Deploy and Manage Azure compute resources

The Virtual Machine service

What is the Azure Virtual Machine service

Generally what does a company need in order to host an application and make it available to users.

Buy physical servers

Buy storage

Setup a network

All of this costs money, there is an initial investment that the company needs to undertake.

Large companies will normally setup data centers. These centers contain a number of servers, storage devices, racks, cooling devices etc.

All of this is an investment from the company.

The first service we are going to look into is the Azure Virtual Machine service.

Virtual Machine

This is a compute service that allows you to host virtual machines on the Azure cloud network.

This is an on-demand scalable compute service.

Here you don't need to buy and invest in physical hardware. This is already managed for you. Microsoft maintains several data centers located across the world.

You can use the Virtual Machine service to host a virtual machine.

Virtual Machine

Workload - Web Server / Database Server

Ubuntu Server/ Windows Server

Server 

The entire data center is managed by Microsoft.

Lab - Building a Windows virtual machine

This is a compute service that allows you to host virtual machines on the Azure cloud network.

What is involved in the deployment of a virtual machine.

What is the size of virtual machine - number of vCPU's, RAM

What is the number and size of the disks you want allocated for the virtual machine.

What is the underlying operating system - Ubuntu, Windows Server.

The network details for the virtual machine.

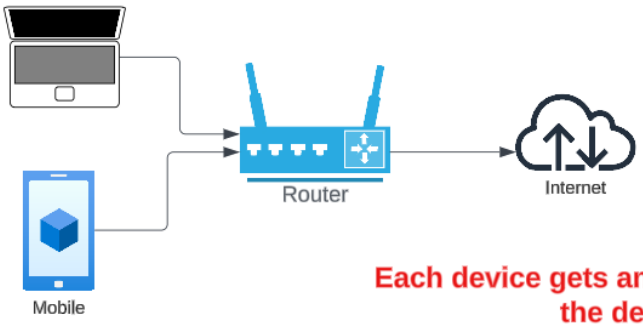
Azure Marketplace - This has in-built templates that you can choose from. For example , there is a template for Ubuntu Server 22.04. If you choose this template for your machine, it will create for you a virtual machine based on that operating system.

You can choose a virtual machine size - This will allocate the required hardware resources for your machine.

Apart from the virtual machine itself, there are other resources created on the Azure platform to complement the Azure virtual machine.

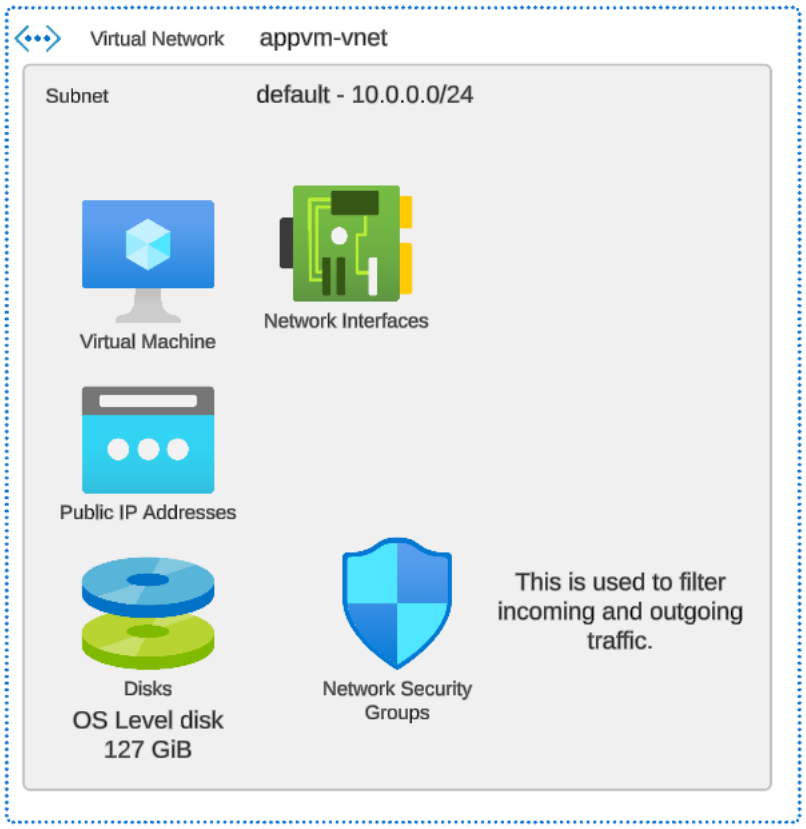
For example, we need a virtual network for the virtual machine.

Home setup

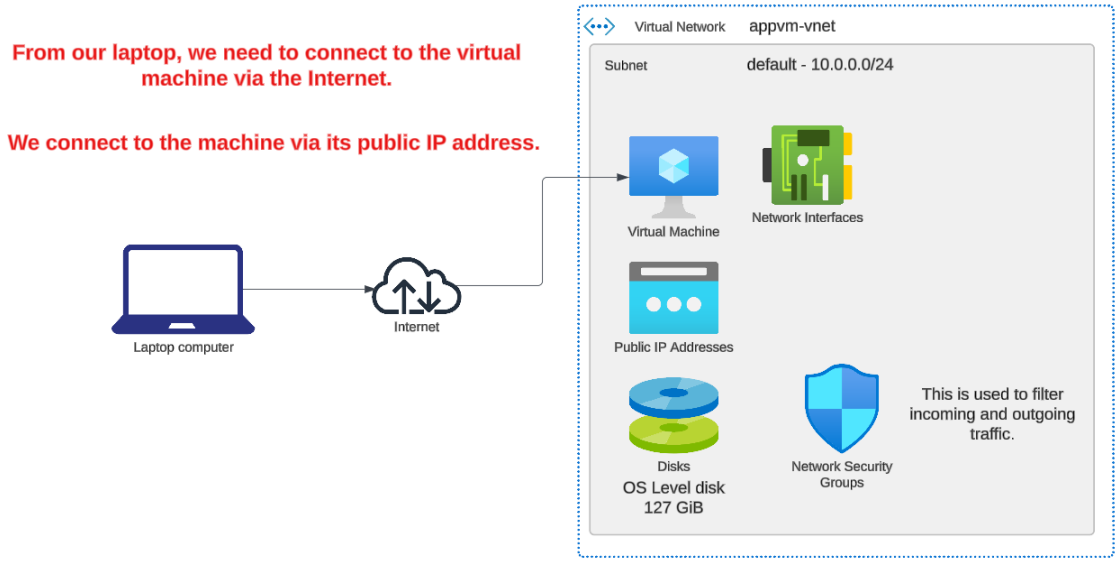


Each device gets an IP address. This helps to identify the device on the network.

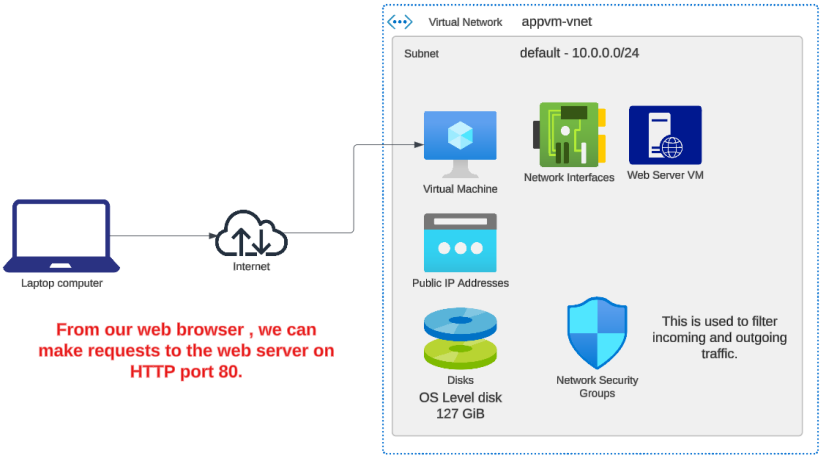
A network allows devices to communicate with each other.



Lab - Connecting to the Virtual Machine



Lab - Installing Internet Information Services



From our web browser , we can make requests to the web server on HTTP port 80.

We are going to install Internet Information Services on the machine.

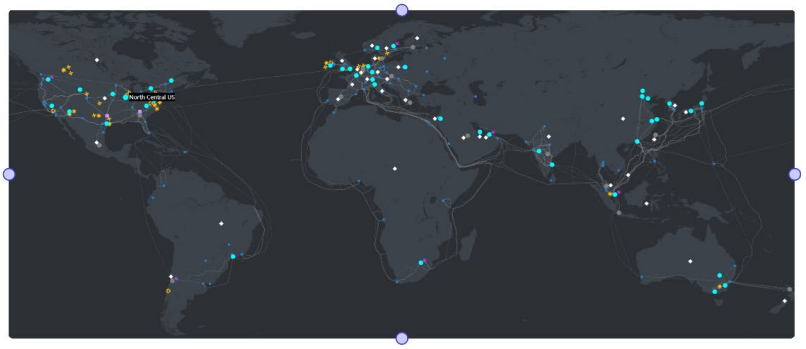
This will make the machine behave as a Web Server.

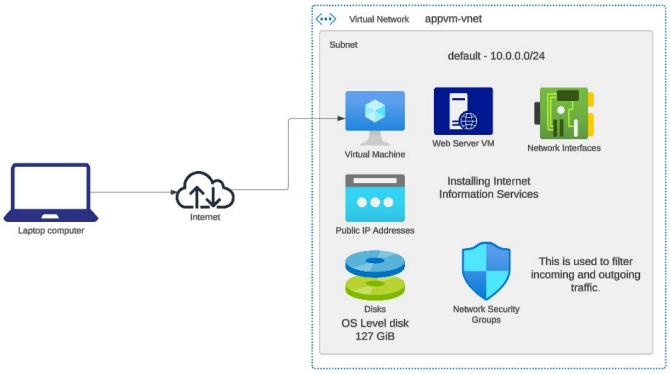
Understanding Azure regions

Azure has data centers located across the world. An Azure region is a geographic location that has one or more data centers.

When you want to host a resource such as an Azure virtual machine, it needs to be hosted on some physical infrastructure in an Azure data center.

These resources are made available to you via the Internet. And the Azure portal is a web interface that allows you to interact with the Azure resources.





