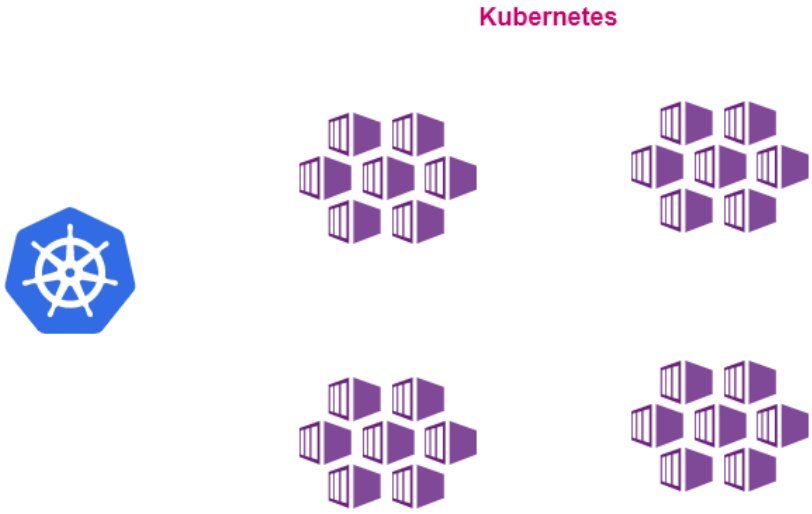
Introduction to Docker



The need for an image registry

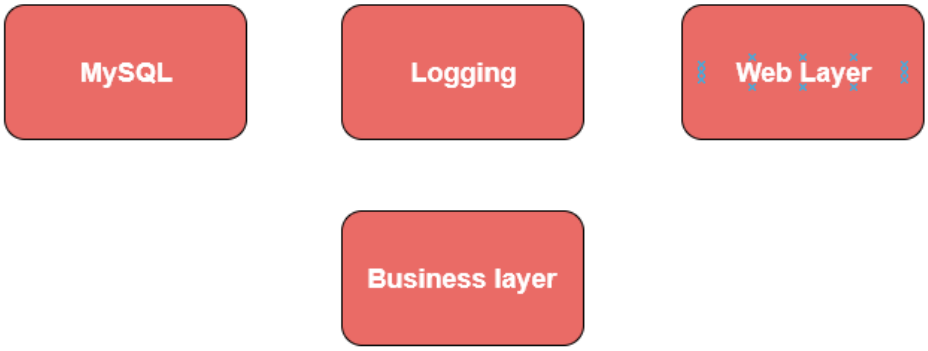


Primer on Azure Kubernetes



Azure Kubernetes - Managed service for Kubernetes on Azure

Kubernetes is used to orchestrate your containers for hosting your applications



Kubernetes cluster

Kubernetes cluster

All calls to the cluster

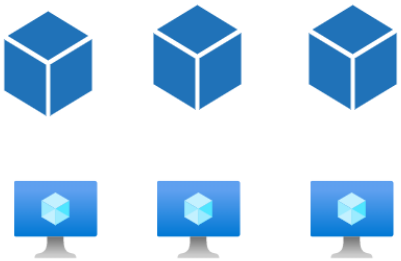
apiserver

etcd - Cluster store

State of the cluster

master node

Nodes - These are used for hosting your containers



The master node is used to control the nodes in the cluster

Node

kubelet - This is a kubernetes agent that runs on the node.

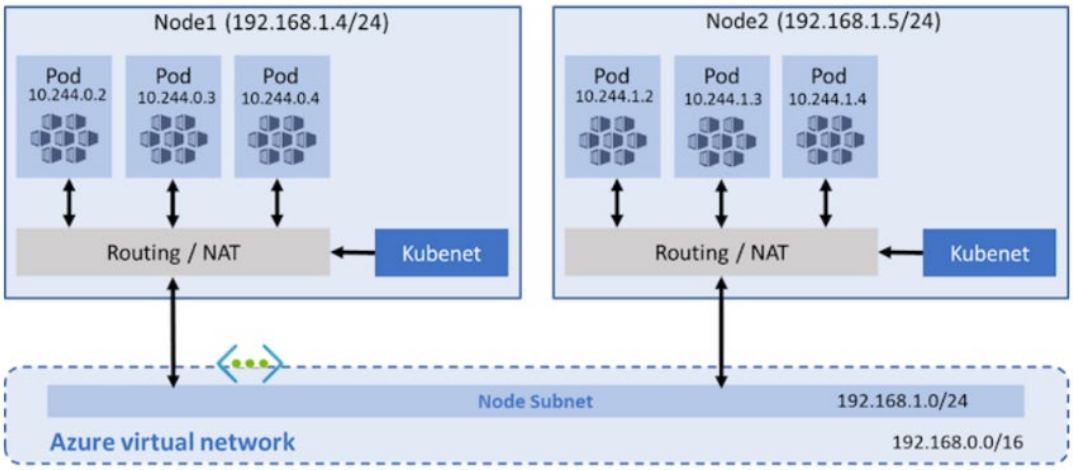
kubelet - It registers the node with the master node

kubelet - Will take commands from the master node for the deployment of containers

Container runtime - This is used to actually taking the images and deploying the containers on the node

Kube-proxy is used for managing the networking aspects for the containers

Azure Kubernetes - Configuring networking



https://docs.microsoft.com/en-us/azure/aks/configure-kubenet

Nodes receive an IP address from the Azure virtual network

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

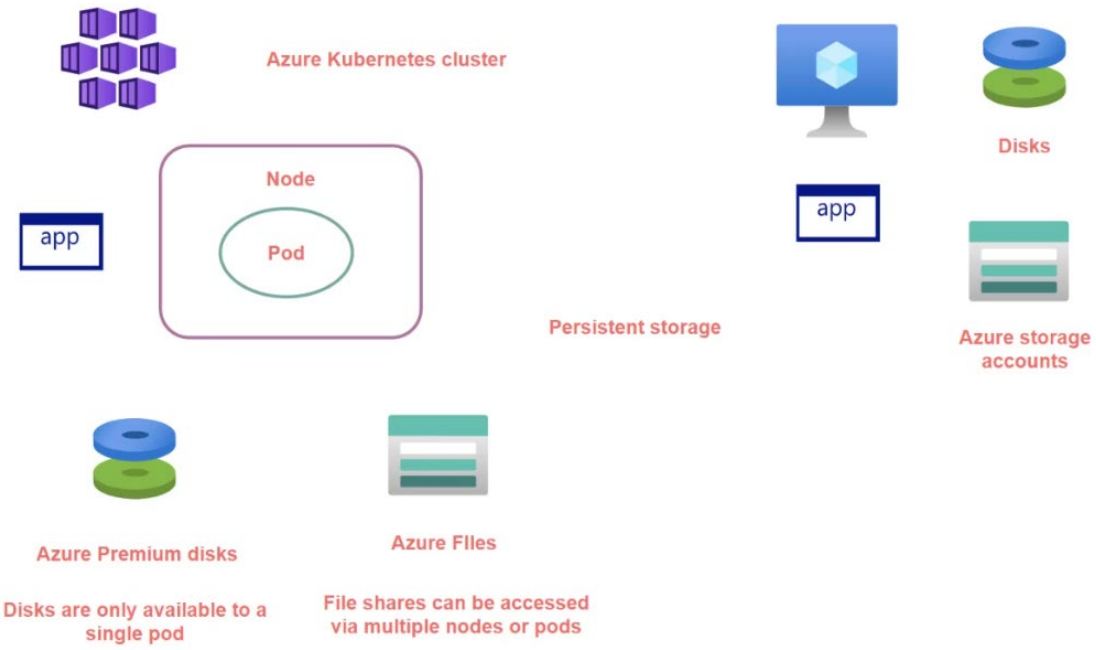
Network Address translation is then used

Azure Container Networking Interface

Every pod gets an IP address from the subnet and can be accesed directly

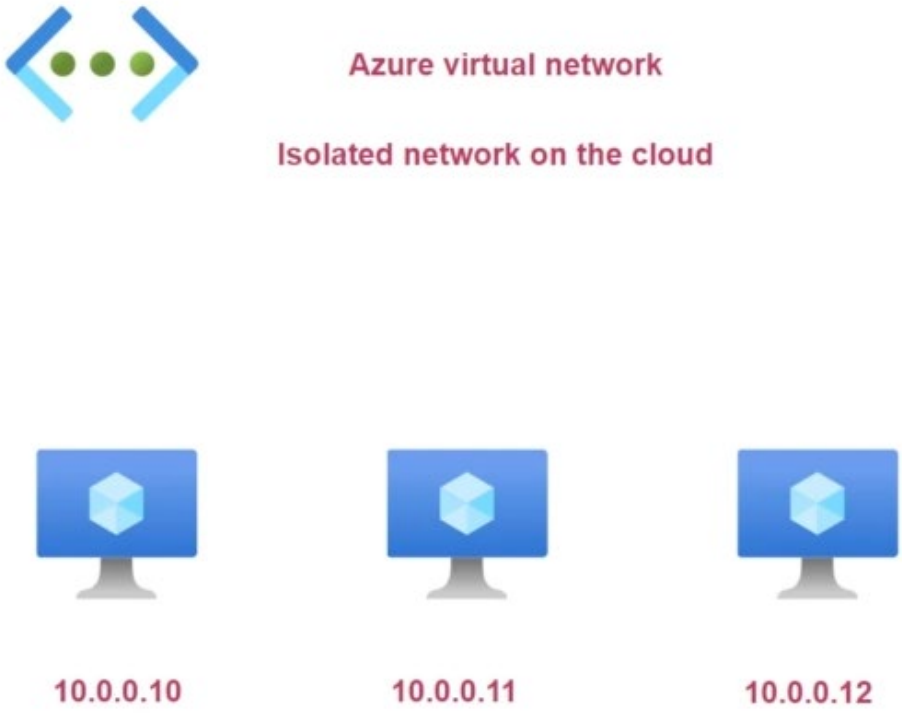
This could also lead to an IP address exhaustion

Lab - Azure Kubernetes - Configuring storage – Disks

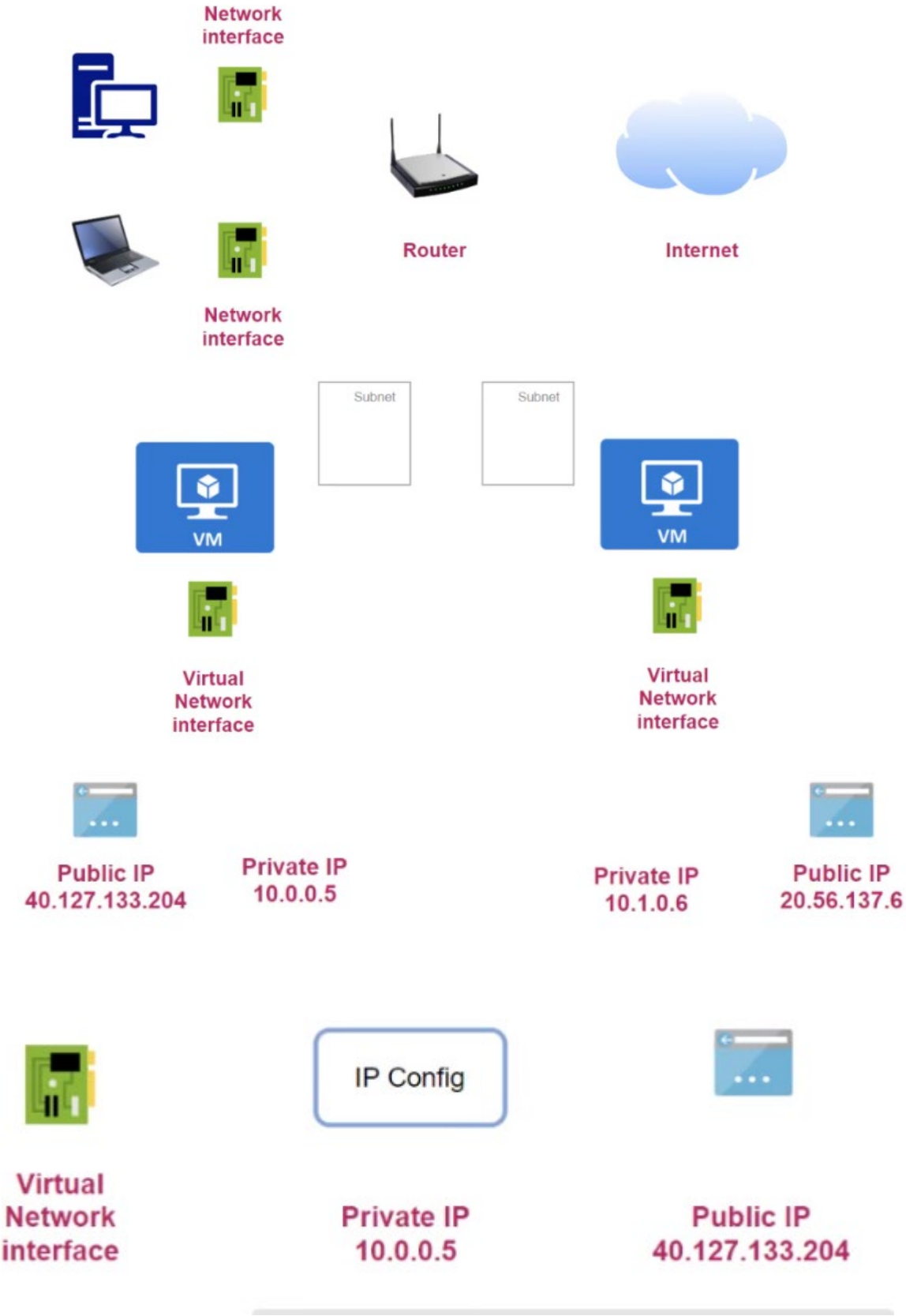


Configure and manage virtual networking

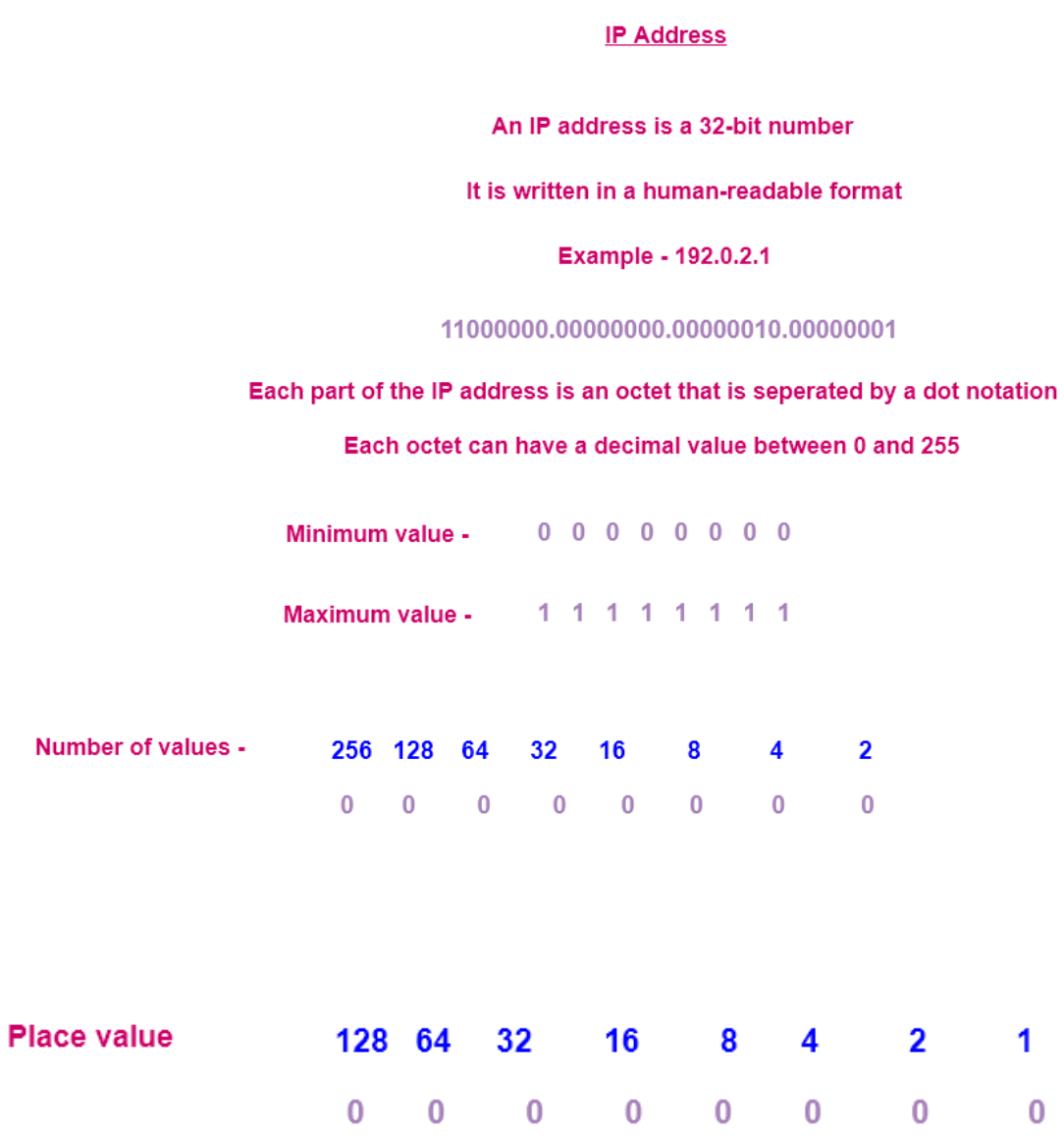
Introduction to Virtual Networks in Azure