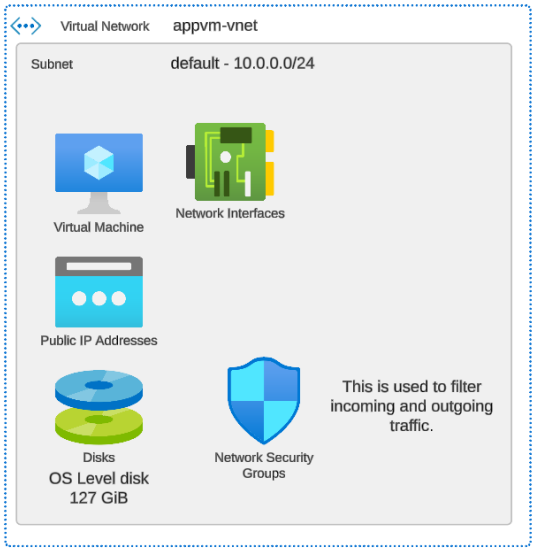
Costing for Azure resources

There are costs associated with the Disks, Public IP address.

Based on the Instance size, you will have a price associated with the machine. The higher the instance size, the higher the costs.

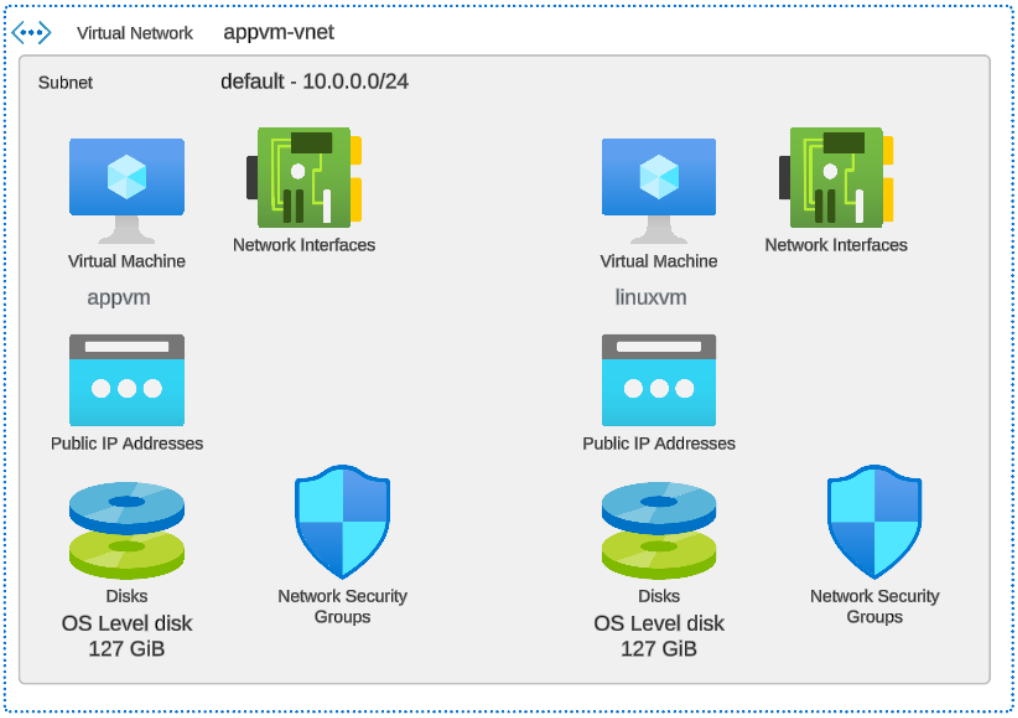
You will normally see the estimated cost per month or hour when it comes to pricing. But in the end, you only pay based on how much you consume. Hence if you only use the machine for 20 minutes, you only pay for the time consumed.

If you stop (deallocate) the machine, then the costing stops for the virtual machine when it comes to compute.



There are no costs linked to the virtual network, the network interface and the Network Security groups.

Lab - Building a Linux Virtual Machine



The Linux-based machine will have its own related resources.

You don't need to have Public IP addresses for machines. If machines need not be accessed from the Internet, they don't need Public IP addresses.

You can have one Network Security Group located at the subnet layer.

Lab - Deploying a Linux machine - SSH keys

Admin Credentials - Password based or SSH.

SSH is an encrypted connection protocol.

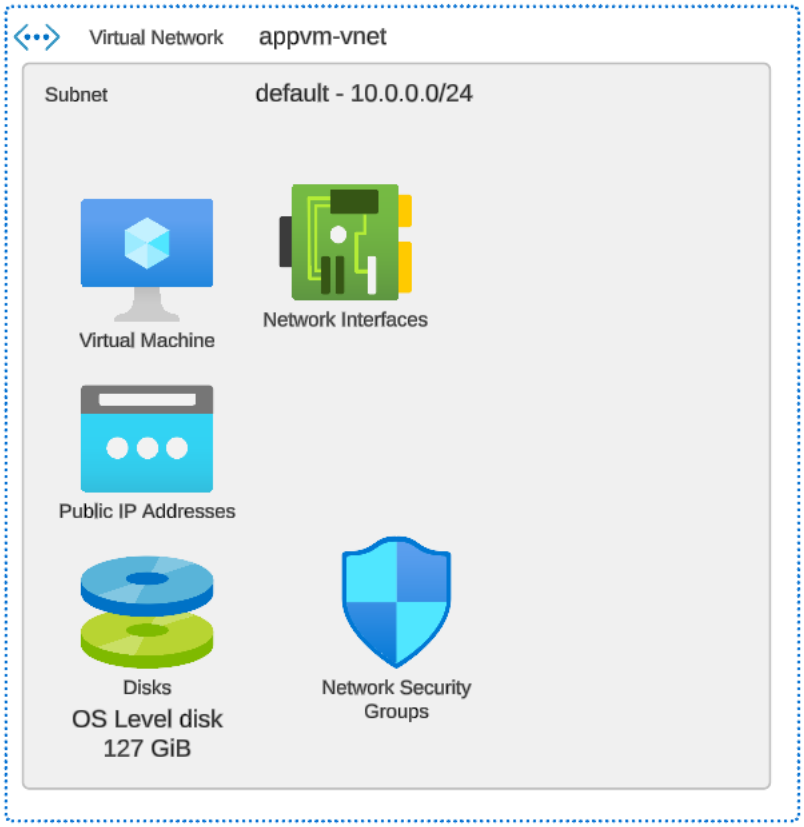
You can use SSH keys for a more secure connection.

This is based on public-private key pairs.

The public key is stored on the virtual machine itself.

The private key can then be used to authenticate onto the Linux virtual machine.

Azure Virtual Machine – Disks



Azure Managed disks - These are block-level storage volumes that are managed by Azure.

These disks are highly available and durable in nature.

You can create and attach disks to a machine either during the launch of the machine or after the machine is created.

Each virtual machine will come with an OS disk. This will have the operating system installed on it.

You can create additional data disks and attach it to the virtual machine.

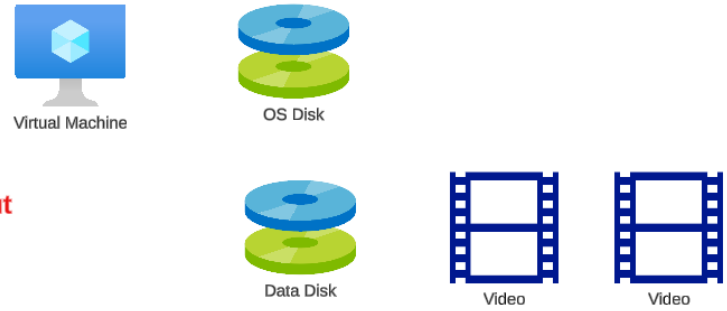
A machine can also get a temporary disk. The size depends on the machine size. The data on this disk can be lost during a maintenance event, or when you redeploy a virtual machine or when you stop the machine.

Different disk types

	Ultra Disk	Premium SSD v2	Premium SSD	Standard SSD	Standard HDD
Disk type	SSD	SSD	SSD	SSD	HDD
Scenario	IO-intensive workloads such as SAP HANA, top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads.	Production and performance-sensitive workloads that consistently require low latency and high IOPS and throughput	Production and performance sensitive workloads	Web servers, lightly used enterprise applications and dev/test	Backup, non-critical, infrequent access
Max disk size	65,536 GiB	65,536 GiB	32,767 GiB	32,767 GiB	32,767 GiB
Max throughput	10,000 MB/s	1,200 MB/s	900 MB/s	750 MB/s	500 MB/s
Max IOPS	400,000	80,000	20,000	6,000	2,000, 3,000*
Usable as OS Disk?	No	No	Yes	Yes	Yes

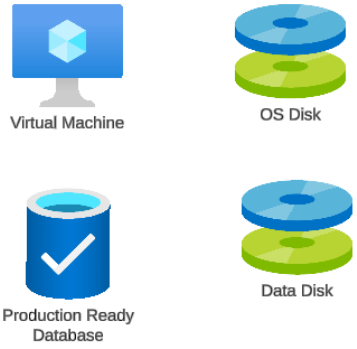
The main performance metrics that need to be noted are throughput and IOPS.

The main performance metrics that need to be noted are throughput and IOPS.



Throughput

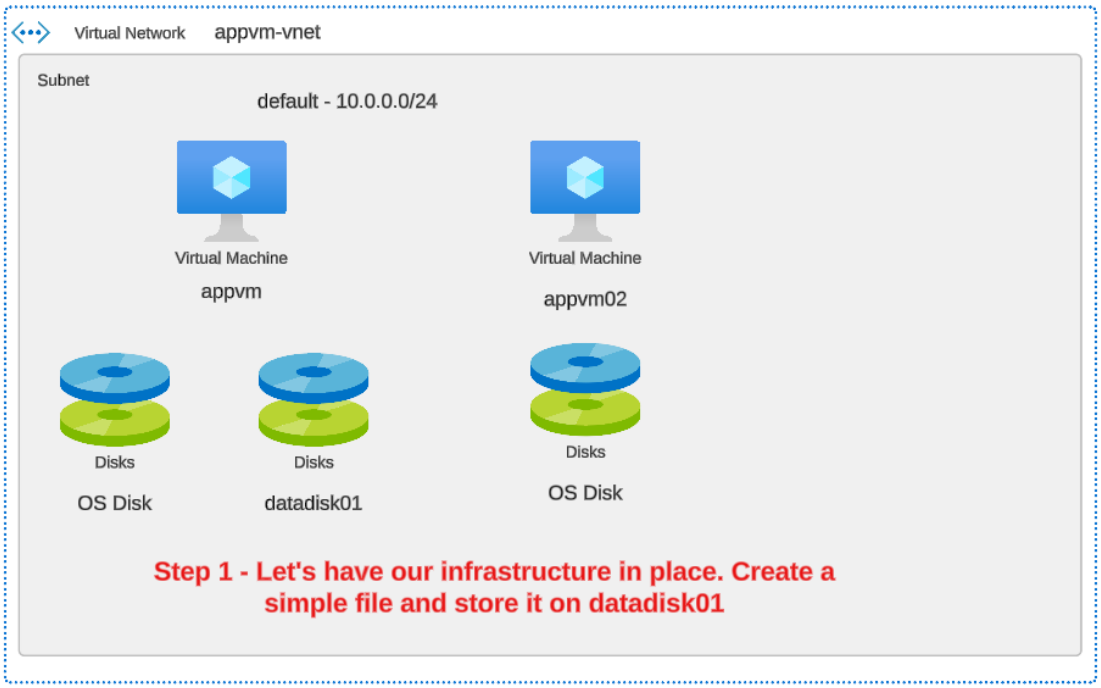
If you need to copy large videos, then a higher throughput is required on the disks.

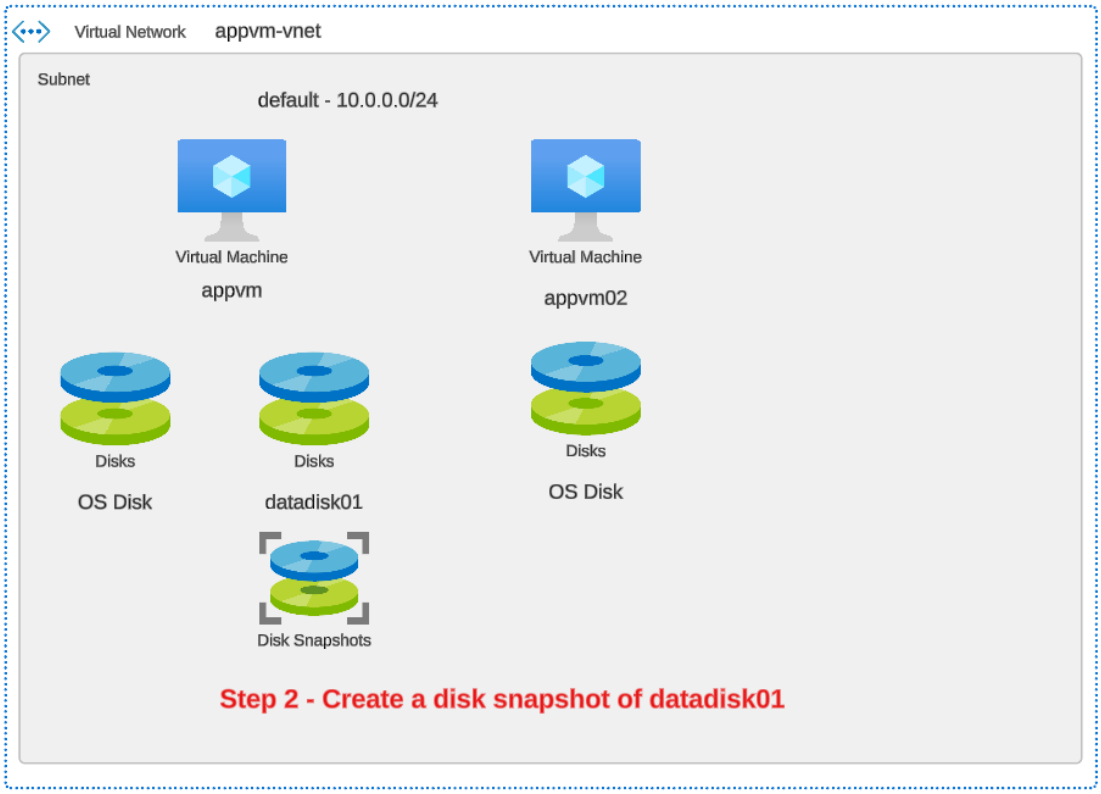


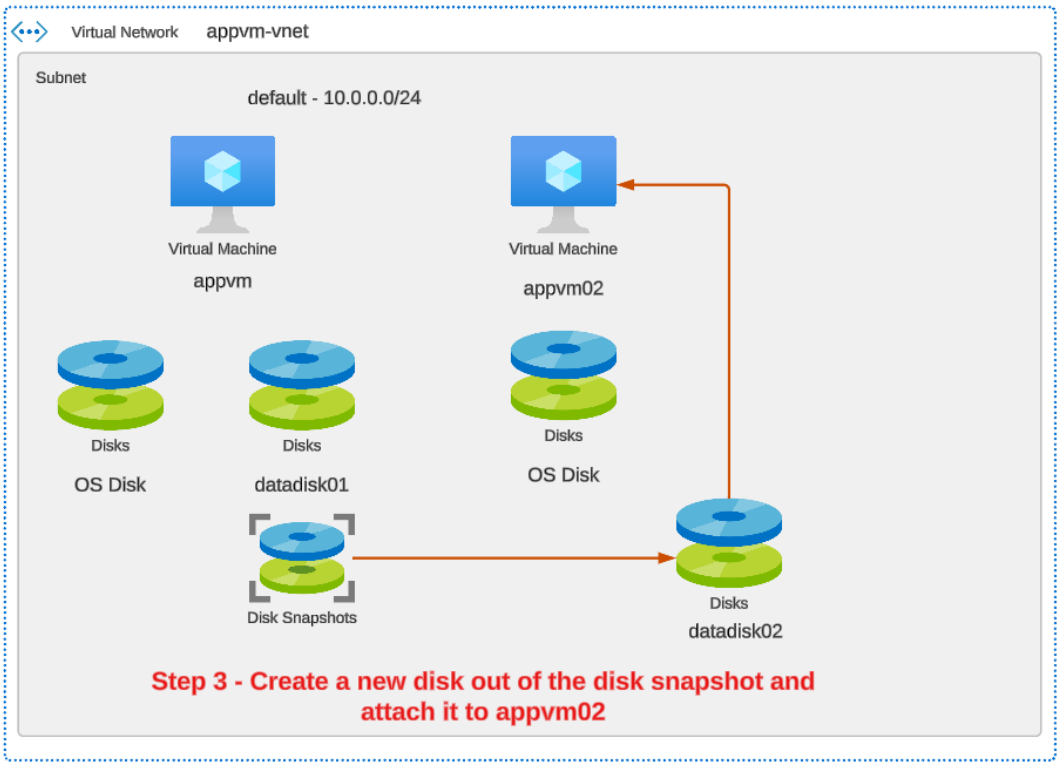
IOPS

If the machine is hosting a database. Many read and write operations occur per second on the database. For this we need higher IOPS - Input/Output operations per second.

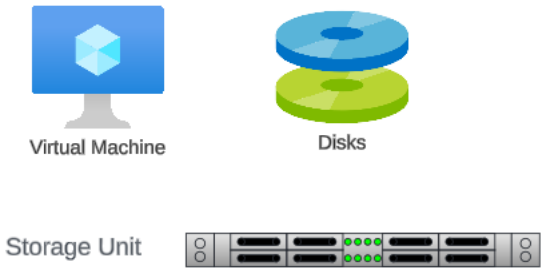
Lab - Data Disks Snapshot






Virtual Network
appvm-vnet
Subnet
default - 10.0.0.0/24
Virtual Machine
appvm
Virtual Machine
appvm02
Disks
OS Disk
Disks
datadisk01
Disks
OS Disk
Disk Snapshots
Disks
datadisk02
Step 3 - Create a new disk out of the disk snapshot and attach it to appvm02

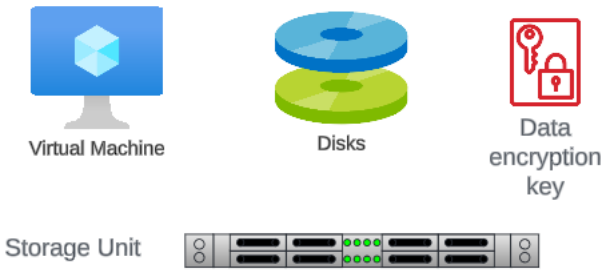
Azure Disks - Server Side Encryption



The disks are stored on Storage Units in the Azure data center. There are many security protocols in place at the data center to protect the infrastructure.

But in the end you as the customer are responsible for the data that you store on Azure.

You can encrypt your data when it comes to disks using a variety of options.



Here when the data is finally stored, it is encrypted using an encryption key and an algorithm. So even if a malicious user were to get hold of the data, they would need the key and know the algorithm used to decrypt the data.

Server-Side Encryption - Here the disks are encrypted with Azure Storage Encryption.

You can use either Platform Managed keys or Customer managed keys.

You can use the Azure Key Vault service to store the encryption keys that can be used as Customer managed keys.

Lab - Disk Encryption Sets

Managed service on Azure for storing secrets , certificates and encryption keys.

We want to encrypt the data on the disks using a key defined in the key vault.

Note that the entire process of encryption and decryption happens in the background.

First we need to create a key vault - This needs to be in the same region and subscription as the virtual machine and disks.

Soft delete and purge protection must be enabled for the key vault.

Ensure that role-based access control is set for the key vault.

Create a disk encryption set

This set can then be used to encrypt the disks.

Custom Script Extensions

Custom Script Extensions

This feature can be used to download and run scripts on Azure virtual machines.

These scripts could reside in Azure Storage or GitHub.

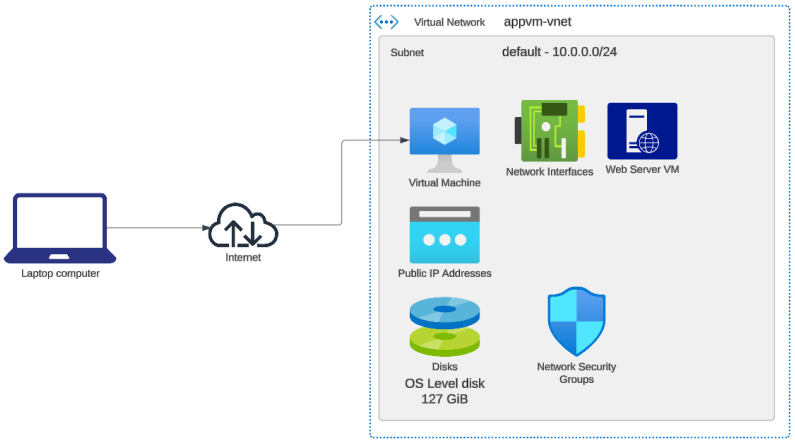
This is useful if you want to run any task post the deployment of the virtual machine.