The network interface



Quick note on address spaces



The CIDR Notation

Network and host ID

An IP address is also associated with a subnet mask

The subnet mask is used to distinguish between the network and the host id

Example - 192.0.2.0

Subnet mask - 255.255.255.0

Here 192.0.2.0 is the network id

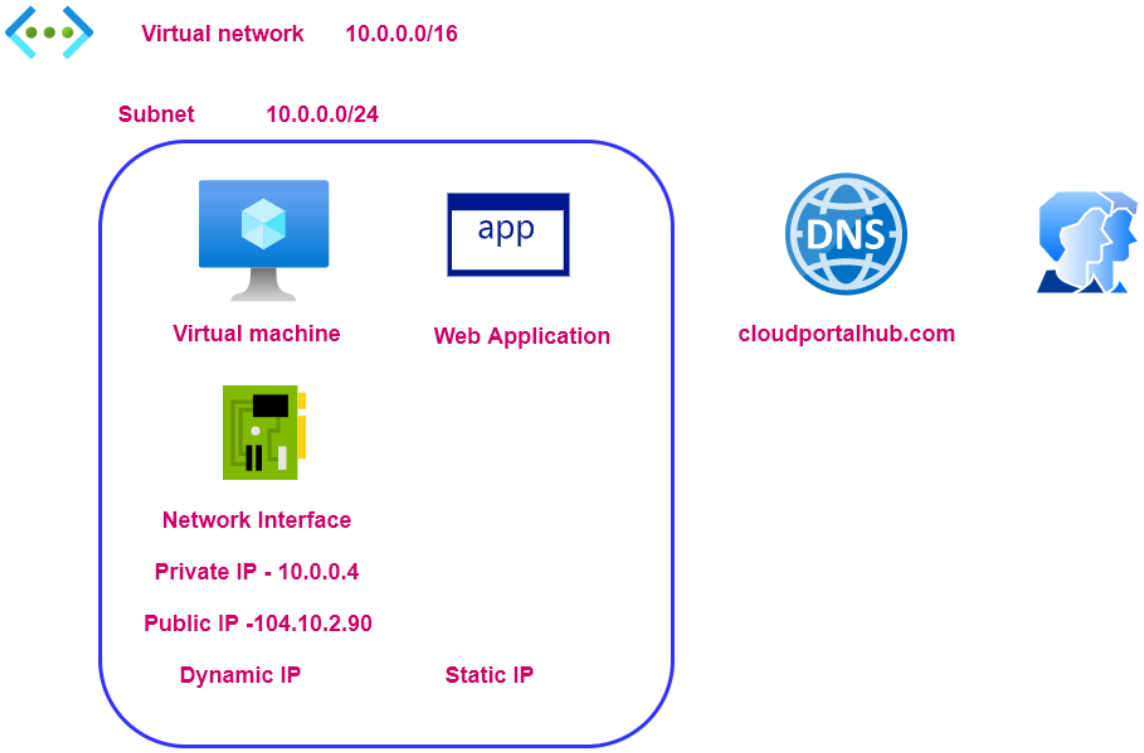
192.0.2.1 192.0.2.2 192.0.2.3

Here you get 256 total number of hosts

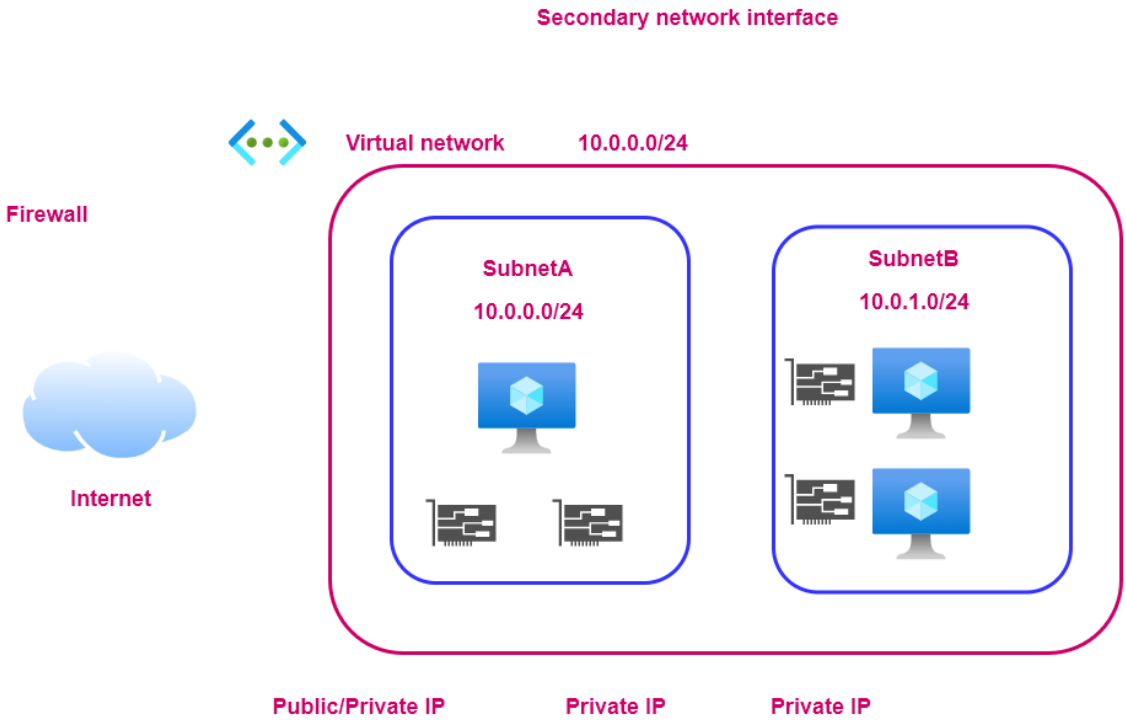
The number of usuable IP addresses is 254

192.0.2.0 is the network id and 192.0.2.255 is the broadcast id

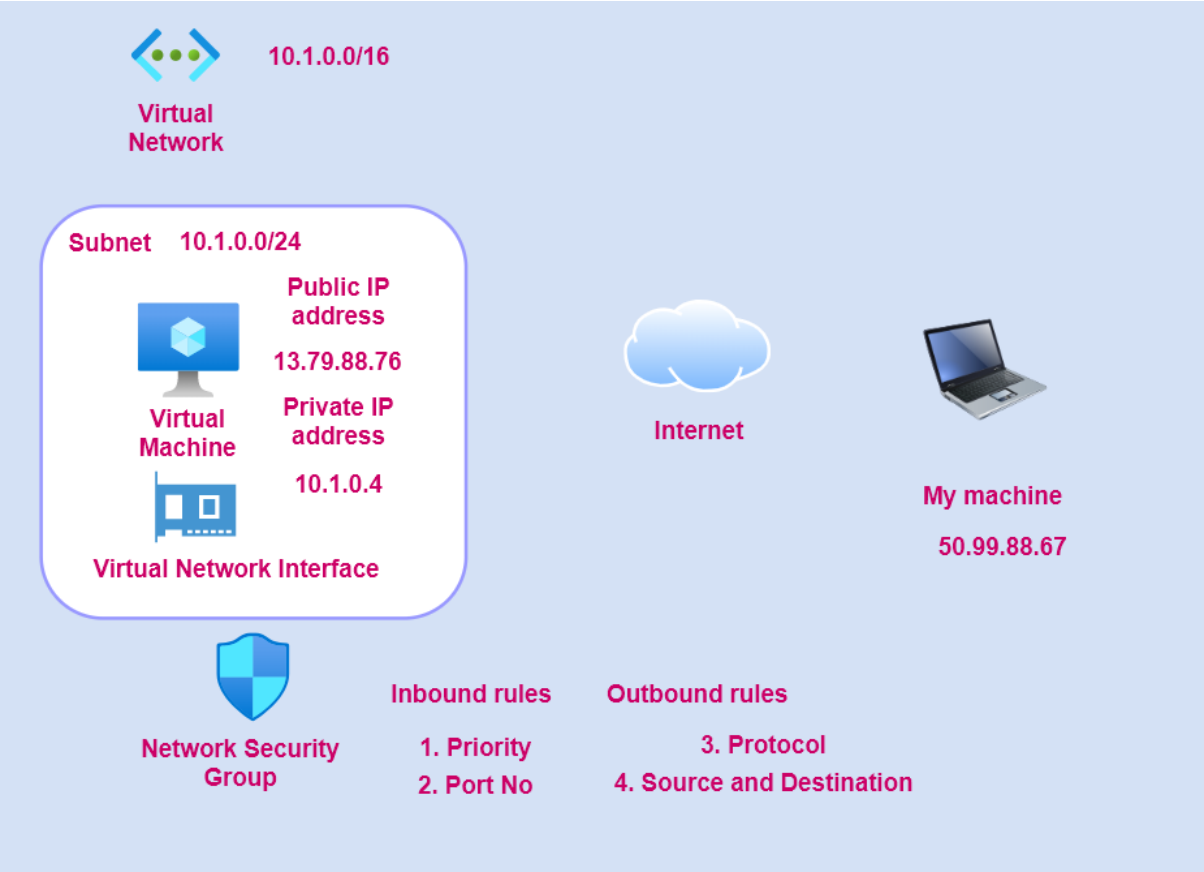
Static IP Address



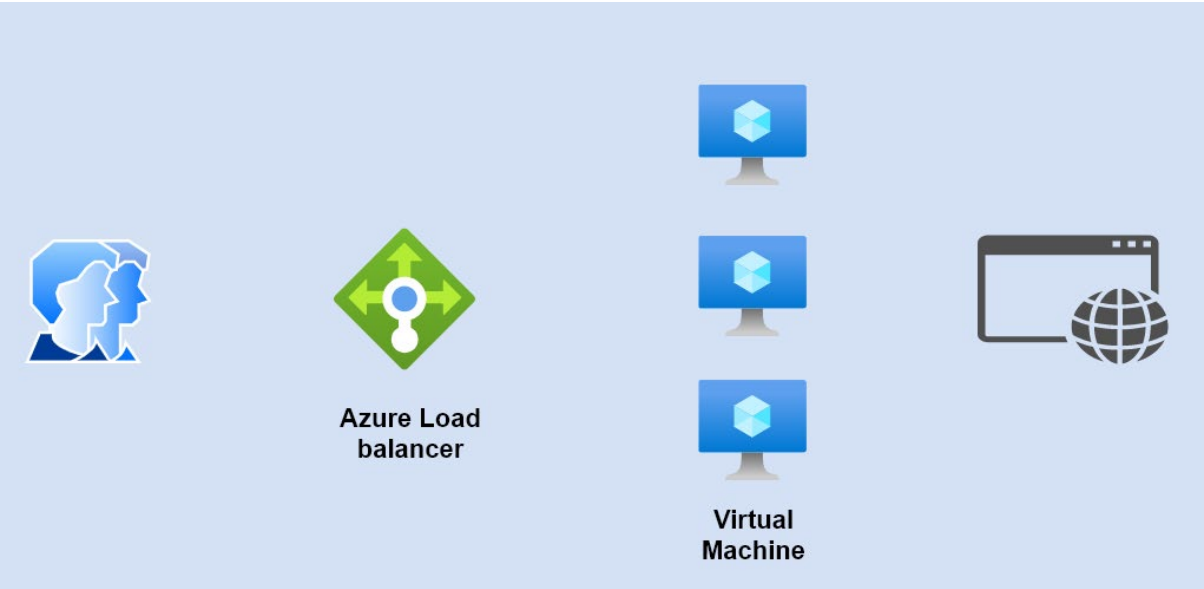
Attaching a secondary network interface



Network Security Groups



The Azure Load Balancer Service



Azure Load Balancer and SKU's

Load Balancer

Virtual Network

Public IP address

If you want to have an internet facing load balancer

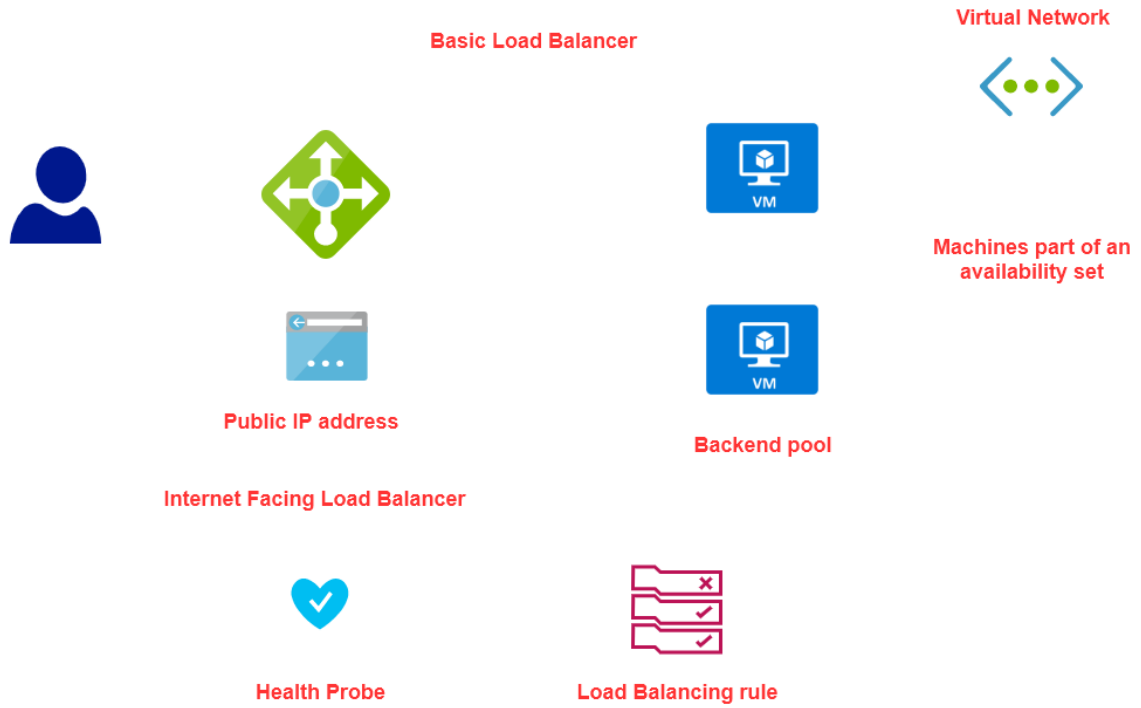
Backend pool

Health Probe

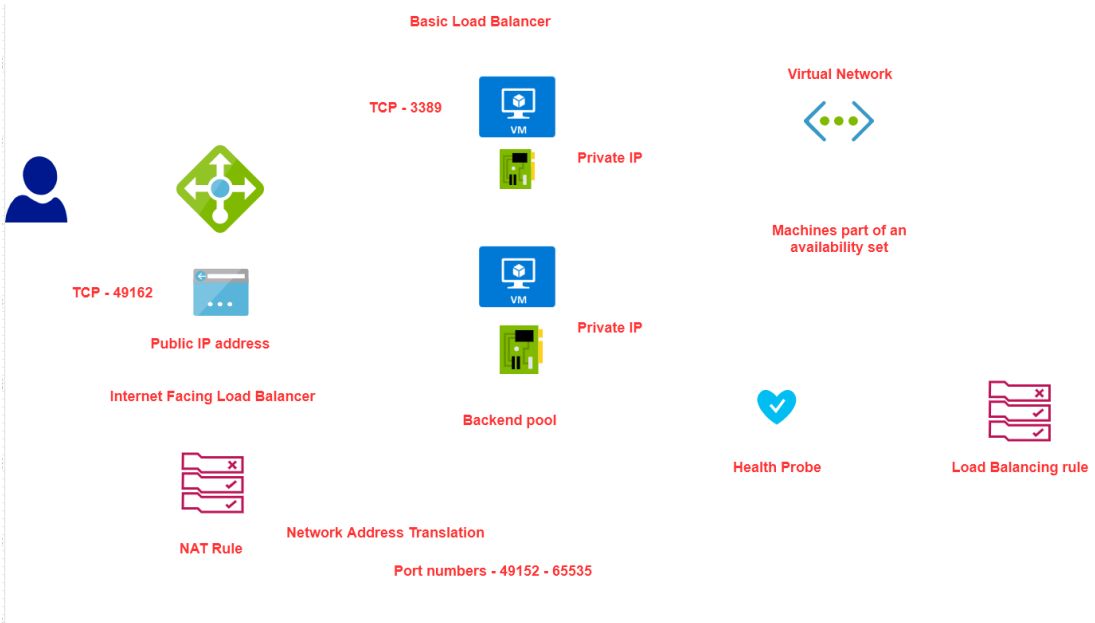
Load Balancing rule

Basic Load Balancer	Standard Load Balancer
Free	Charge per hour
The machines in the backend pool need to be part of an availability set or scale set	Here the machines can also be indepedent machines that are part of a virtual network
Health probes - TCP, HTTP	Health probes - TCP, HTTP, HTTPS
No support for Availability zones	Support for Availability zones
No SLA	SLA of 99.99%