Ensure the scripts don't require any user input when they run.

The script is allowed 90 minutes to run.

Don't put any restart instructions in the script.

What are we going to do



Earlier on we saw how we could install Internet Information Services as a role on a Windows Server machine.

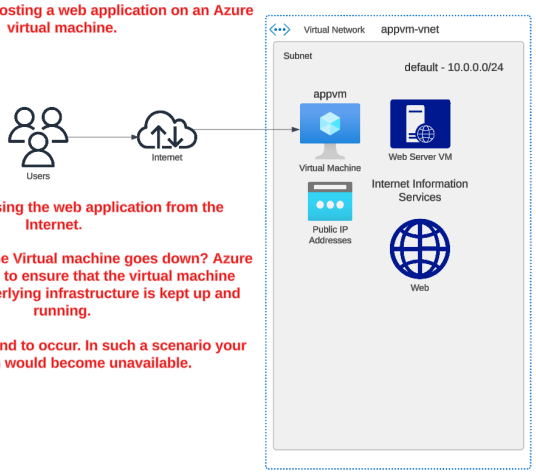
We had manually logged into the machine and installed the role.

We are going to create a PowerShell script file that will automate the installation of Internet Information Services.

When creating the machine, we will use Custom Script Extensions to pick up the PowerShell script file to perform the required installation.

Availability Sets

Your company is hosting a web application on an Azure virtual machine.

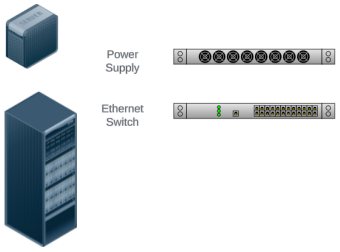


Users are accessing the web application from the Internet.

What happens if the Virtual machine goes down? Azure does everything to ensure that the virtual machine service, the underlying infrastructure is kept up and running.

But issues are bound to occur. In such a scenario your application would become unavailable.

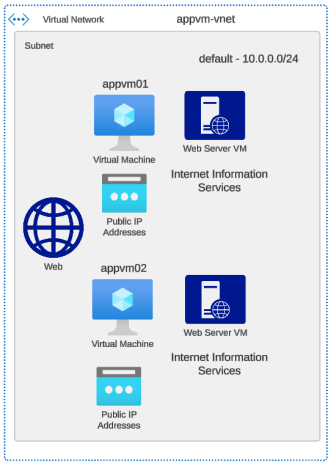
There could be faults in the underlying physical layer, maybe a network issue, a power issue.



Sometimes Microsoft also has to perform vital updates to the physical machines that host the virtual machines. At that point in time, a reboot of the physical server could be required. This would again cause a disruption to the application.

We need to look at increasing the availability of our system.

You can look towards hosting your application on multiple virtual machines.



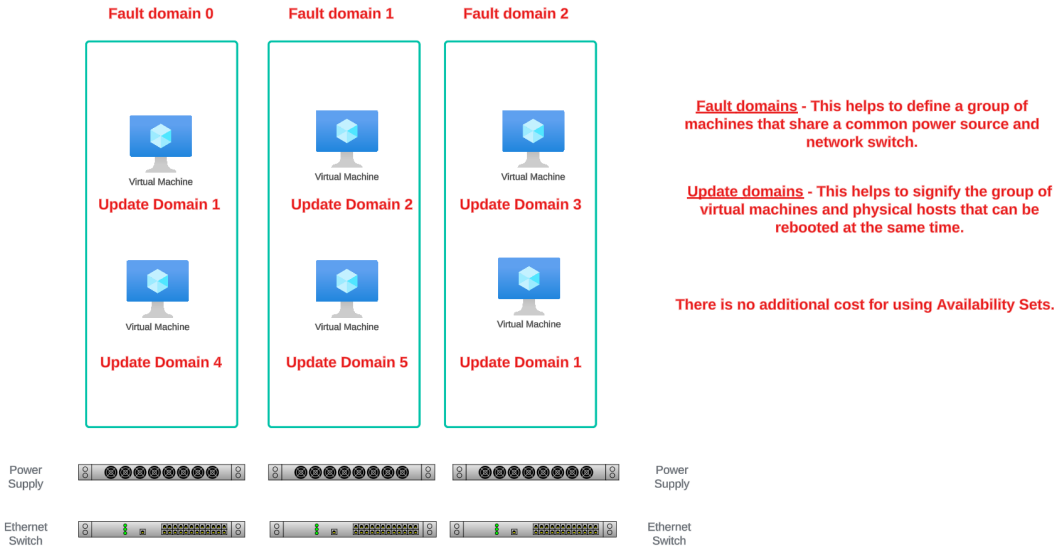
But what happens if both virtual machines are launched on the same physical server. By default we can't specify the underlying physical servers for the virtual machines.

Availability sets

This is a logical grouping of machines that helps to reduce the chances of multiple VM's going down because of hardware issues.

To make use of Availability sets, you need to deploy a Virtual Machine to an Availability Set. You can just create an Availability Set and deploy the machine to the set. The machine can only be part of a set when the machine is created.

The virtual machine is placed as part of a fault and update domain in the Availability set.



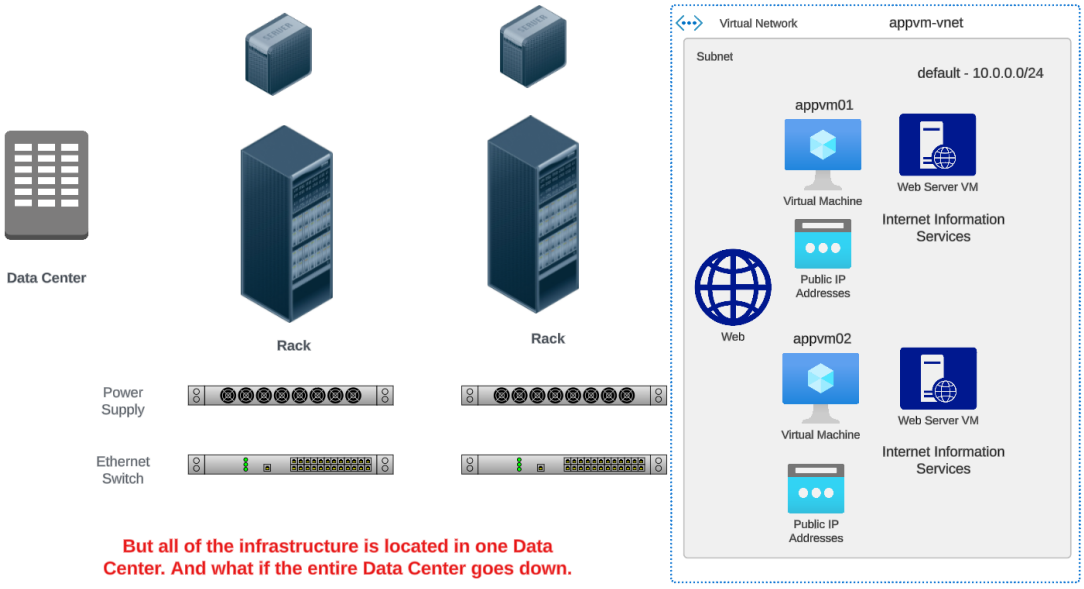
Fault domains - This helps to define a group of machines that share a common power source and network switch.

Update domains - This helps to signify the group of virtual machines and physical hosts that can be rebooted at the same time.

There is no additional cost for using Availability Sets.

Availability Zones

We learnt about the concept where we can spread virtual machines across multiple power supply and network switches via the use of Availability sets.

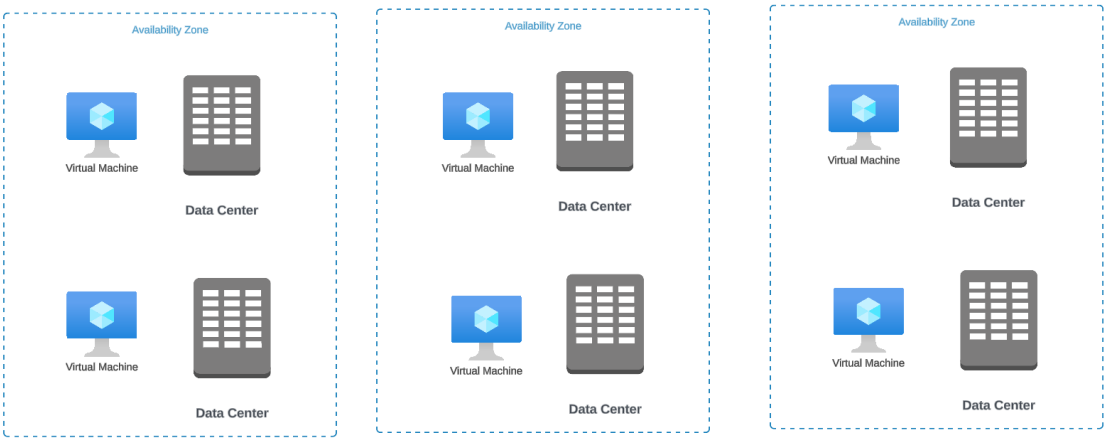


But all of the infrastructure is located in one Data Center. And what if the entire Data Center goes down.

You can spread your infrastructure across multiple Availability Zones.

An Availability zone is a group of data centers. There are fast links across Availability Zones to ensure low latency.

An Azure region has multiple Availability zones.



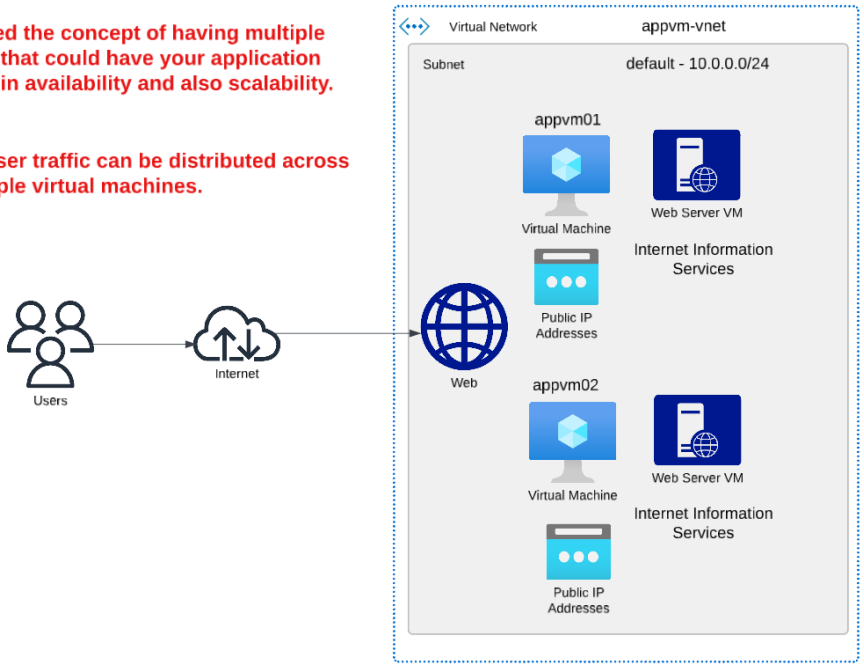
Data Transfer	Price
Data Transfer In	Free
Data transfer between Availability Zones(Egress and Ingress)*	$0.01 per GB
Data transfer within same Availability Zone	Free

There is no cost for using an Availability zone, but there is a bandwidth cost.

Azure virtual machine scale sets

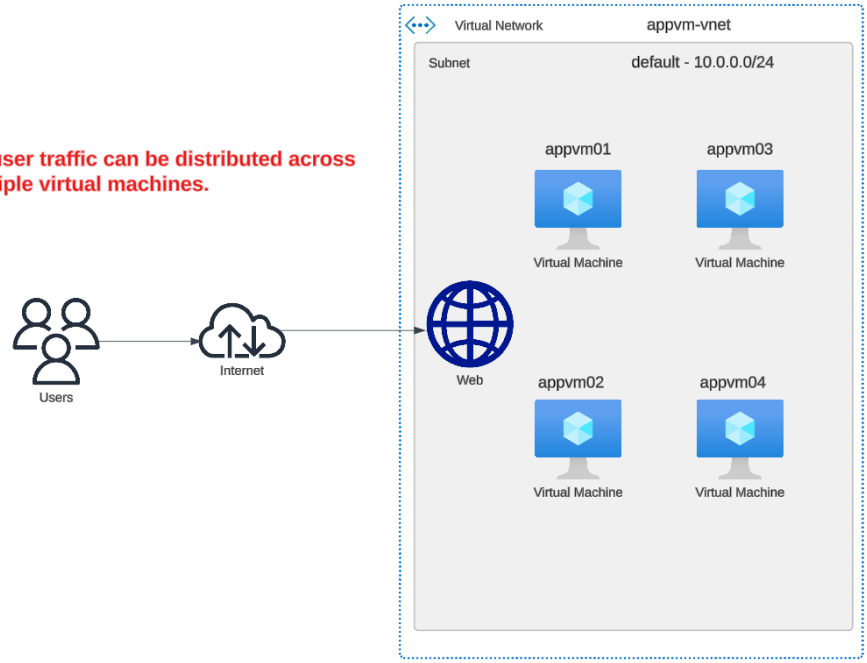
Earlier we discussed the concept of having multiple machines in place that could have your application running. This helps in availability and also scalability.

By Scalability, the user traffic can be distributed across multiple virtual machines.



But maybe the user traffic has increased so much that we need more number of virtual machines. So we create more machines to handle the user load on the application.

By Scalability, the user traffic can be distributed across multiple virtual machines.



But maybe the traffic is high during the day time and light during the night time and we don't need so many machines during the night. Why does this concern us? Well the cost of having machines in place.

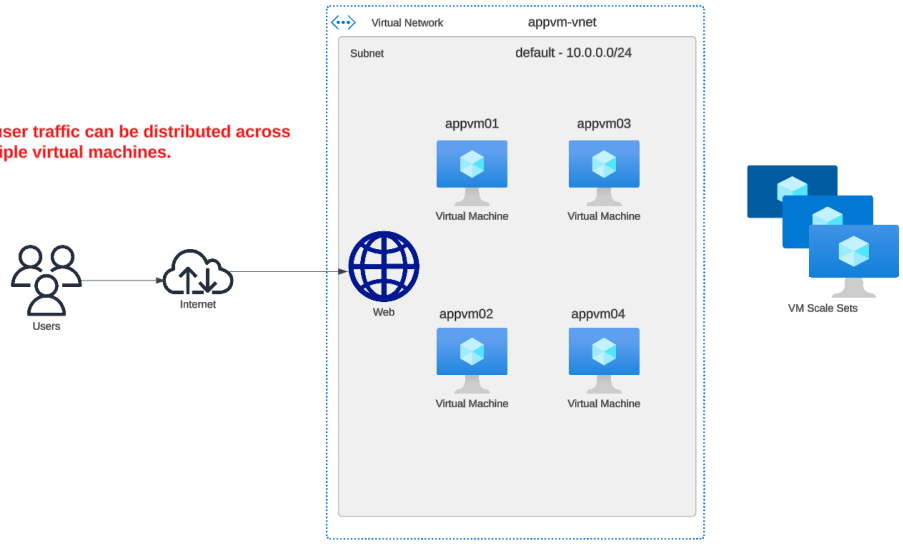
Are you manually going to monitor whether the traffic is high or low, and create and delete machines whenever required.

Azure virtual machine scale sets

This service helps you to create and manage a group of load balanced virtual machines.

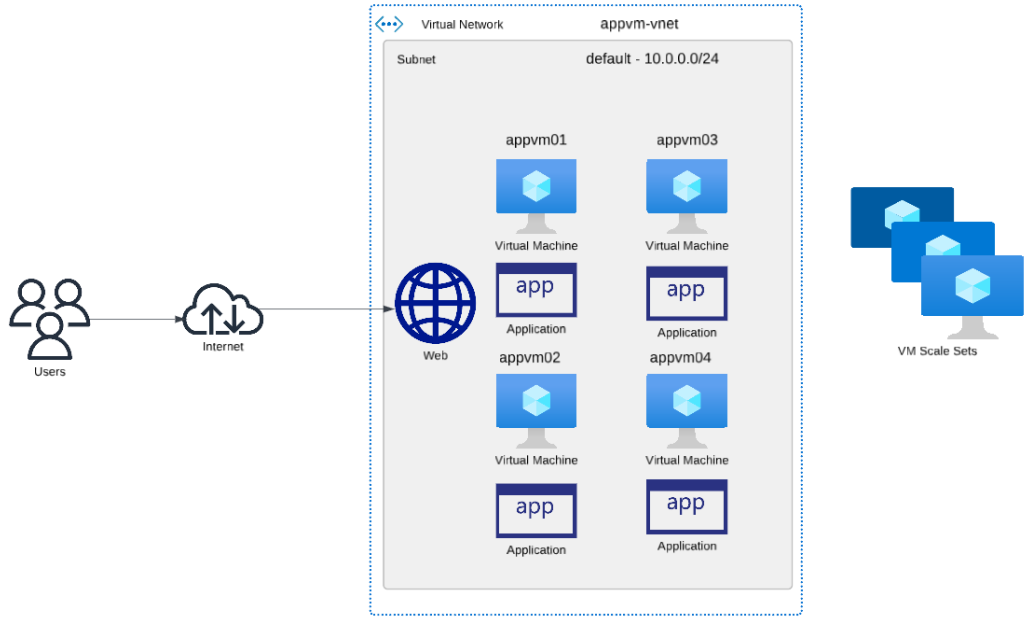
The number of virtual machines can then grow based on demand or on a schedule.

By Scalability, the user traffic can be distributed across multiple virtual machines.



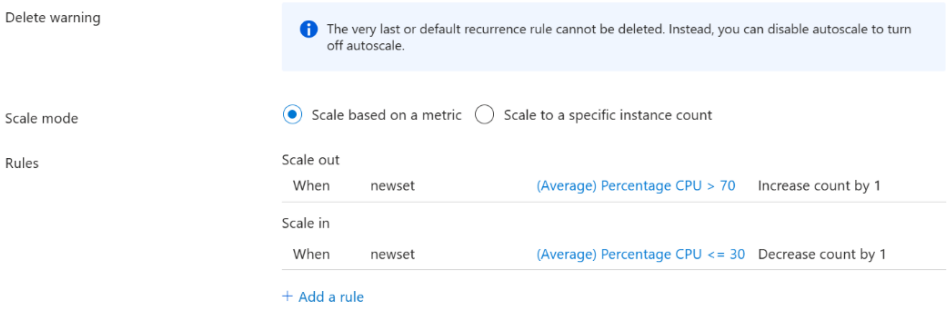
Your machines can be managed by the virtual machine scale set service. You can define rules to define different scaling conditions.

Virtual Machine Scale Sets - More aspects



The virtual machine scale set can scale machines based on demand. But what about the application on the machines. Would it ensure that the application also resides on new machines.

Well the application running on each machine is your responsibility. You can use various mechanisms to ensure that applications are up and running on new machines - Custom Script Extensions , Custom images.



Also let's say that you have 2 machines running as part of the scale set, the threshold would consider the metrics of both machines. Which means the overall CPU percentage of both virtual machines will be considered by the scaling rule.

Understanding virtual machine images

Virtual Machine

Application

Let's say that you have a virtual machine that has an application in place and other tools and services as well.

Now let's say that you want to create more virtual machines that has the same set of applications, tools and services.

You could use Custom Script Extensions to install the applications, tools etc. But it could take time to have the machine in place if the installation process takes time.

Instead you can build your own custom image and then create machines based on the image.

The image can have a copy of the full virtual machine that includes the data disks.

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

You can share the Azure compute gallery across your organization so that other users can create virtual machines on the images stored in the gallery.

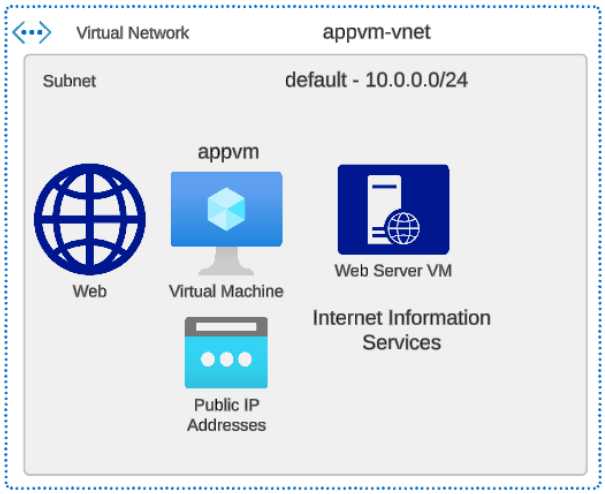
Image Definition - This is a grouping of image versions. Each image definition has information about why the image was created and other information related to the image.