Lab - Basic Load Balancer – Setup



Lab - Basic Load Balancer - NAT rules



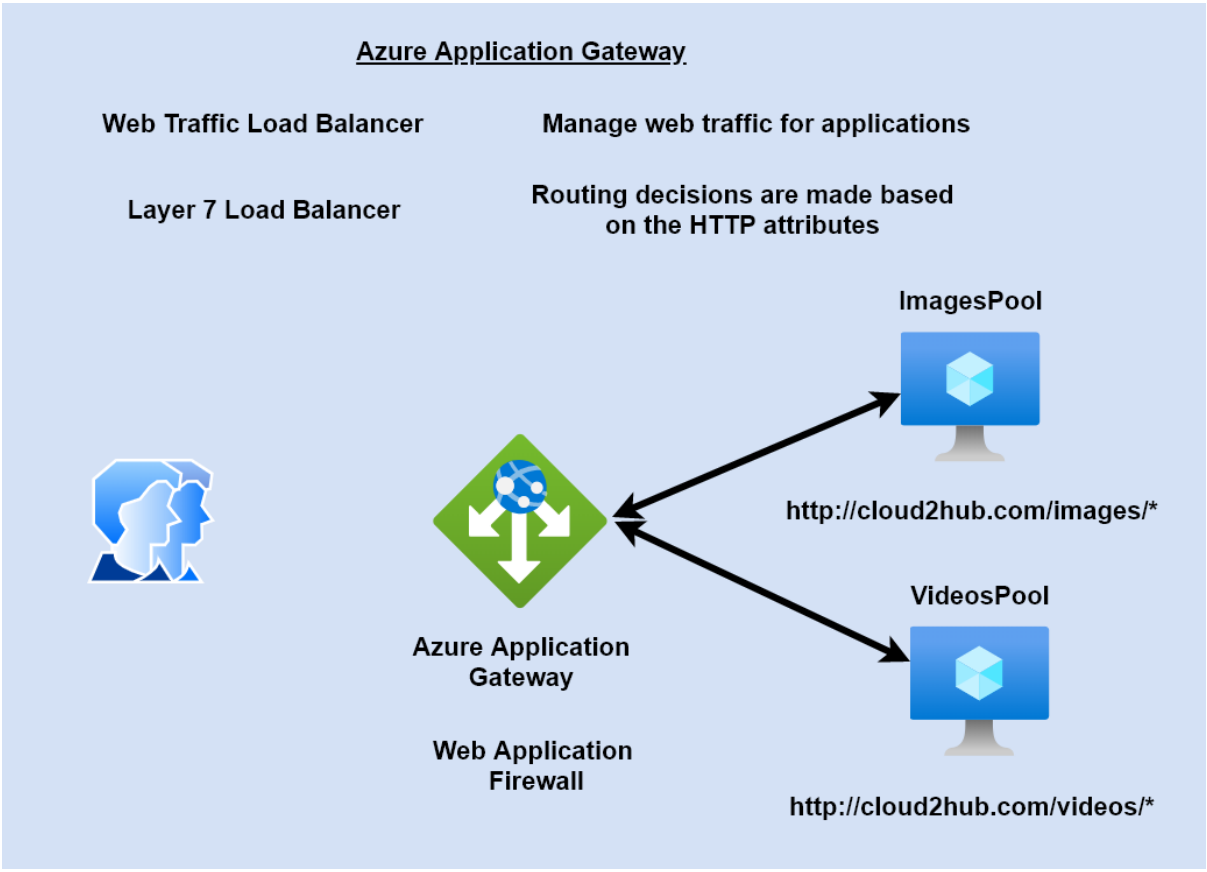
Load Balancer - Session Persistence

The Load balancer will create an affinity between the Load Balancer and the client for a session

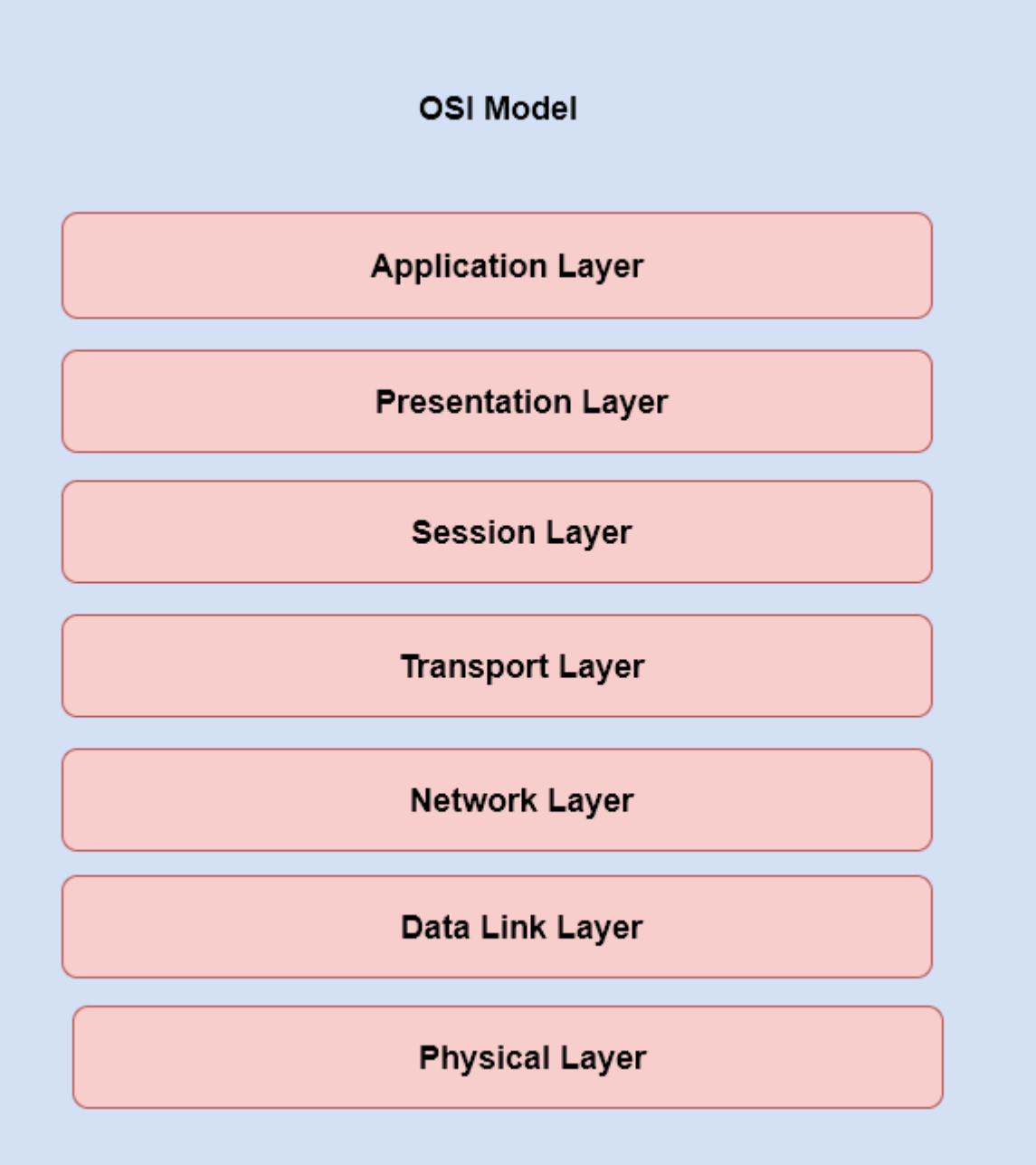
Advantage - Can help in better performance for sessions

Disadvantage - If too many sessions are persisted on a server.

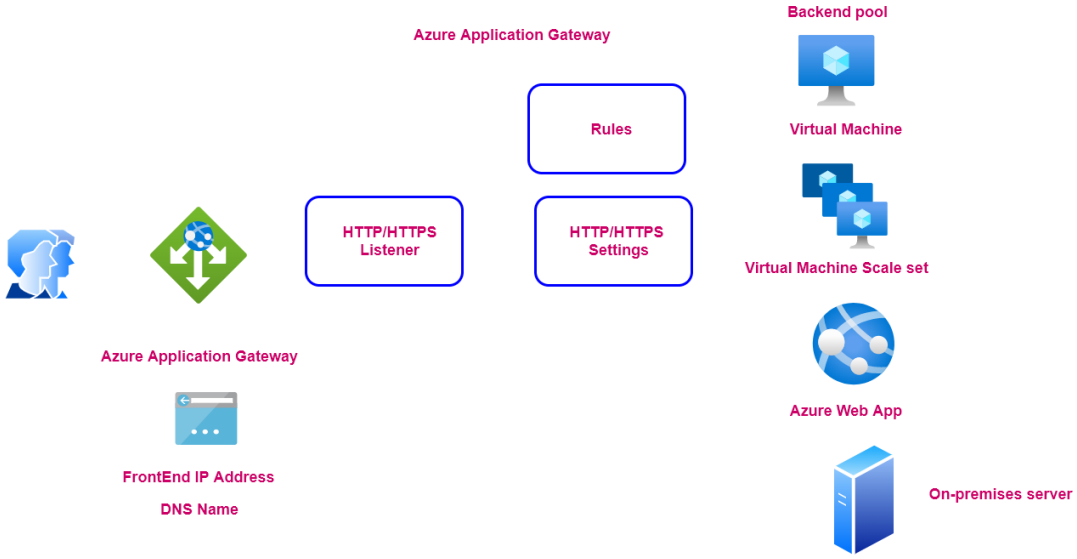
Azure Application Gateway



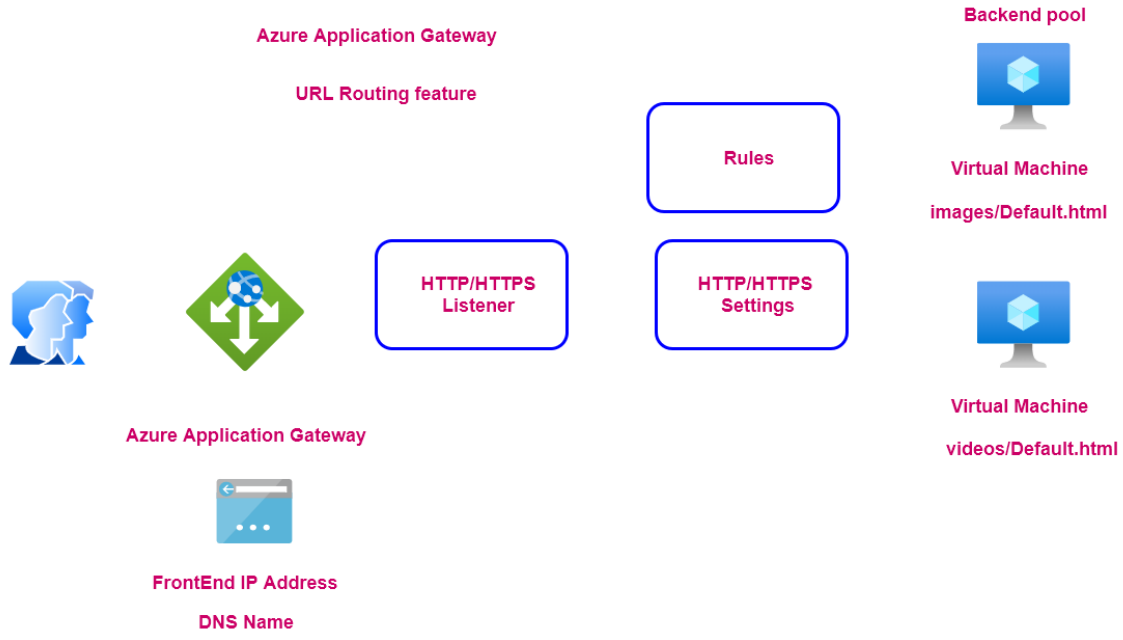
Open Systems Interconnection Model



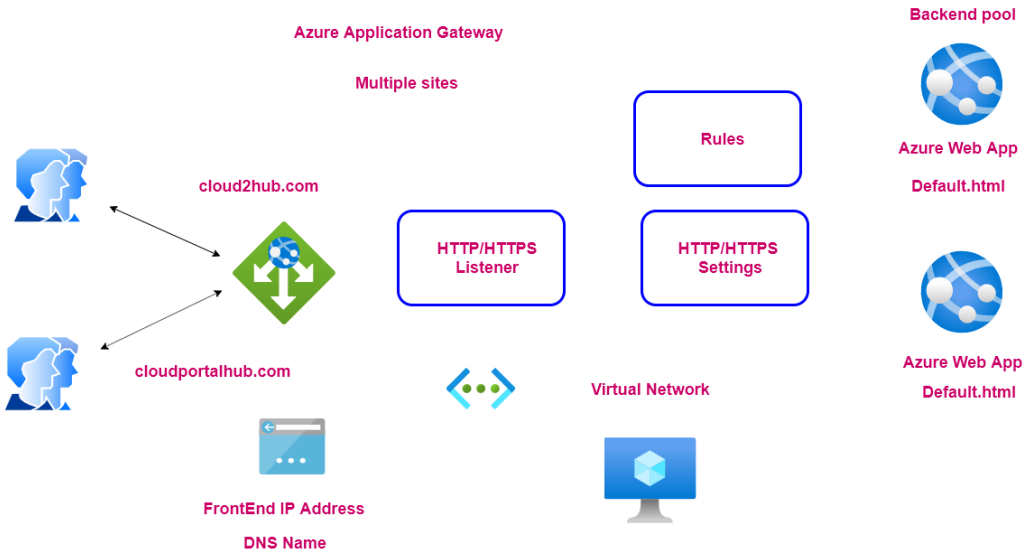
Azure Application Gateway – Components



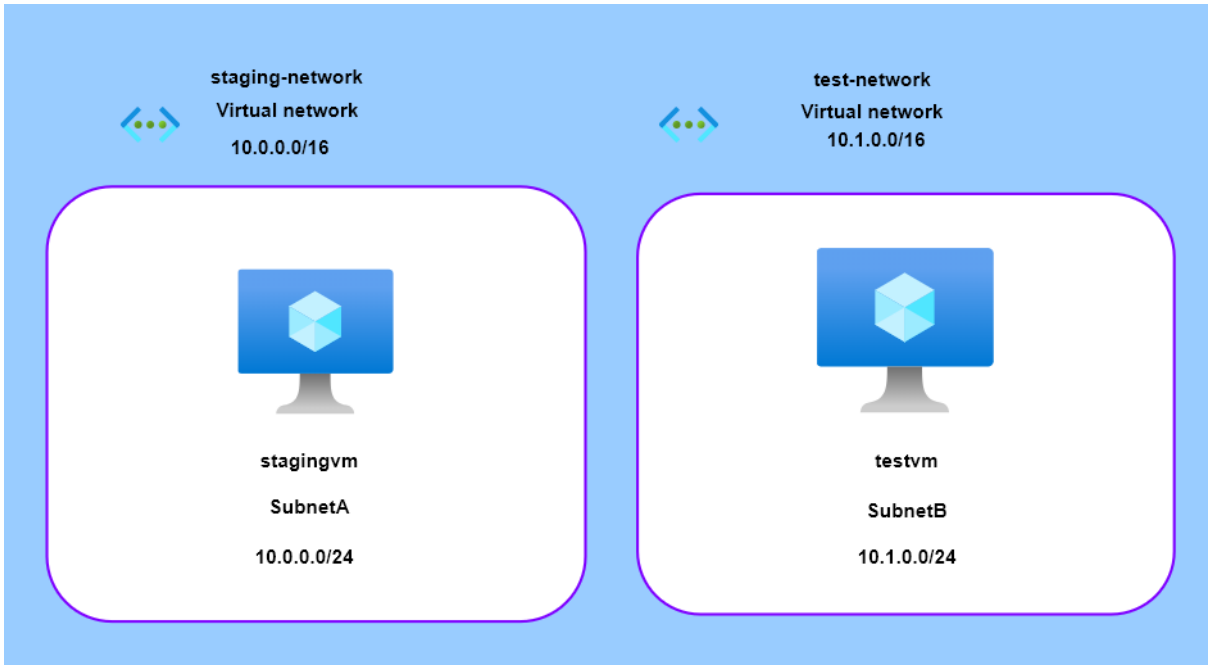
Lab - Azure Application Gateway - URL Routing – Setup