Image Version - This is used to create the virtual machine.

Specialized VM images	Generic VM images
Here information about specific users and machine information is retained.	Here information about specific users and machine information is removed.
Here the new virtual machines will have the same computer name and admin user information.	Here we need to perform the process of generalization. After this the original virtual machine will be unusable.

Introduction onto Azure Web Apps

We understand the concept wherein we can host web applications on Azure virtual machines



Physical server

Azure Datacenter

Azure Web App Service

web application

Azure Websites

Virtual Machine

Physical server

This is a managed service. Here the virtual machine and physical infrastructure is managed for you.

There is support for web applications based on .NET, Java, Node.js, PHP, Python.

Here the patching of the framework and the operating system is managed by the service.

You also get other features such as High Availability.

If you have a web application that fits the framework and you don't want to manage the virtual machines, then you can opt for the Azure Web App service.

But if you need to host a custom application that needs to be installed, then you would probably need to use the Azure virtual machine service.

Deployment Slots

We have deployed our application

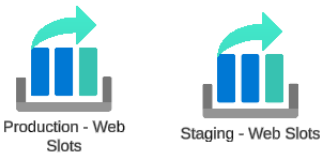
Now before we actually deploy the newer version of the application, we would ideally first want to test the application. At one phase, with a set of business users.

We now have a newer version of the application.

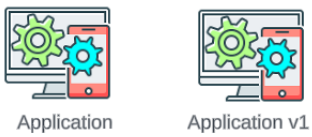
1. Create a new Azure Web App
2. Deploy the newer application
3. Test the application
4. Publish the application after successful testing to the primary Azure Web App

In Azure Web Apps , we can make use of deployment slots.

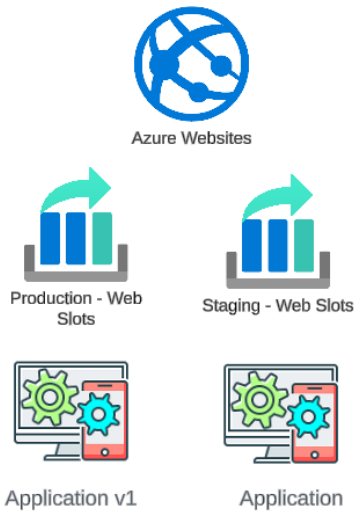
This feature is available with the Standard, Premium and Isolated App Service Plan.



Create a new slot and publish the newer version of the application to the slot.



Each slot is a live web application with its own host name.

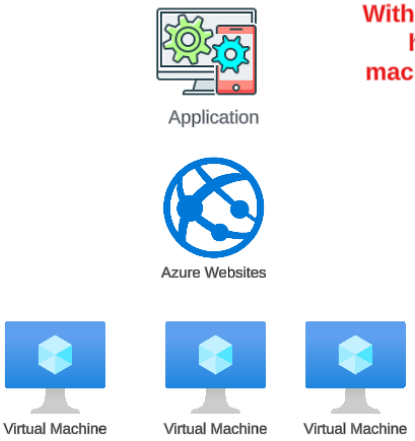


Then at any point in time, you can swap the slots. So that the newer version of the application runs as part of the production slot.

This helps in first testing of the application in the staging slot and then swapping the slots at any point in time.

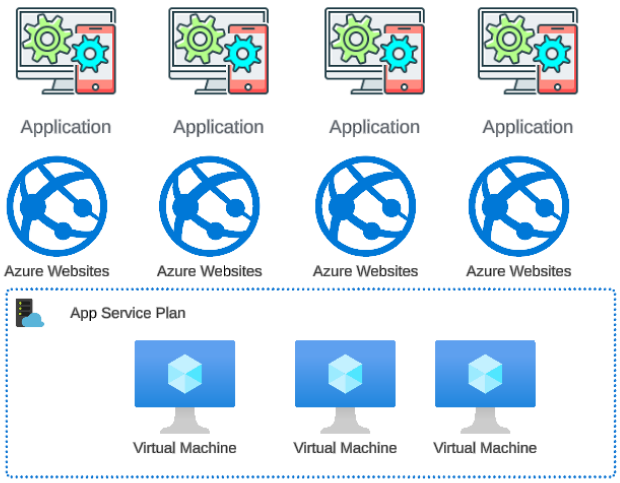
It also helps in recovery from failure. If the swap succeeds , but the newer version of the application is not working, you can easily swap back at any point in time.

Autoscaling for Web Apps



With the Basic App Service Plan or higher, you have dedicated machines that can be used to host your web apps.

For the Basic App Service Plan, you can have a maximum of 3 machines running your Azure Web Apps.



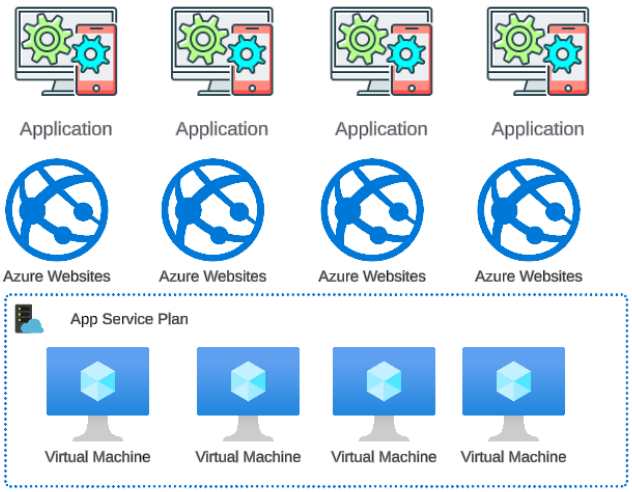
You can define multiple Azure Web Apps that can share the same App Service Plan.

With the Basic App Service Plan , you can manually scale out and scale in the number of machines running as part of your infrastructure - Remember costing of the machines are important.

With the Standard App service plan and higher, you can also configure autoscaling based on rules.

With the Premium App service plan and higher you can configure automatic scaling.

Example - Standard App Service Plan



Here we can have a maximum of 10 machines running as part of our infrastructure.

But instead of manually scaling out or scaling in, we can set rules to autoscale based on conditions.

For example, if the CPU threshold goes beyond 70%, then scale our infrastructure out by one machine. If the CPU threshold goes down, then scale down by one machine.

Using Containers

Virtual Machine

Application

We have seen how to host a web server on a virtual machine.

You can then host your web application on the machine.

Azure Websites

We can also host applications using Azure Web Apps.

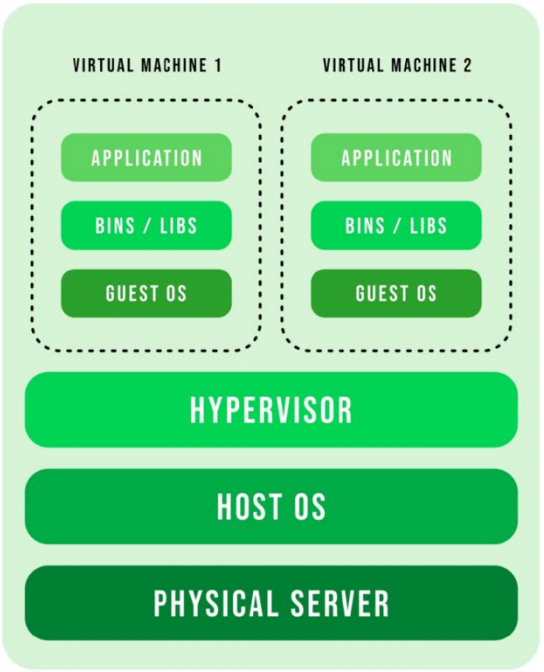
But we can also make use of container-based technologies for hosting applications.

History behind the advent of containers.

History behind the advent of containers.

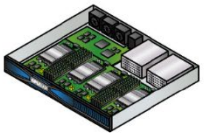
Virtual Machines

These are virtual computers that run on physical machines



VMware / Hyper-V

Linux or Windows



VIRTUAL MACHINE
ARCHITECTURE

Each virtual machine can make use of resources such as CPU/Memory from the

Each virtual machine is isolated from each other.

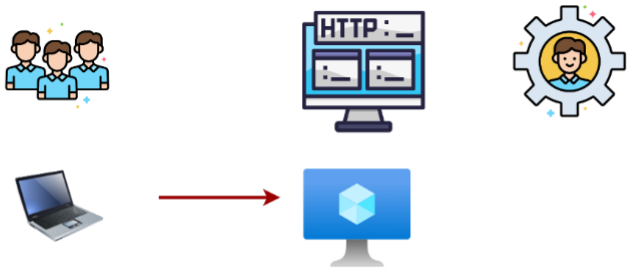
Containers

Having virtual machines was a big breakthrough

Companies could host multiple virtual machines on a physical server and make use of the server.

But then there were issues when it came to deploying applications.

Developers develop the application on their machines



When the application is deployed to a virtual machine it does not work as intended.

This could be because of differences in machine software configuration, libraries not present etc.

You have 2 applications on the same machine.

One application update requires a library/component to be installed.

This causes the other application to stop working.

Welcome to containers

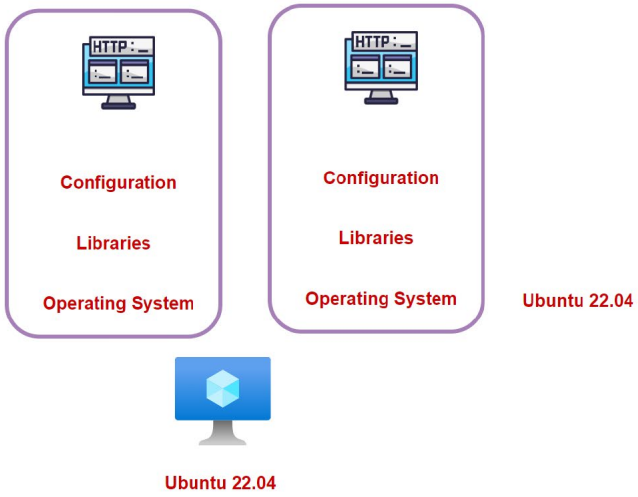
This is a unit of software that packages up all the code and dependencies that are required for the application to run.

dependencies that are required for the application to run.