Lab - Azure Application Gateway - Multiple Sites – Setup



Virtual Network Peering



What is a Virtual private network

VPN - Virtual Private Network

Internet

Your Internet Services provider will know all of the requests that are made from your machine onto the Internet

Sometimes privacy can always be a concern

VPN is used to create a private network

Here your public IP address is not placed in the requests that are made onto the Internet

Also VPN connections are encrypted so that the data transfer is more secure

VPN server

Internet

Point-to-Site VPN Connections

10.0.0.0/16

GatewaySubnet

10.0.1.0/24

default

10.0.0.0/24

10.0.0.4

The gateway subnet is used to host gateway VM's and services

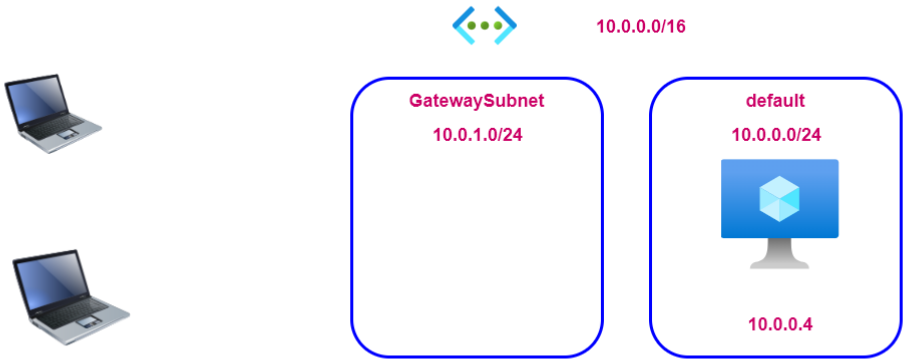
The VM's in the gateway subnet are configured with the required VPN gateway settings

No other VM's must be deployed to the gateway subnet

The gateway subnet can be configured as /29, but Microsoft recommends /27, /26

Next Step

Authentication via certificates



Root certificate

Self-Signed Root certificate

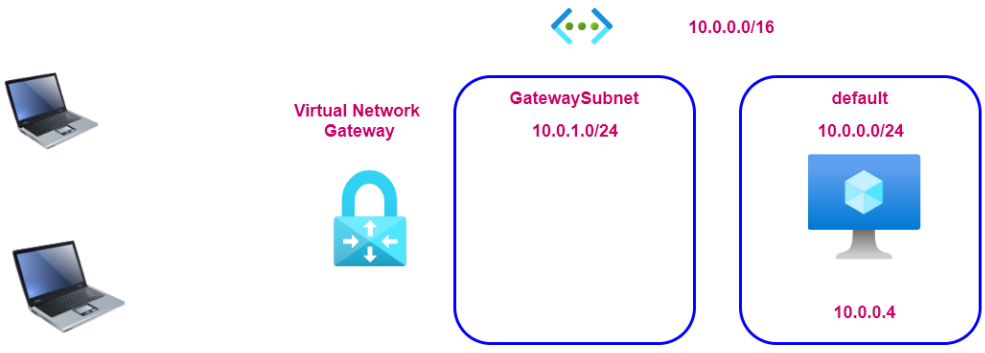
Self-Signed Root certificate

Client certificate

Enterprise CA authority

Next Step

Point-to-Site configuration



Root certificate

Client certificate

Self-Signed Root certificate

Virtual Network Gateway

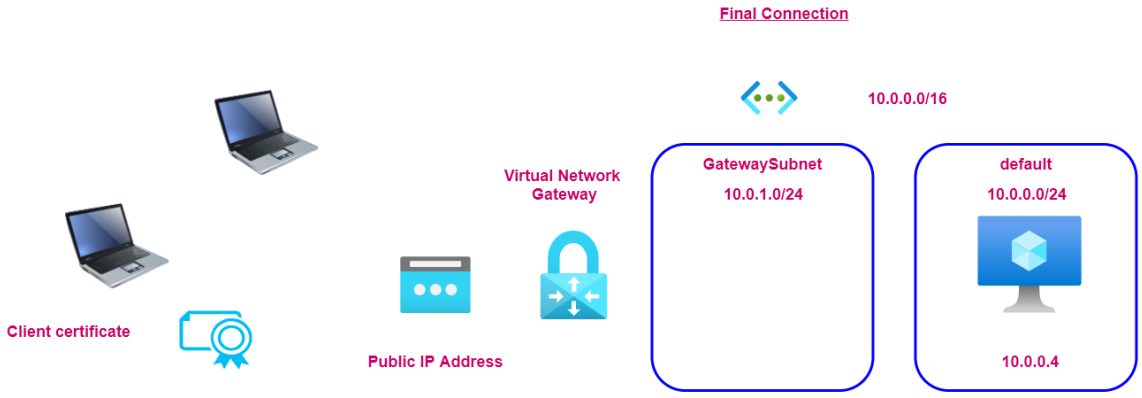
Point-to-Site configuration

IP Address range

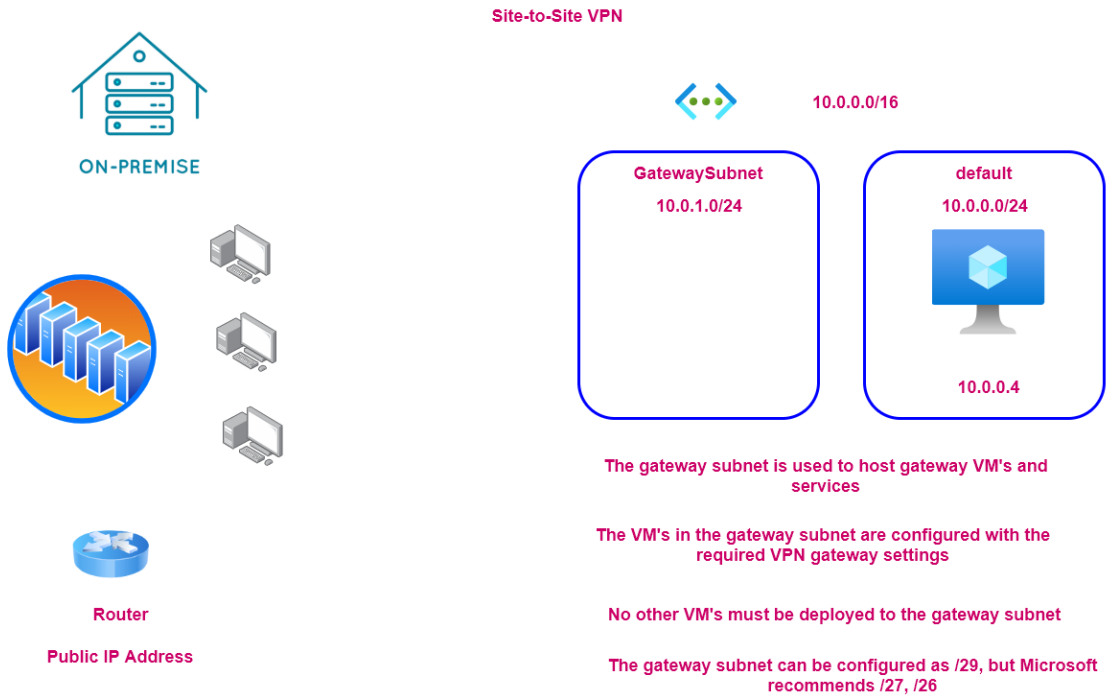
Tunnel type

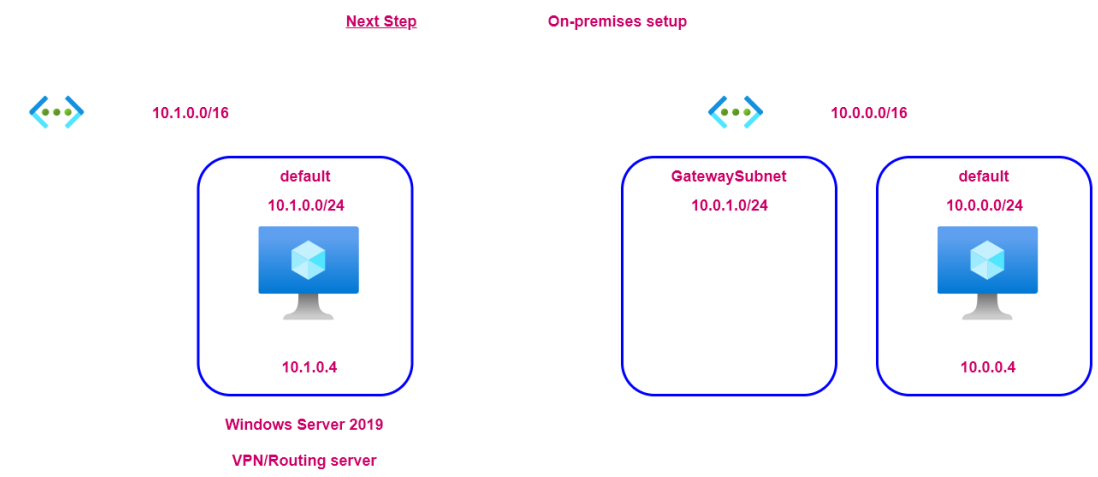
Authentication type

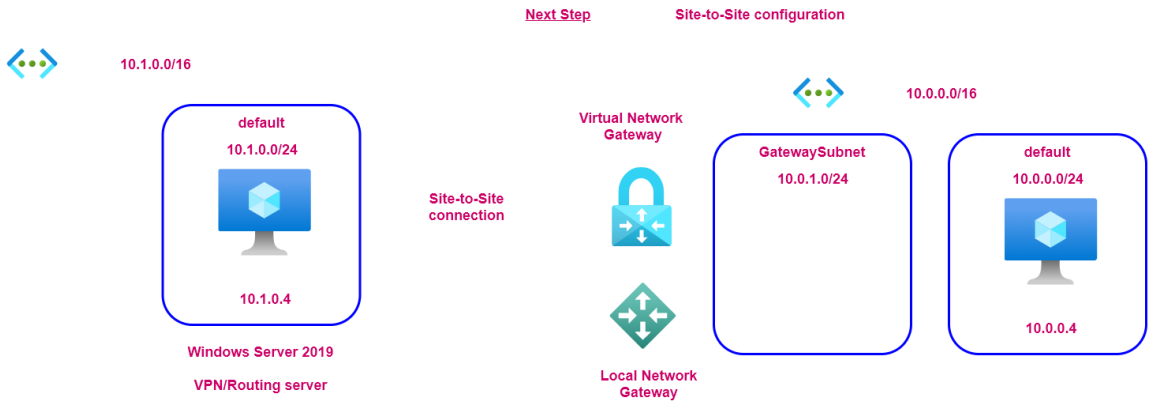
Upload the root certificate public key



Site to Site VPN Connection

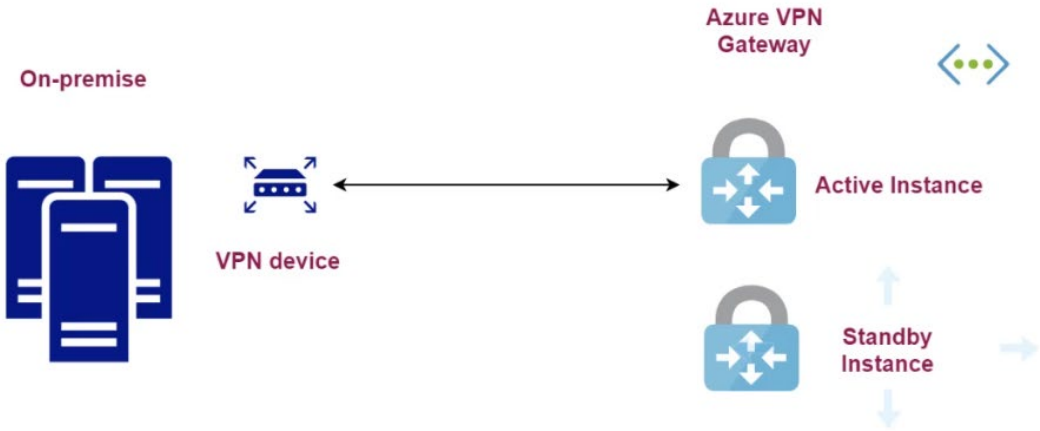


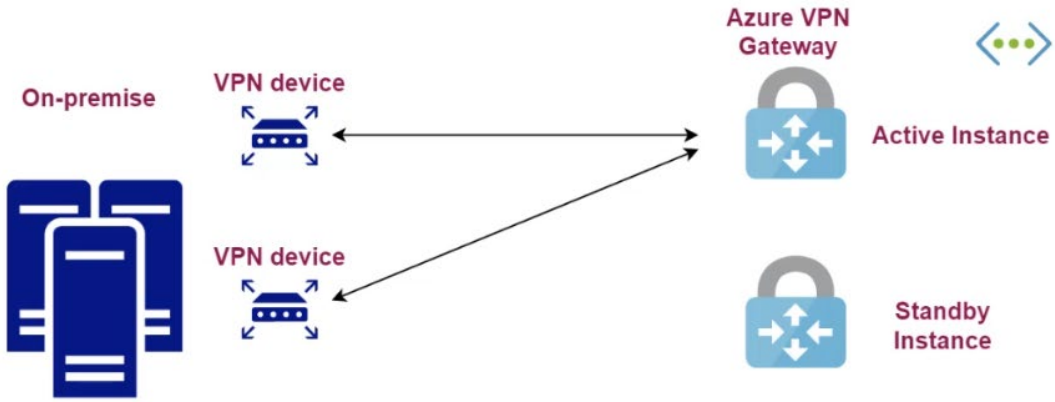




Azure VPN Gateway - High Availability

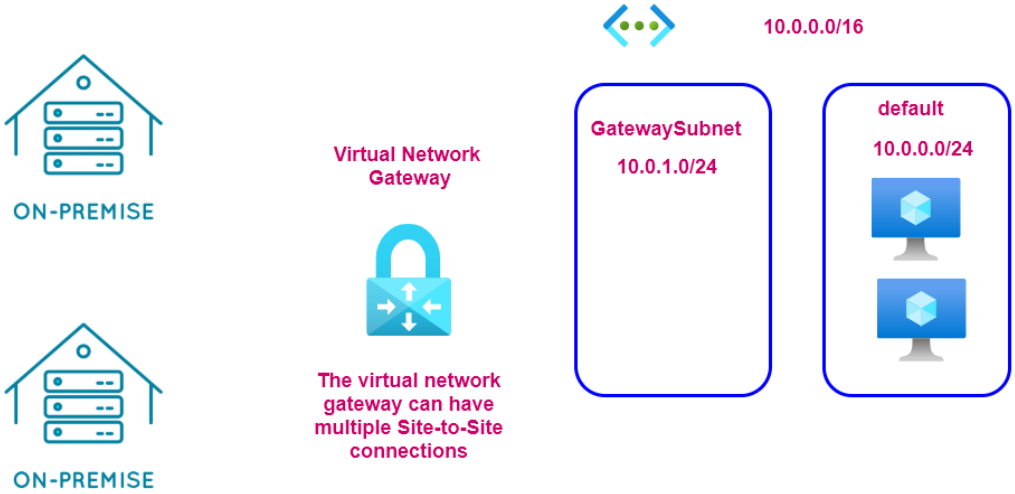
1. Planned maintenance - 10 to 15 seconds
2. unplanned issues - 1 - 1.5 minutes