CONTAINER ARCHITECTURE

The underlying container will have a light-weight operating system, the application, libraries etc.

Each container runs in isolation



Ubuntu 20.04

Ubuntu 22.04

Ubuntu 22.04

Lab - Deploying Docker on a virtual machine

We will first deploy a Linux-based virtual machine.

If you wanted to host a web application , we would first need to install a Web server and then host our web application.

For example, we can install the NGINX web server.

But we will run NGINX via the use of Docker containers.

We will then run the NGINX web server in a Docker-based container.

The container is run by first downloading the NGINX image from an online repository known as Docker Hub.

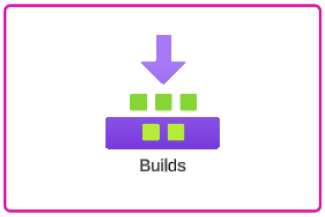
We will first install the Docker tool set on the virtual machine.

The need for an image registry

There are readymade images available on Docker Hub.

You can use these images to run containers.

But let's say we want to run our own application within a container.



We can take our code, create a build and use Docker to first create an image that would contain our application.

We can then run a container out of the image and hence run our application.

We need a place to store our newly created application image. We can store it in Docker Hub. Or use an Azure service known as Azure Container Registry. This is a private registry that can be used for storing your Docker-based images.

Configure and manage virtual networking

Understanding IP addresses

When it comes to computer systems, it only understands binary numbers.

With binary numbers, we only have 0 and 1.

So how can start representing values via the use of binary numbers.

0 0 0 0

0 0 0 1

0 0 1 0

0 0 1 1

0 1 0 0

0 1 0 1

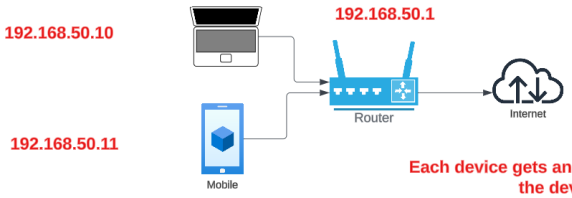
Number of possible values	256	128	64	32	16	8	4	2
	0	0	0	0	0	0	0	0

How can we convert binary values to a decimal value.

Place value	128	64	32	16	8	4	2	1
	0	0	0	0	0	0	0	0
48	0	0	1	1	0	0	0	0

An IP address

This helps to identify a device on a network



Each device gets an IP address. This helps to identify the device on the network.

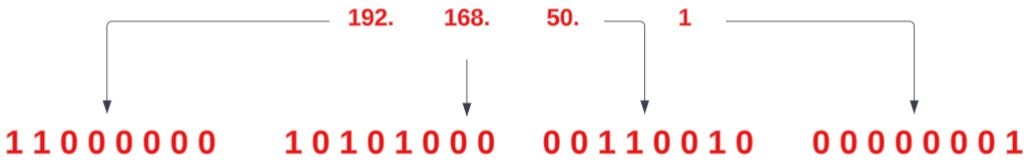
The IP address is a string of numbers that are seperated by periods.

It's just a human readable way of representing the identifier for the device.

It is represented as a 32-bit number.

The entire set of 192.168.50 is used to represent the network id.

The last octet can be used to assign IP addresses to the devices on the network.



So the first 24 bits will always be the same for the network.

We use a network mask to divide the IP address into the network address and the host address.

255.255.255.0

And we can represent the network using a CIDR block - Here the IP address will always have the same network prefix.

192.168.50.0/24

Introduction to Virtual Networks in Azure

This is an isolated network on the cloud.

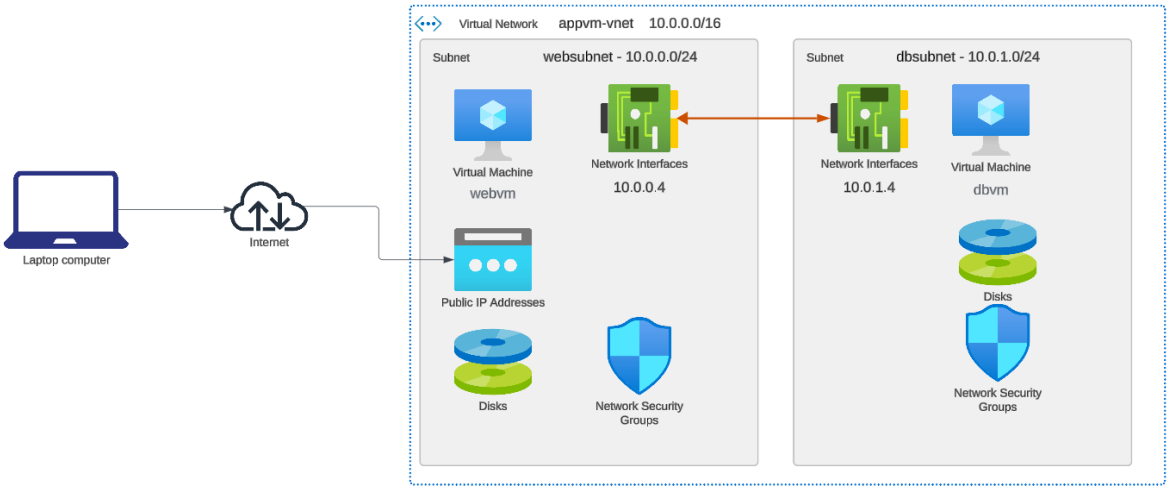
This is similar to having a network in an on-premises data center.

You can host resources such an Azure virtual machines in an Azure virtual network. These resources can securely communicate with each other.

A virtual network is scoped to a particular region and subscription.

You also specify an IP address space for your virtual network.

Concept behind subnets



Subnets help to segregate your workloads within a virtual network.

We can have the web servers located in one subnet and the database servers located in another subnet.

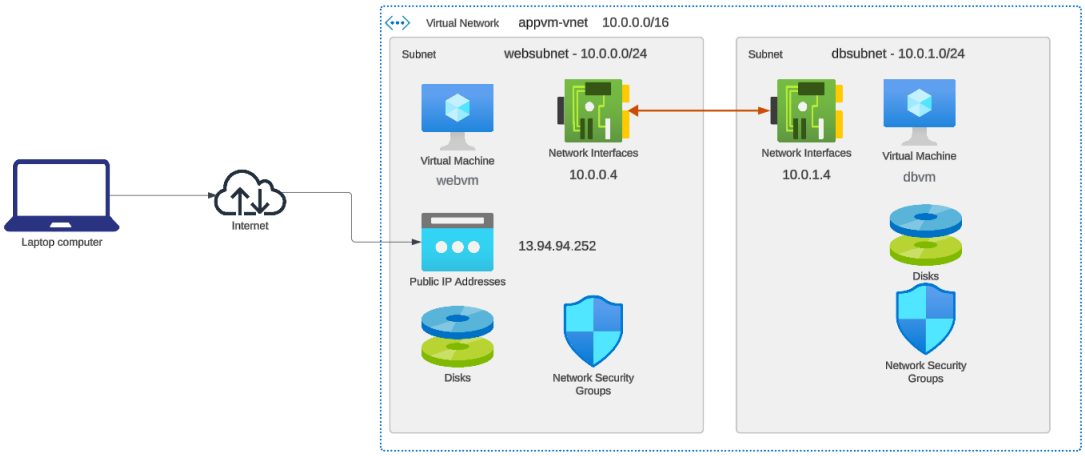
Clients can reach the web server via a Public IP address.

The Web server can talk to the database server on its private IP address.

From a security standpoint we don't need to expose the database server to the Internet.

About IP Addresses

Understanding more on IP addresses



Private IP address allow communication across resources within a network.

Azure reserves the first four IP addresses in each subnet address range.

Private IP Address ranges

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

Public IP addresses allow Internet-based resources to communicate with Azure resources in the network.

2 SKU's or pricing tiers - The Basic tier is going to retire on September 30, 2025

Public IP address	Standard	Basic
Allocation method	Static	For IPv4: Dynamic or Static; For IPv6: Dynamic.
Idle Timeout	Have an adjustable inbound originated flow idle timeout of 4-30 minutes, with a default of 4 minutes, and fixed outbound originated flow idle timeout of 4 minutes.	Have an adjustable inbound originated flow idle timeout of 4-30 minutes, with a default of 4 minutes, and fixed outbound originated flow idle timeout of 4 minutes.
Security	Secure by default model and be closed to inbound traffic when used as a frontend. Allow traffic with network security group (NSG) is required (for example, on the NIC of a virtual machine with a Standard SKU Public IP attached).	Open by default. Network security groups are recommended but optional for restricting inbound or outbound traffic.
Availability zones	Supported. Standard IPs can be nonzonal, zonal, or zone-redundant. **Zone redundant IPs can only be created in regions where 3 availability zones are live.** IPs created before availability zones aren't zone redundant.	Not supported.
Routing preference	Supported to enable more granular control of how traffic is routed between Azure and the Internet.	Not supported.
Global tier	Supported via cross-region load balancers.	Not supported.

Reference - https://learn.microsoft.com/en-us/azure/virtual-network/ip-services/public-ip-addresses

Dynamic IP address - Here the IP address is only assigned when the Public IP address is assigned to a resource. It is released when you stop or delete the resource.