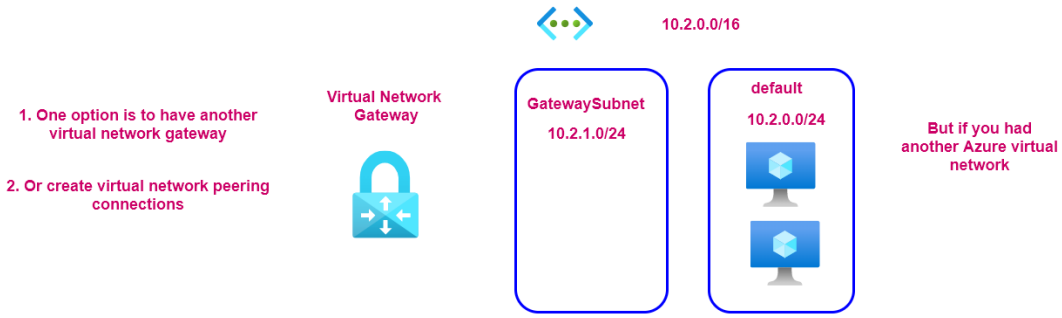


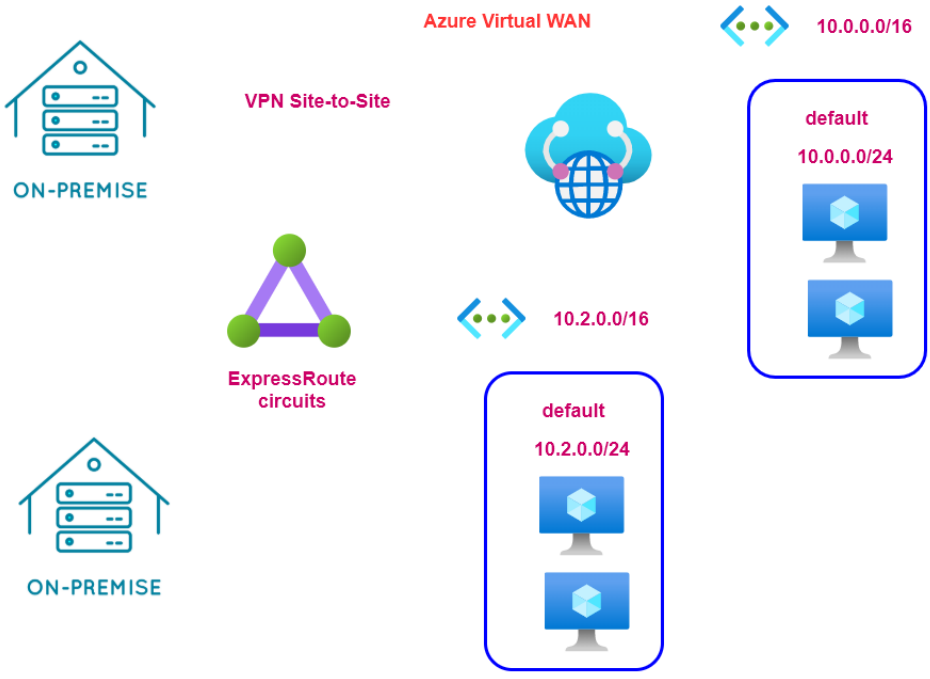


1. Here you need two public IP addresses in Azure
2. You need two local network gateways
3. One connection from Azure VPN to each local network gateway

Azure Virtual WAN


10.0.0.0/16
ON-PREMISE
Virtual Network Gateway
GatewaySubnet
10.0.1.0/24
default
10.0.0.0/24
ON-PREMISE
The virtual network gateway can have multiple Site-to-Site connections


10.2.0.0/16
1. One option is to have another virtual network gateway
2. Or create virtual network peering connections
Virtual Network Gateway
GatewaySubnet
10.2.1.0/24
default
10.2.0.0/24
But if you had another Azure virtual network


Azure Virtual WAN
10.0.0.0/16
ON-PREMISE
VPN Site-to-Site
default
10.0.0.0/24
ExpressRoute circuits
10.2.0.0/16
default
10.2.0.0/24
ON-PREMISE

The different resources

virtualWAN - This represents the virtual overlay of the Azure virtual network and other resources

Hub - You create a virtual hub in the virtual WAN resource. This is a Microsoft-managed virtual network

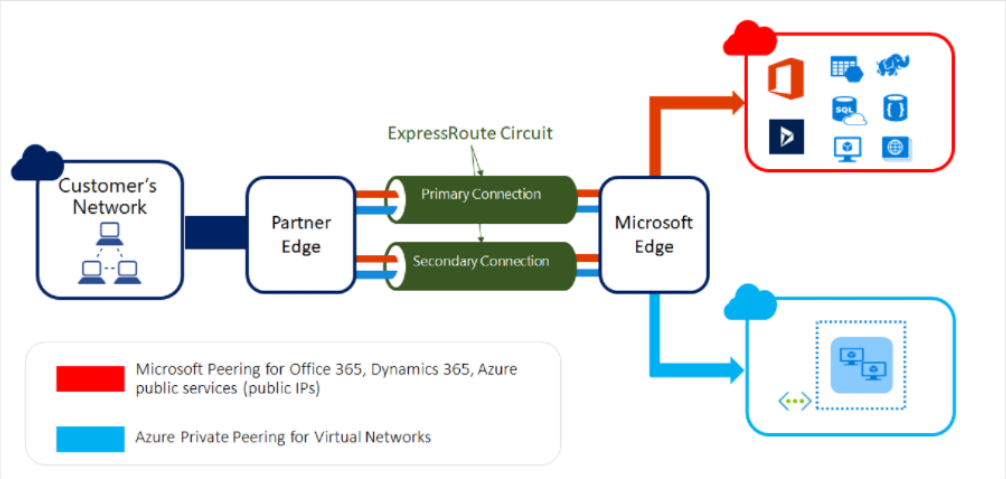
You then connect the various endpoints to the Hub - Azure virtual network, Site-to-Site

Azure ExpressRoute

Azure ExpressRoute

Allows you to connect your on-premises networks to Microsoft cloud over the private connection

Here the connection is established with the help of a connectivity provider

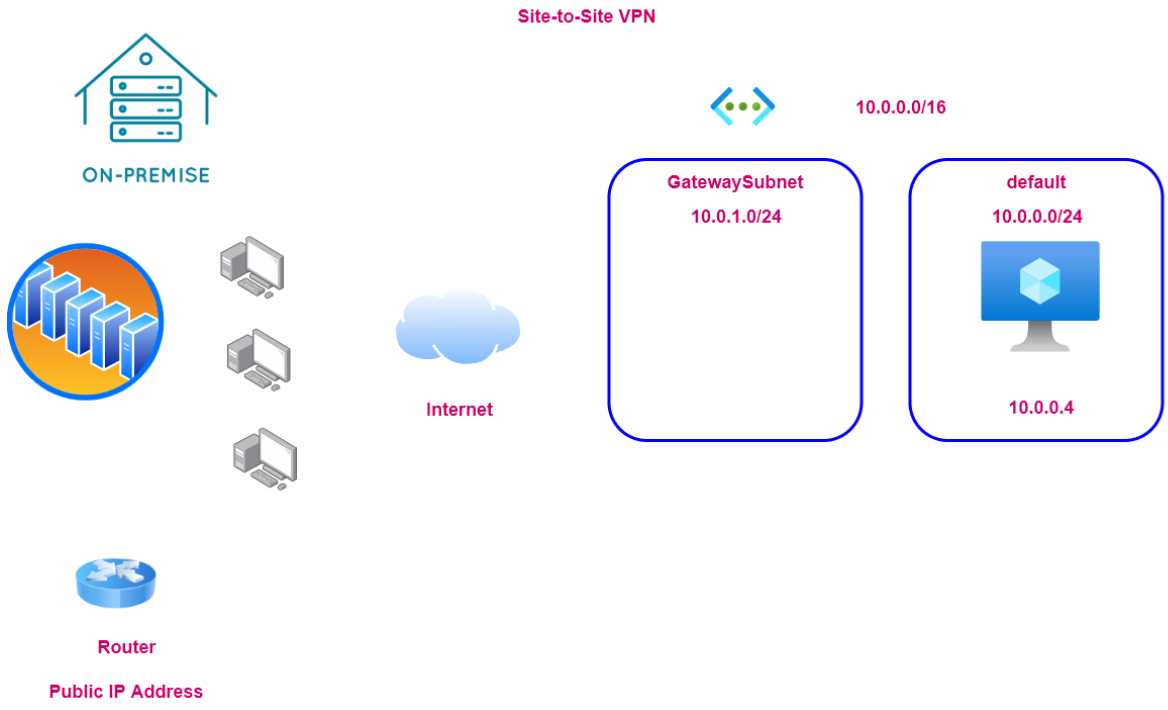


Reference - https://docs.microsoft.com/en-ca/azure/expressroute/expressroute-introduction

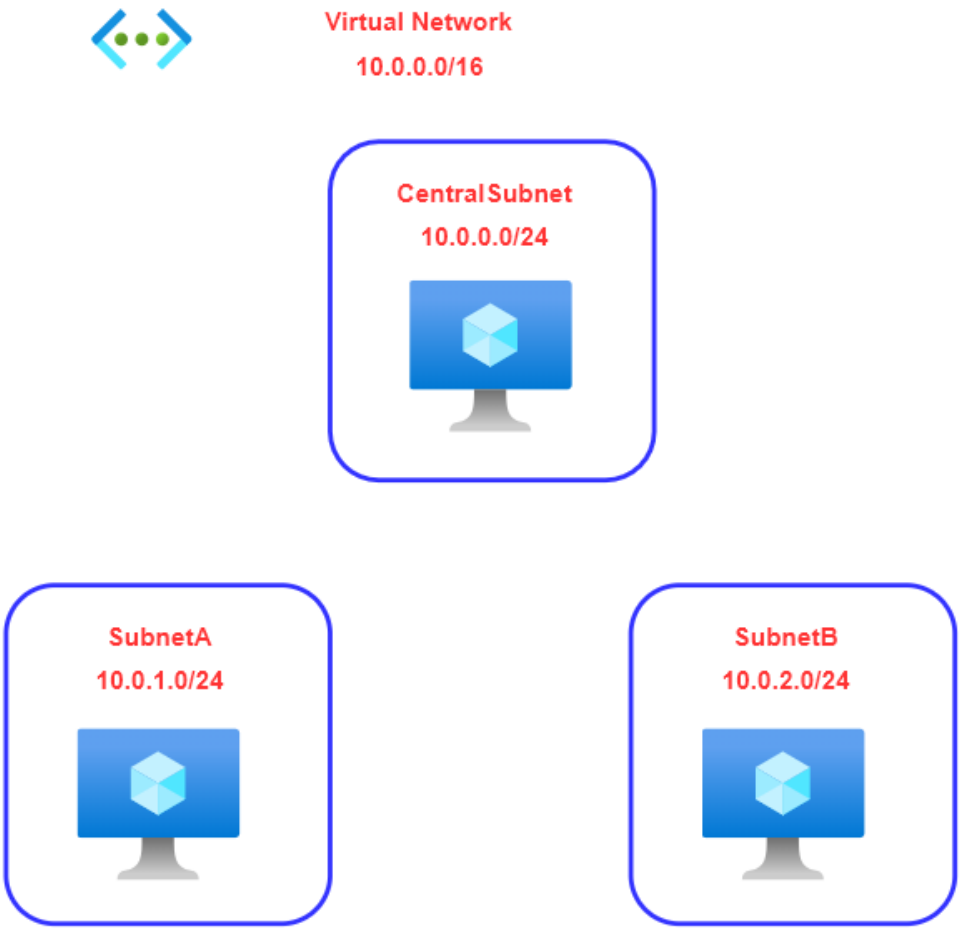
The ExpressRoute connection does not go over the public Internet

Your connections are more reliable, faster and you get less latency

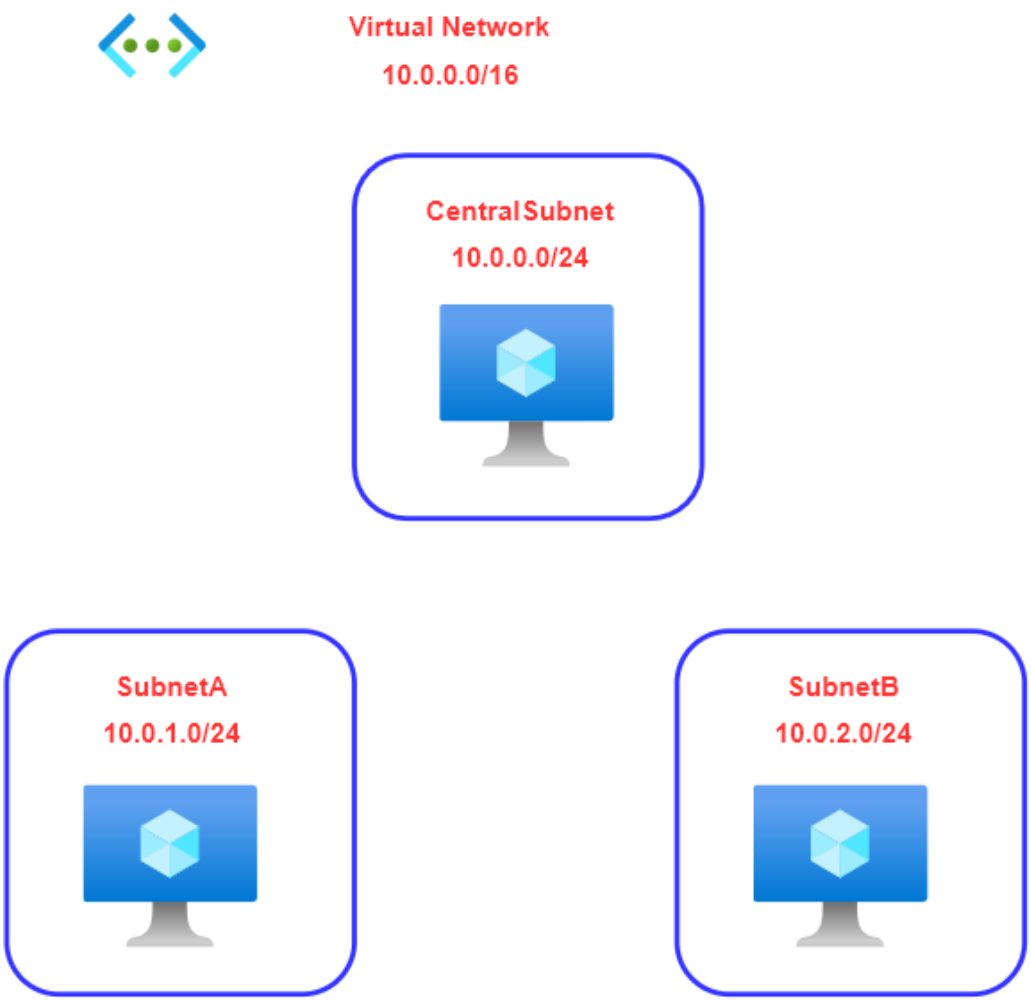
You get two connections for each ExpressRoute circuit for redundancy


Site-to-Site VPN
ON-PREMISE
10.0.0.0/16
GatewaySubnet
10.0.1.0/24
default
10.0.0.0/24
Internet
10.0.0.4
Router
Public IP Address

User Defined Routes



User Defined Routes - What are we going to do

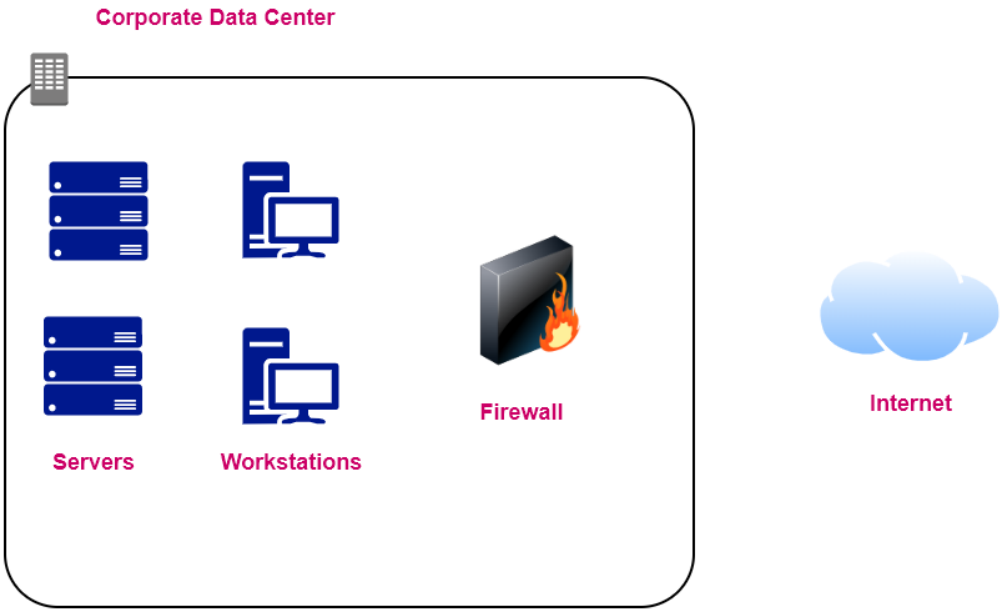


1. Create our environment

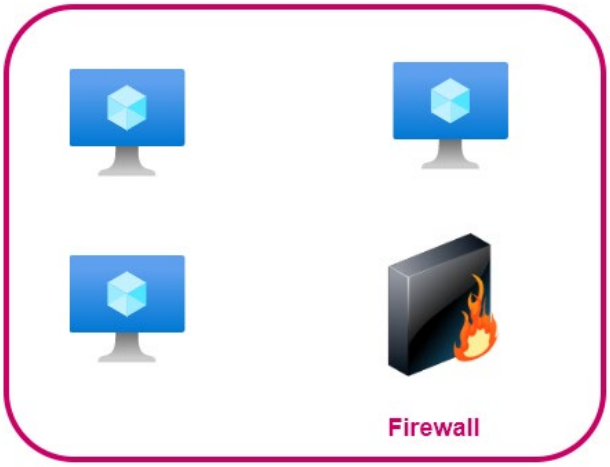
2. Create a user defined route and attach it to SubnetA and SubnetB

3. Enable routing on the machine in CentralSubnet

Azure Firewall


Corporate Data Center
Servers
Workstations
Firewall
Internet

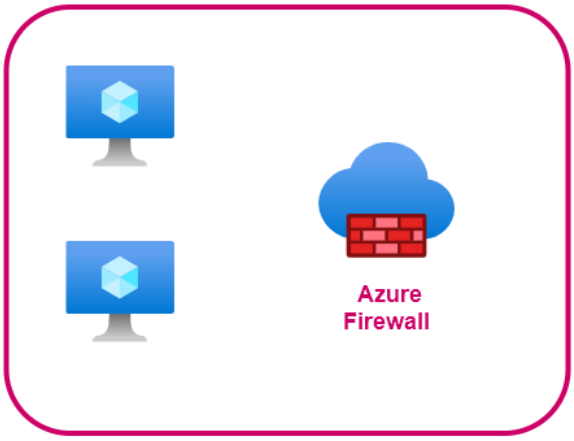
Virtual Network



Internet

Firewall

Virtual Network



Azure Firewall

Internet

1. Has built-in high availability

2. Can deploy the Azure Firewall Instance across two or more Availability zones - 99.99% SLA

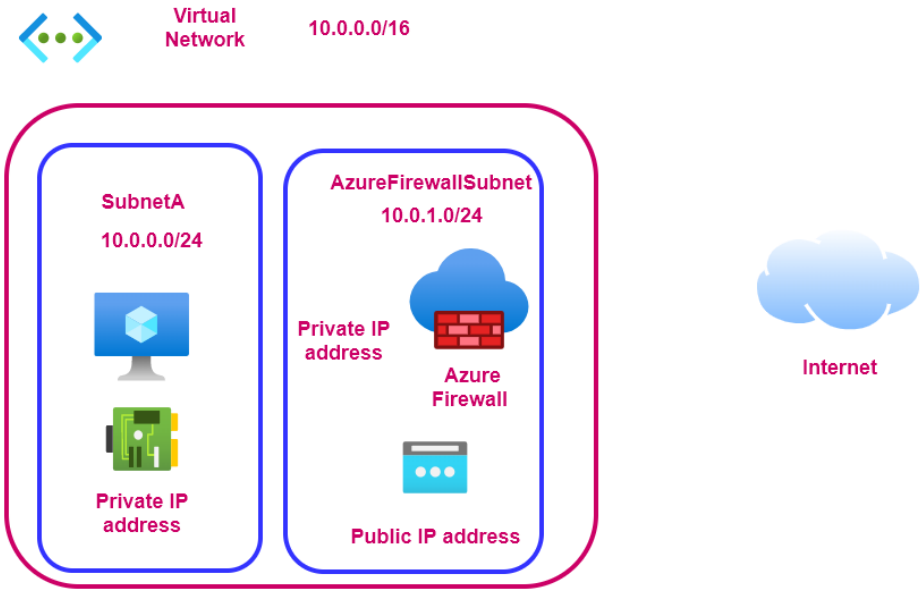
3. You can filter traffic based on fully-qualified domain names

4. You can also create network filtering rules - Based on source and destination IP address, port and protocol

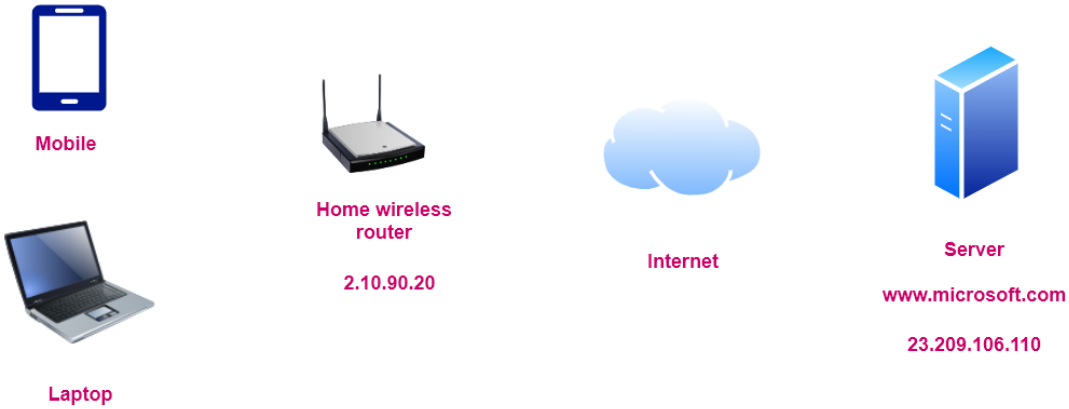
5. It is stateful in nature, so it understands what packets of data to allow

6. It has built-in Threat Intelligence - Here you can get alerts or deny traffic from/to malicious IP addresses and domains

Lab - Azure Firewall – Deployment

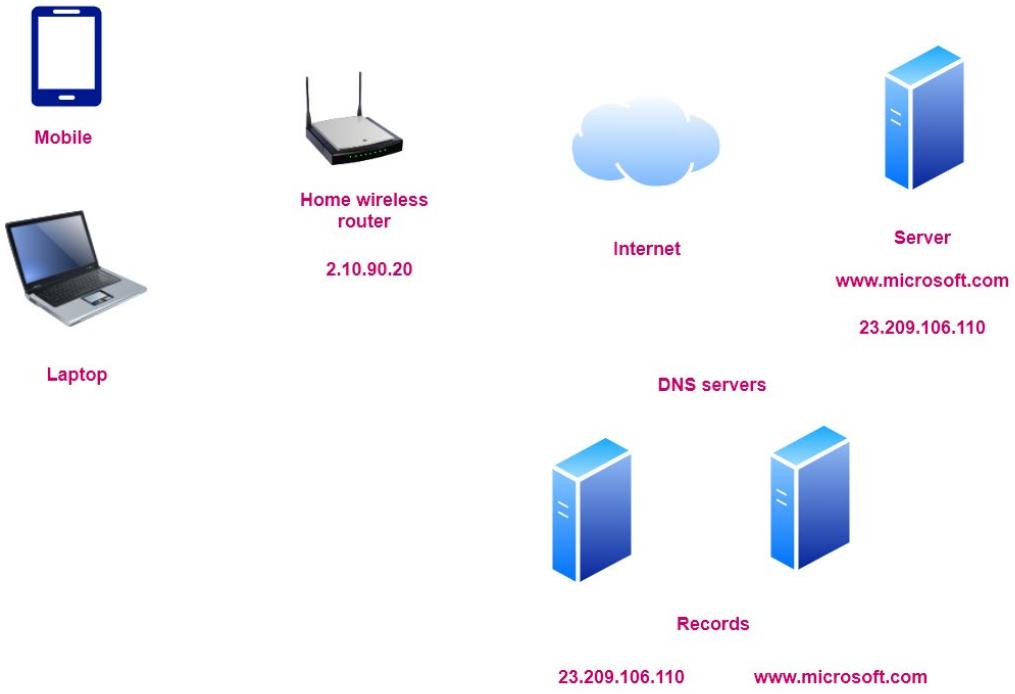


What is the domain name system



When packets of data need to be routed via the TCP protocol , a connection needs to be established between the client and the server with the use of IP addresses

So how does my client know the IP address of www.microsoft.com



Lab - Local DNS - Setting up the domain

new-network

10.0.2.0/16

SubnetA - 10.2.0.0/24

dns-server

1. Install Active Directory Domain services

2. Promote the server to a domain controller

3. Specify a root domain name - cloud2hub.com

6. Use Azure provided DNS names web-server.internal.cloudapp.net

SubnetB - 10.2.1.0/24

web-server

4. Create a new server as part of a new subnet

5. Install Internet Information Services on the server

7. Now its time to use our DNS server

7.1 For the network , we need to mention our DNS Server

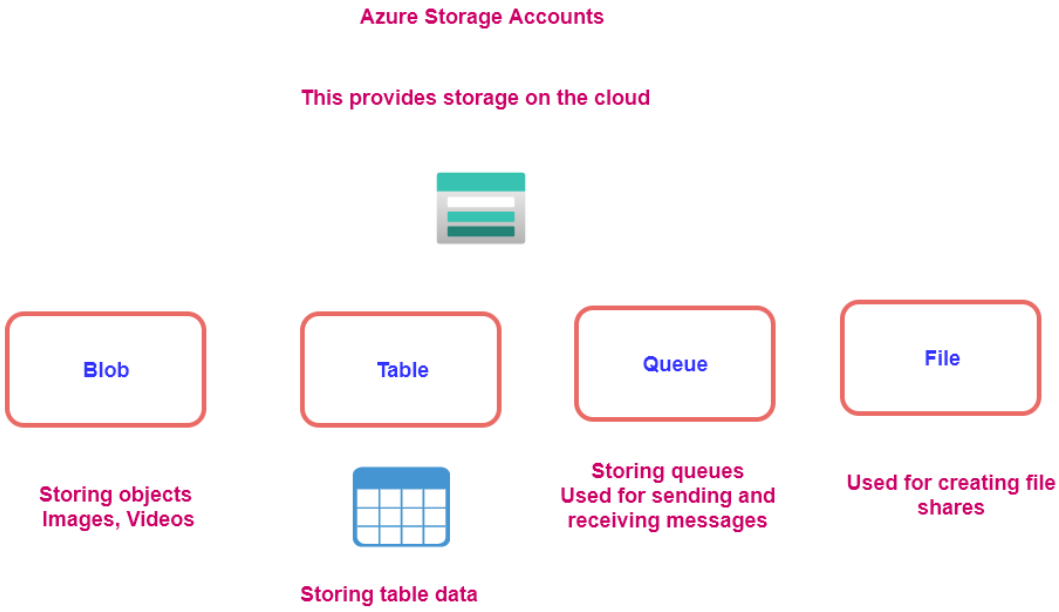
7.2 Restart our servers

7.3 Add a record to the zone

Azure Private DNS

Implement and manage storage

What are storage accounts



Azure Blob service

Its optimized for storing large amounts of unstructured data

Azure Storage Account

Azure virtual machine

Blob service

Container

Files

Unique URL

Images

Videos

Block blobs

This is made up of blocks of data that can managed individually

Append blobs

These are block blobsthat are optimized for append operations - Good for logging

Page blobs

This is used for virtual hard drive files for Azure virtual machines

Azure Storage Accounts - Different authorization techniques

Azure Storage Accounts - Data Redundancy

Azure Storage account - Redundancy

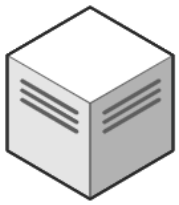
Multiple copies of your data are stored

This helps to protect against planned and unplanned events - transient hardware failures, network or power outages.

Storage Device

Locally-redundant storage

Data Center



Central US

Here three copies of your data are made

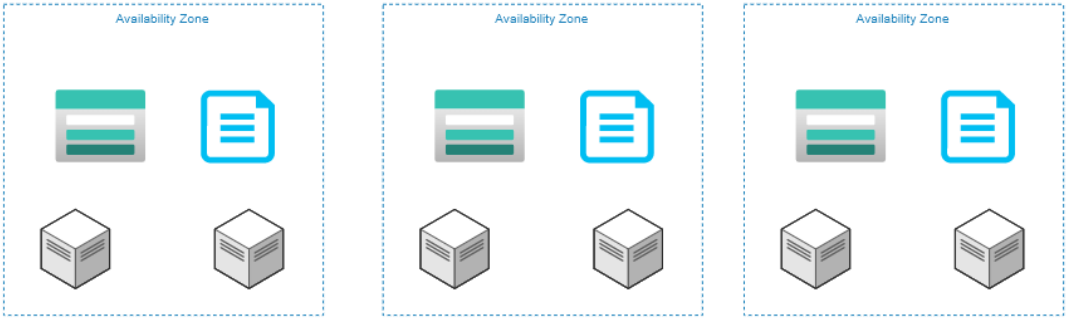
It helps to protect against server rack of drive failures

Storage Device Storage Device Storage Device

Zone-redundant storage

This helps to protect against data center level failures

Here data is replicated synchronously across three Azure availability zones

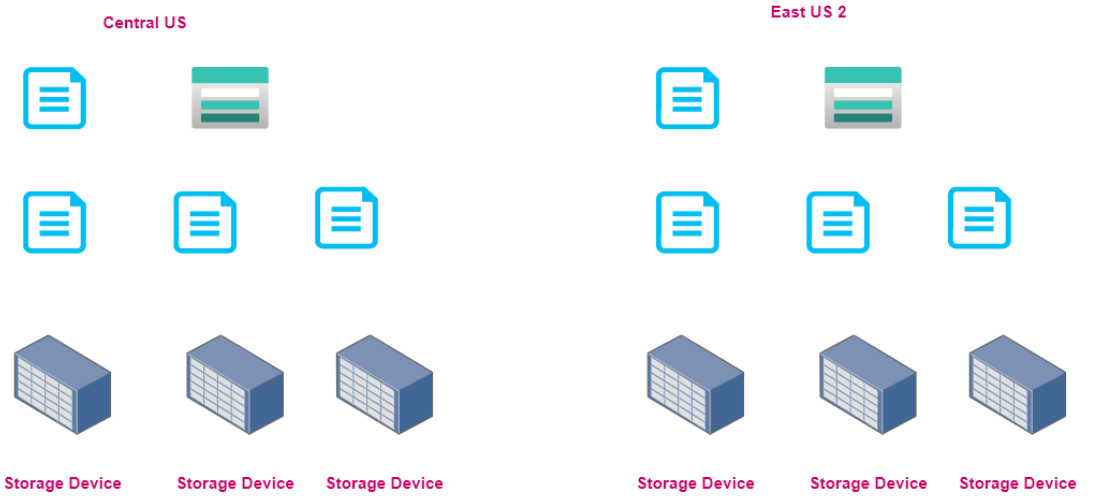


Central US

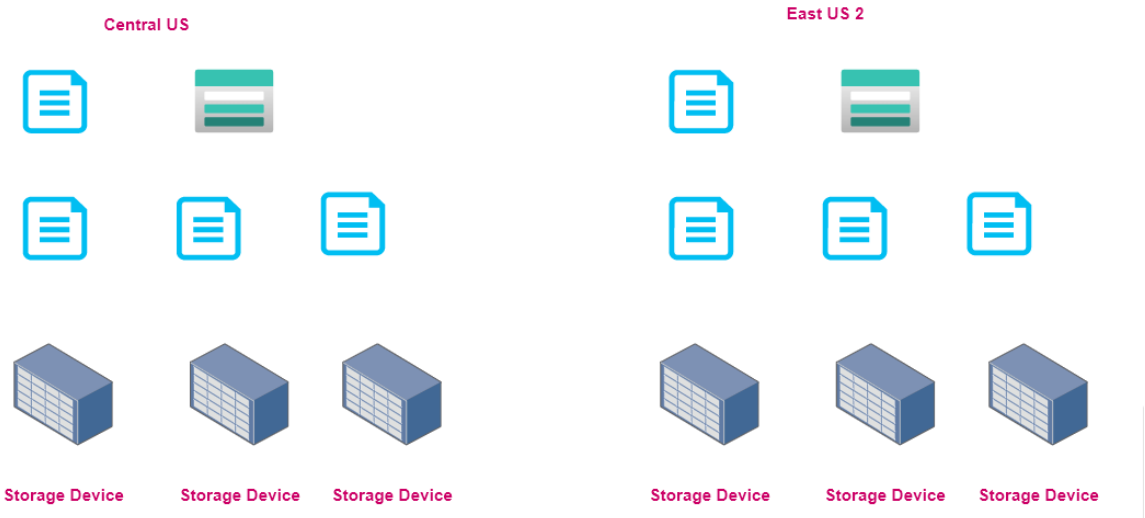
Each availability zone is a seperate physical location with independent power, cooling and networking

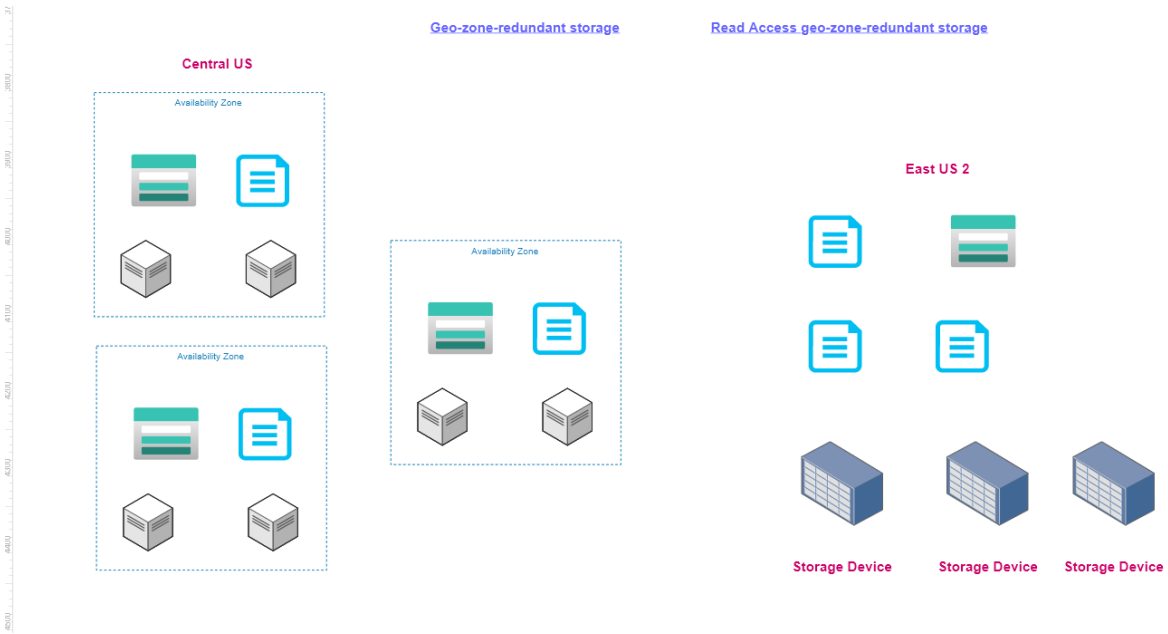
Geo-redundant storage

Here data is replicated to another region

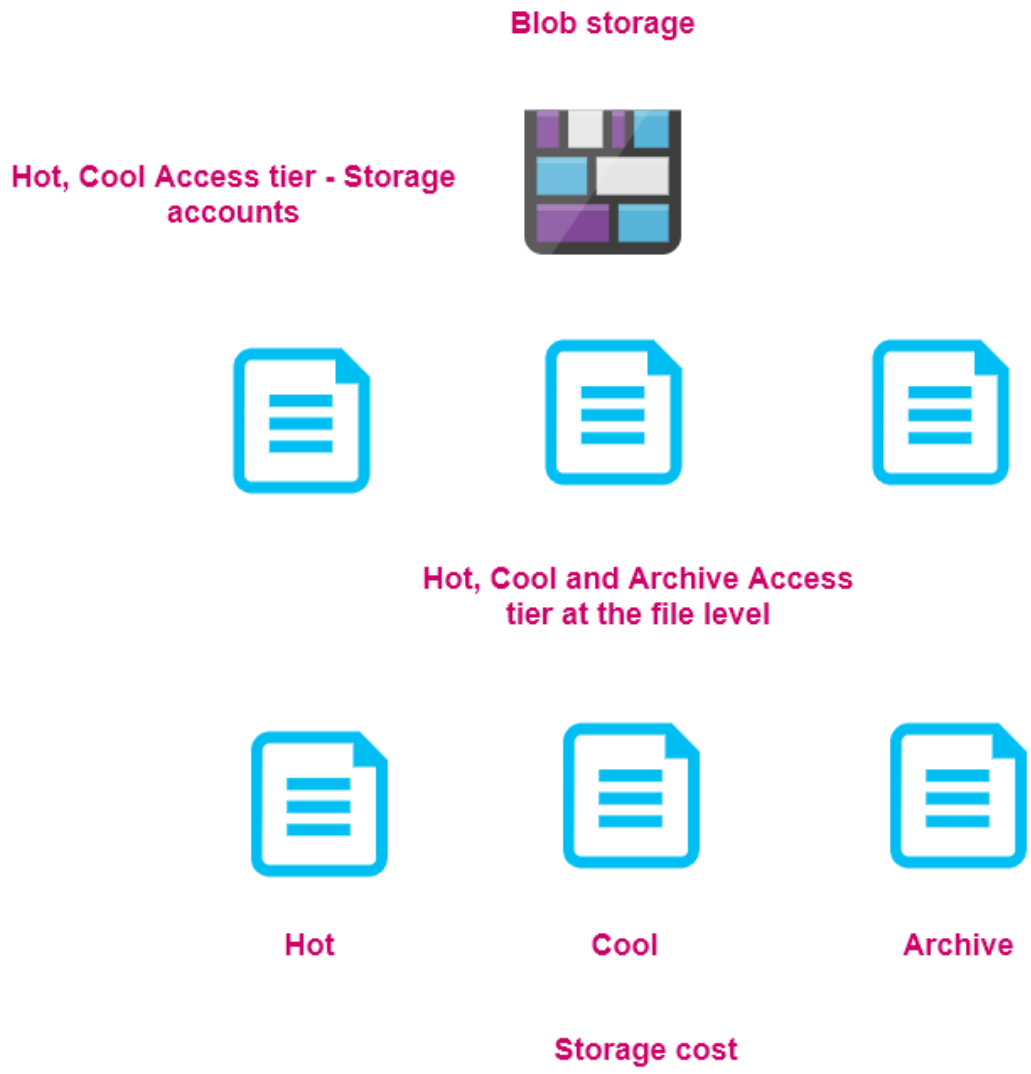


Read-access geo-redundant storage




Geo-zone-redundant storage
Read Access geo-zone-redundant storage
Central US
Availability Zone
Availability Zone
Availability Zone
East US 2
Storage Device
Storage Device
Storage Device

Storage Accounts - Access Tiers



Early deletion fees

Cool

Here the data needs to be stored for at least 30 days

Archive

Here the data needs to be stored for at least 180 days

To read an object in the Archive tier

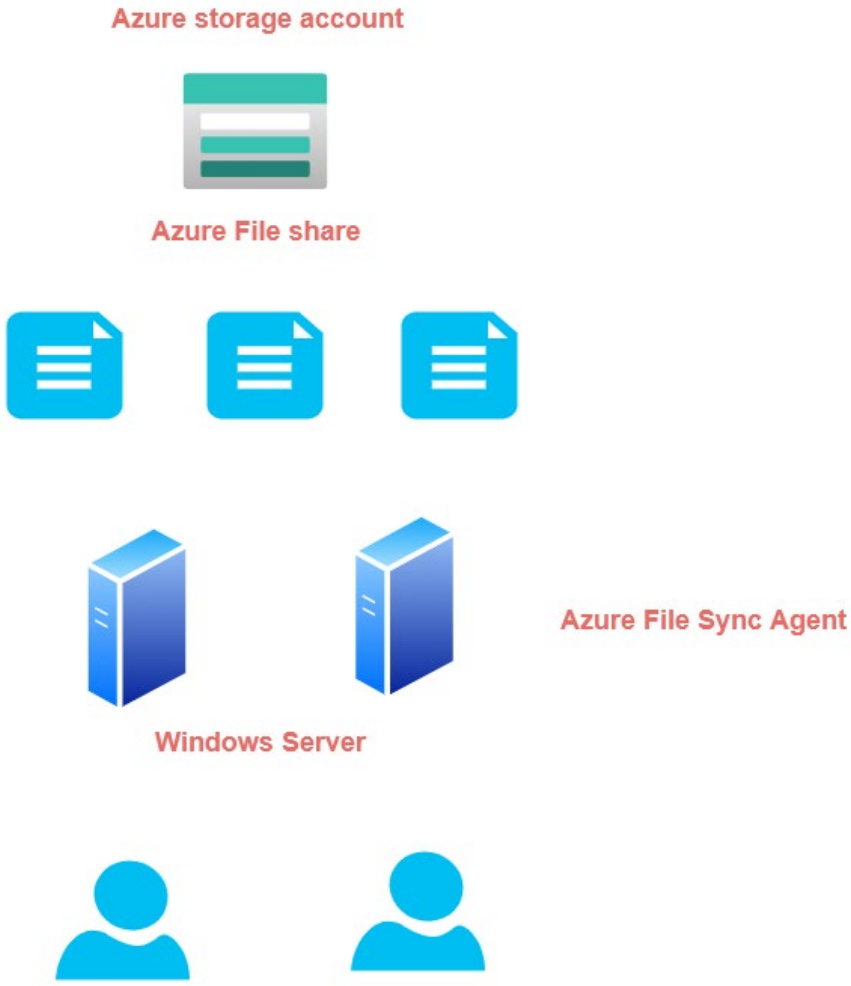
Archive

Cool

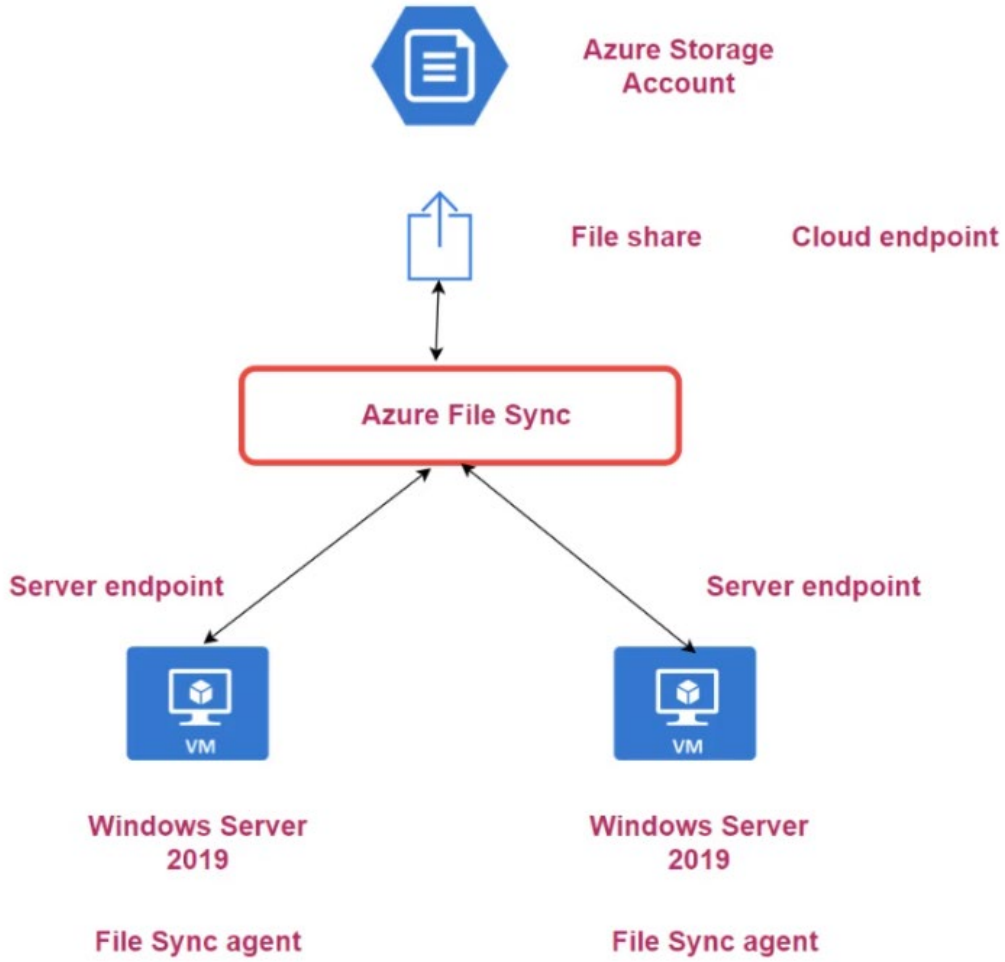
Rehydration

Hot

Azure File Sync

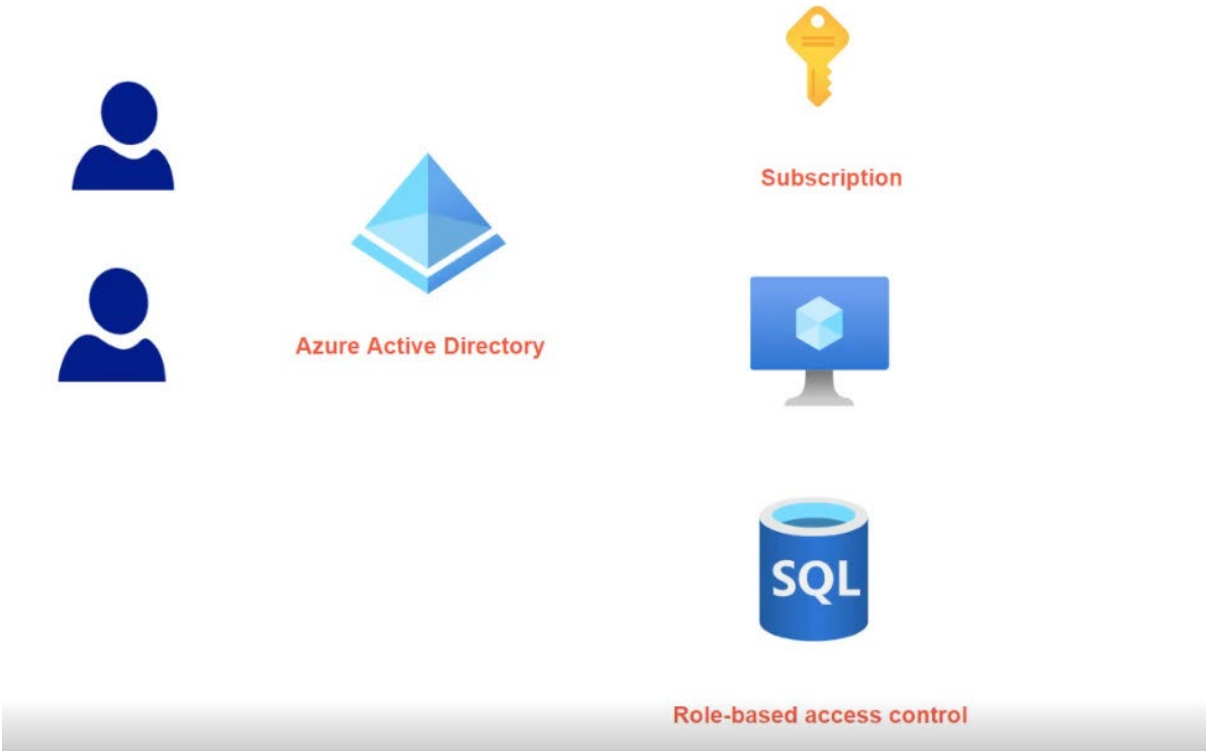

Azure storage account
Azure File share
Azure File Sync Agent
Windows Server

Azure File Sync Service – Setup

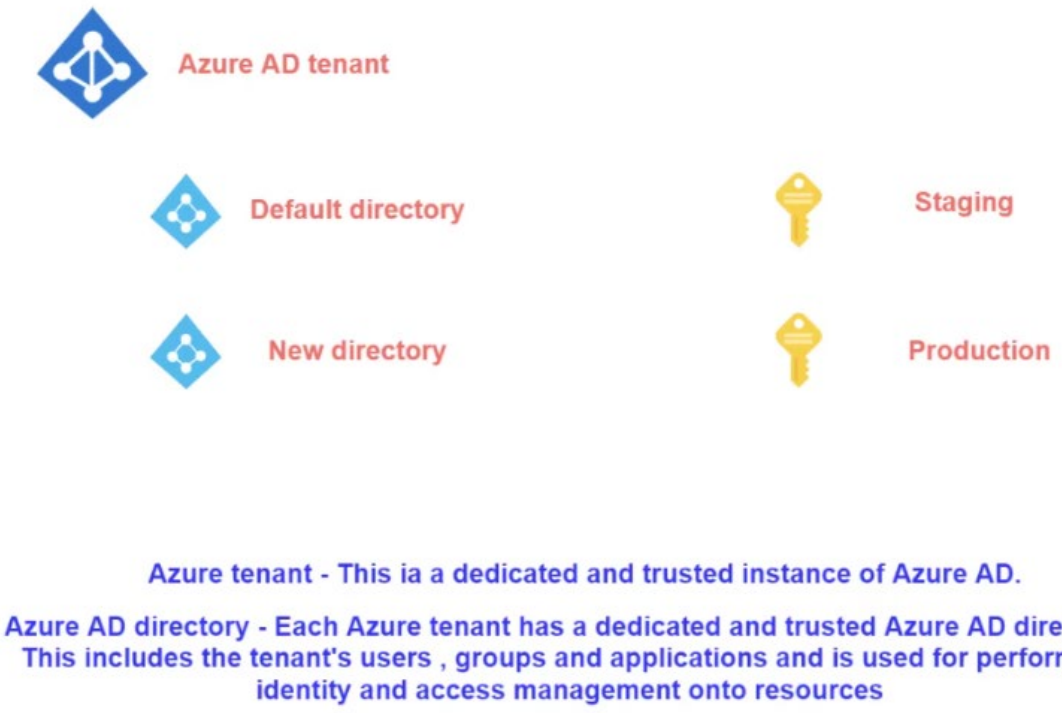


Manage Azure identities and governance

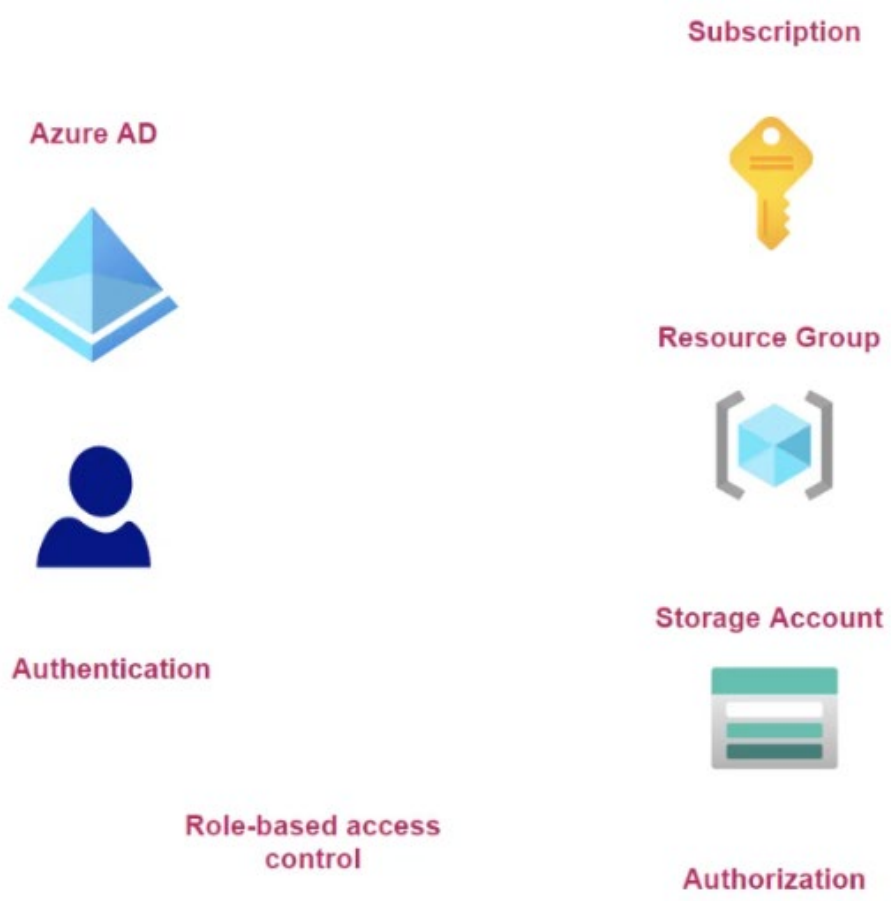
What is Azure Active Directory



Trust between Azure Subscription and Azure AD

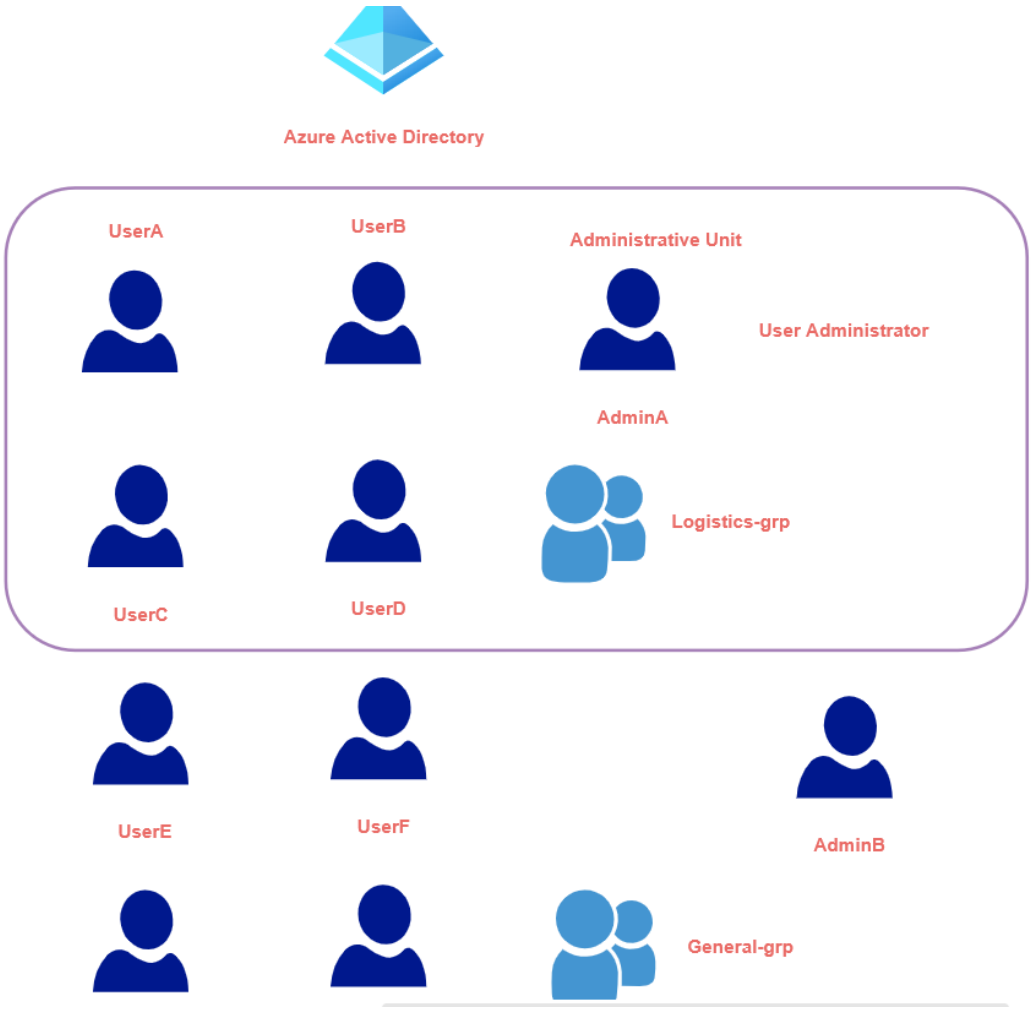


Introduction to Role Based Access Control



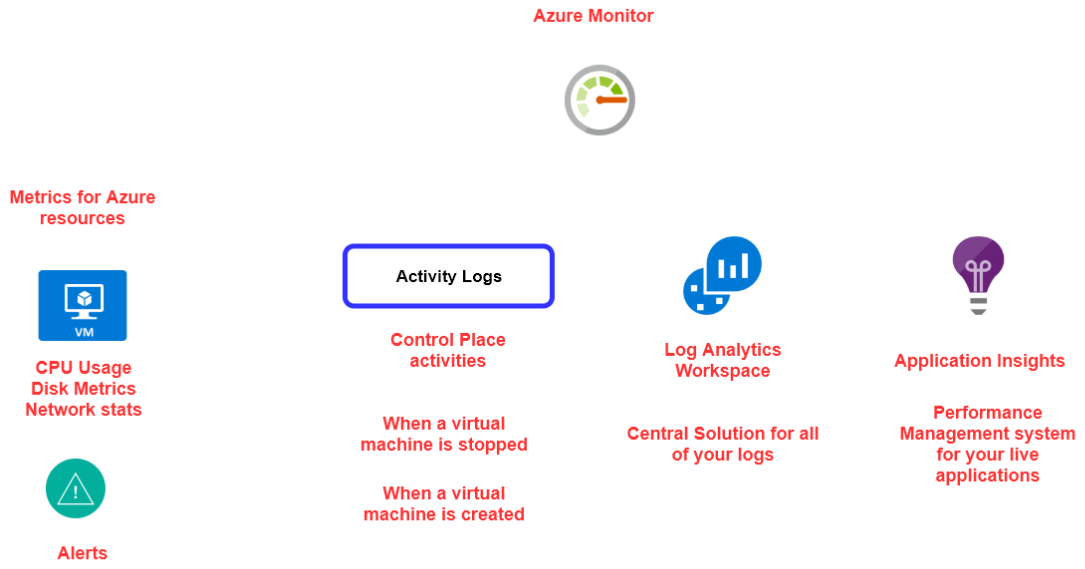
Administrative Units

Lab - Administrative Units

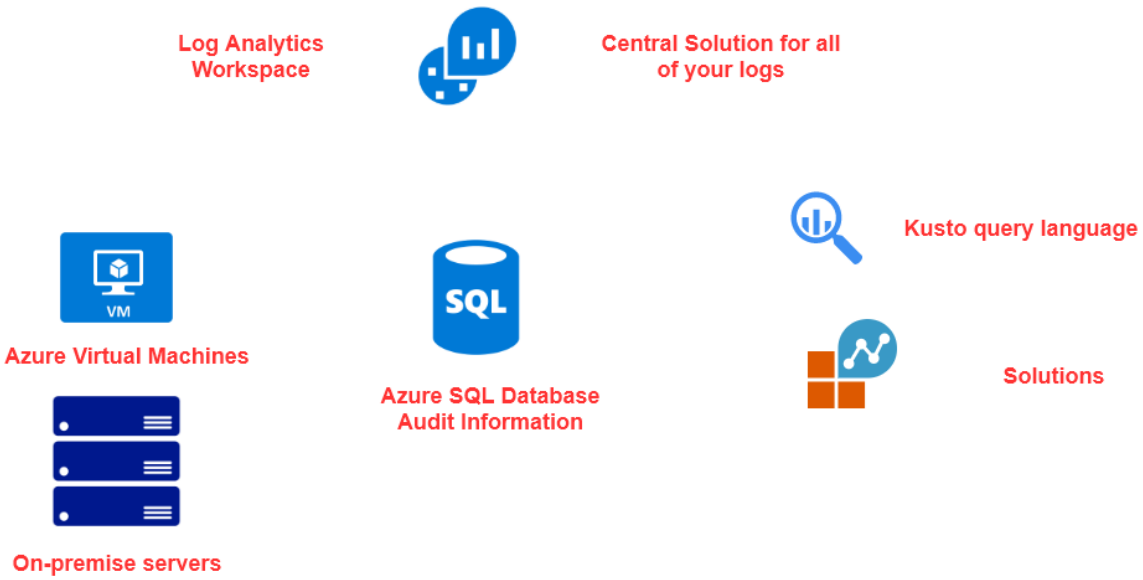


Monitor and back up Azure resources

What is the Azure Monitor Service



What is a Log Analytics Workspace



What is the Azure Backup feature

Azure Backup for virtual machines

This provides access to data on the VM if something happens to the original VM

The backup data gets written to a Recovery Services vault

Azure Site Recovery Services vault

East US

Azure virtual machines

East US

Steps during a backup

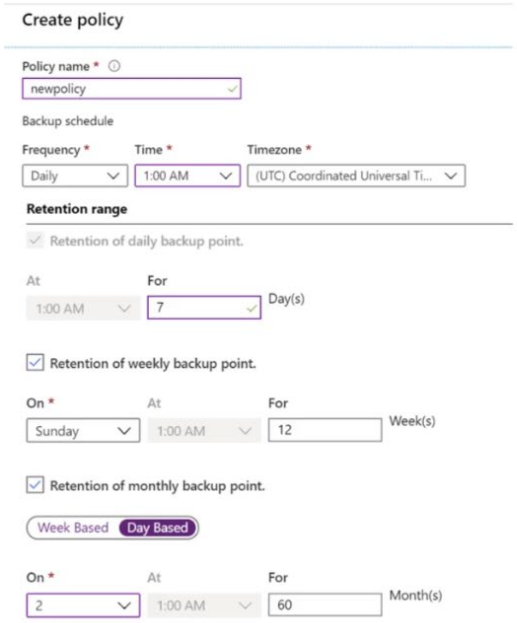
1. First an extention is installed on the VM - Supported for both Windows and Linux VM's

2. The backup tool first takes a snapshot of the data and stores it on the local machine

3. The snapshot of data is then copied to the Recovery Service svault

4. When the data is transfered, the snapshot is then removed and a recovery point is then created

What is the Azure Backup feature



You
configure the backup for the Azure virtual machine on 1st of April – Wednesday.

How many
recovery points will be available on the 9th of April at 14:00?

Backup Taken	Daily retention point	Weekly Retention point	Monthly Retention point	Yearly retention point
1st April (Wed)– 1:00 a.m				
2nd April (Thurs)– 1:00 a.m			Available	
3rd April (Fri) – 1:00 a.m	Available			
4th April (Sat)– 1:00 a.m	Available			
5th April (Sun)– 1:00 a.m	Available	Available		
6th April (Mon)– 1:00 a.m	Available			
7th April (Tues)– 1:00 a.m	Available			
8th April (Wed)– 1:00 a.m	Available			
9th April (Thurs)– 1:00 a.m	Available			Available

Review - Azure Site Recovery

Azure Site Recovery

Used for business continuity and for disaster recovery

Ensures your apps and workloads are running when there are planned or unplanned outages

Physical servers

Hyper-V VM's

VMWare

Server running your applications

Primary data center

Secondary data center

Server running your applications

Primary data center

Servers in Azure

VM in Azure

VM in Azure

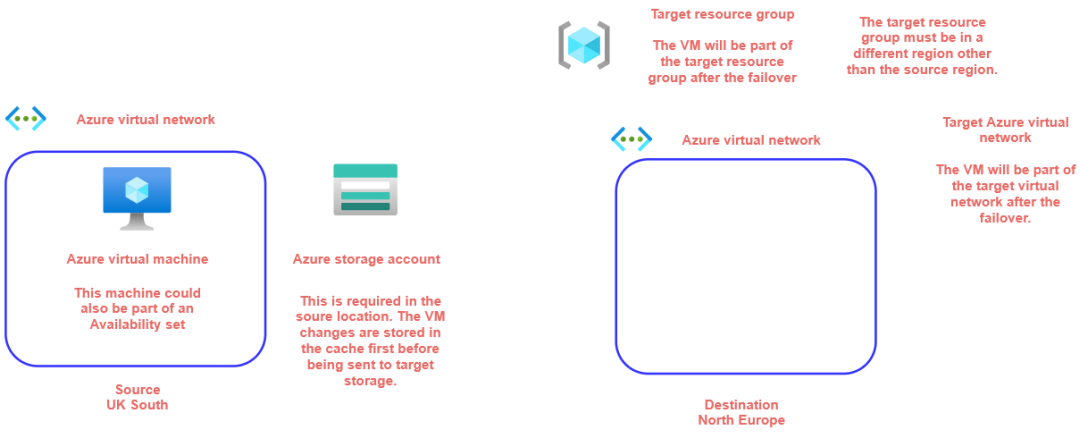
The replication frequency is high , being as low as every 30 seconds for Hyper-V VMs

Hence the RPO is low. And because you can switch over quickly, the RTO is also low

You can run planned failovers with zero-data loss

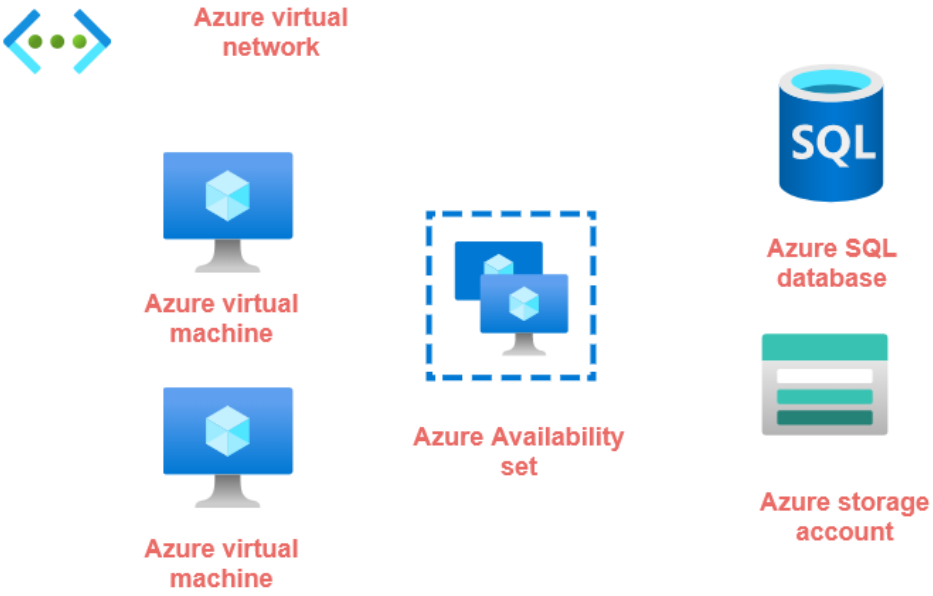
Or unplanned failovers with minimal data loss

Azure Site Recovery - Azure VM – Overview



Azure Resource Manager Templates

What are Azure Resource Manager templates



You define your infrastruture as code

Create an Azure Resource Manager template

This is a JavaScript Object Notation file that actually contains the definition of the infrastructure

You can store the ARM templates in your source code repository along with your application code