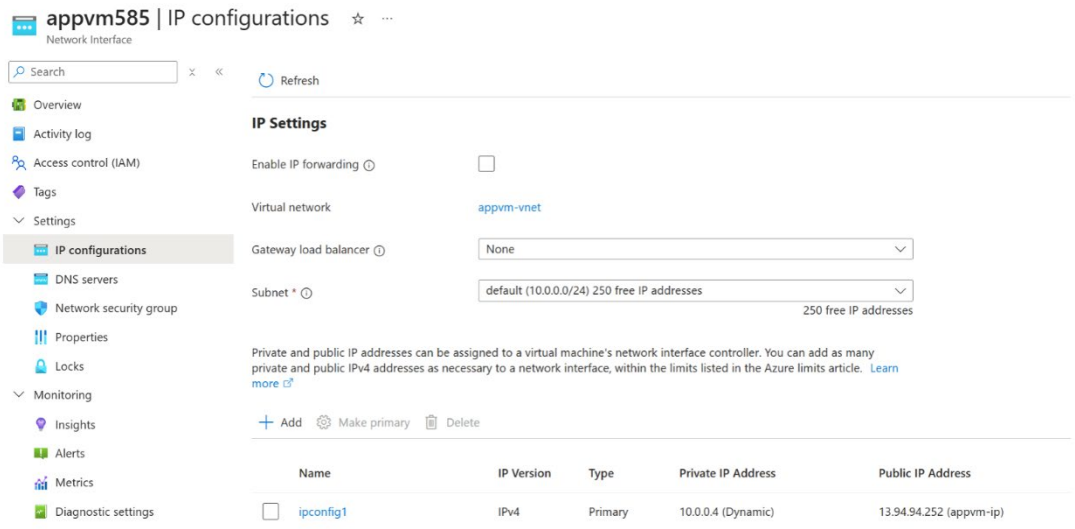
Static IP address - Here the IP address is assigned when it is created. The IP address is released when the resource is deleted.

What's the use of a static IP address

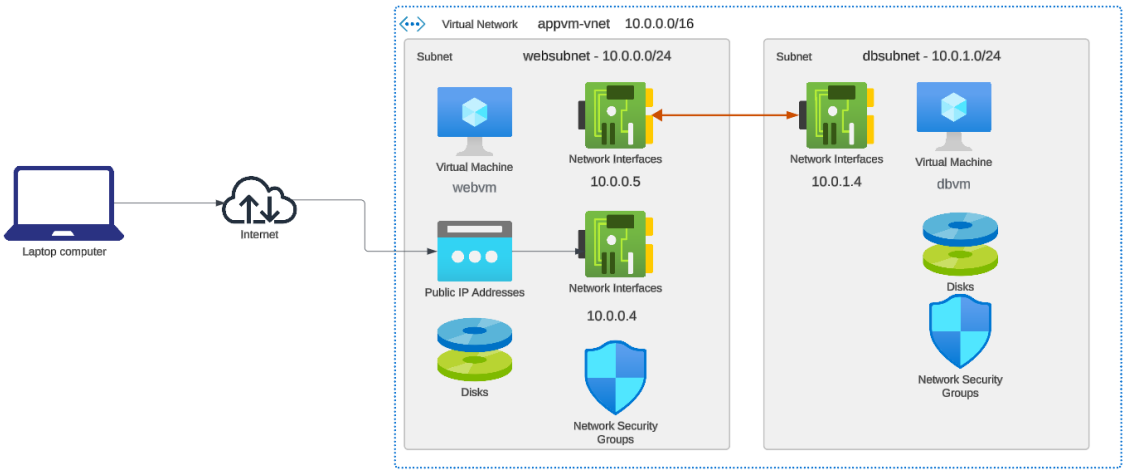
If you had a dynamic IP address and you stop and start the machine, the IP address would change.

www.cloudportalhub.com - 13.94.94.252

The IP addresses are assigned to the Network Interface via an IP configuration.



Lab - Adding a secondary network interface



You can add another network interface to a virtual machine.

You can have one network interface accepting traffic from the Internet. And the other interface forwarding traffic to the machines in the network.

Network Security Groups

Network Security Groups

This is used to filter network traffic between Azure resources in an Azure virtual network.

Here you create Inbound and Outbound rules to allow or deny traffic.

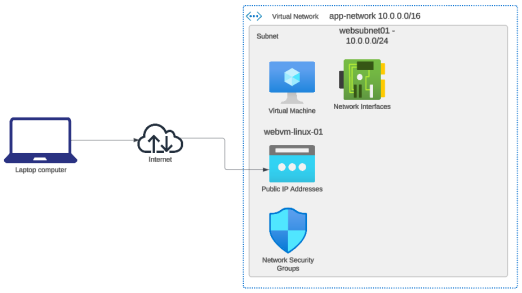
Rules

1. **Name of the rule**
2. **Priority - Rules are processed in the order of priority**
3. **Source or destination - IP address, Service Tag , Application Security Group.**
4. **Protocol - TCP, UDP, ICMP etc.**
5. **Port Range**
6. **Action - Allow or Deny**

Default Rules

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc···	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Network Security Groups - Priority setting



Priority ↑	Name	Port	Protocol	Source	Destination
Inbound port rules (4)					
300	SSH	22	TCP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any
Outbound port rules (3)					
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork
65001	AllowInternetOutBound	Any	Any	Any	Internet
65500	DenyAllOutBound	Any	Any	Any	Any

By default we cannot connect to the web server running on the machine.

Let's then add a rule and ensure we can reach the web server.

Search rules | Source == all | Destination == all | Protocol == all | Action == all

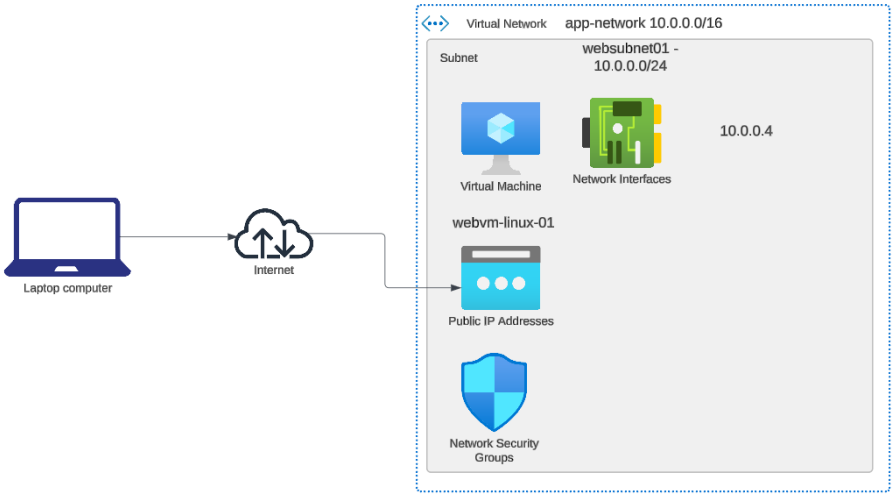
Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (5)						
300	SSH	22	TCP	Any	Any	Allow
310	AllowAnyHTTPInbound	80	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Let's add another rule to Deny traffic on a set of port numbers and have a lower priority number

Inbound port rules (6)						
200	DenyAnyCustom70-100Inbound	70-100	TCP	Any	Any	Deny
300	SSH	22	TCP	Any	Any	Allow
310	AllowAnyHTTPInbound	80	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

The higher priority rule will be evaluated first, it matches the request , hence other rules will not be evaluated.

Lab - Network Security Groups - IP Address

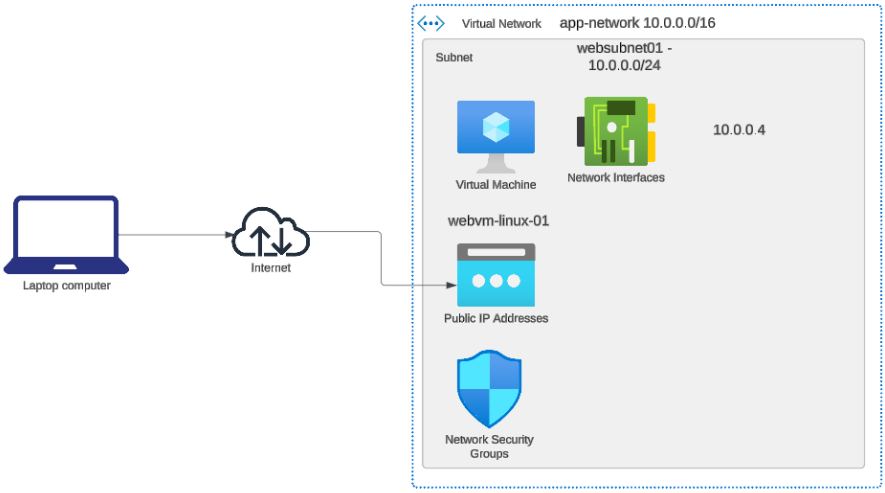


Let"s add a rule this time with a lower priority to allow HTTP traffic, but to just the IP address of the machine.

Inbound port rules (7)

190	Allow80	80	TCP	Any	10.0.0.4	Allov
200	DenyAnyCustom70-100Inbound	70-100	TCP	Any	Any	Deny
300	SSH	22	TCP	Any	Any	Allov
310	AllowAnyHTTPInbound	80	TCP	Any	Any	Allov
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allov
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allov
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Lab - Network Security Groups - Outbound Rules



Let's add an Outbound rule to deny all outbound traffic to the Internet.

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (7)						
190	Allow80	80	TCP	Any	10.0.0.4	Allow
200	DenyAnyCustom70-100Inbound	70-100	TCP	Any	Any	Deny
300	SSH	22	TCP	Any	Any	Allow
310	AllowAnyHTTPInbound	80	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (4)						
320	DenyCidrBlockCustomAnyOutbound	Any	Any	10.0.0.4	Internet	Deny
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Can we still access our web server?

We can still access the web server. When an inbound request is allowed, its stateful in nature. The outbound response will also automatically be allowed.

Then's what the point of the outbound rule - well its for outbound initiation of requests from the virtual machine.

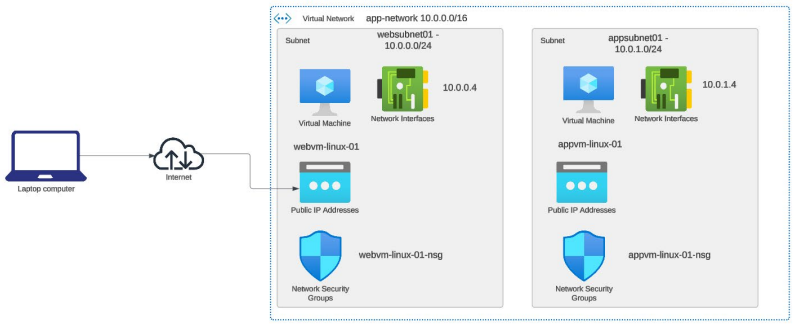
```
linuxadmin@webvm-linux-01:

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
linuxadmin@webvm-linux-01:~$ curl http://10.0.0.4
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
linuxadmin@webvm-linux-01:~$ curl https://portal.azure.com
```

Lab - Network Security Groups - Access to other machines



Let's deploy another Linux-based virtual machine to another subnet in the same virtual network.

No need to deploy any workload on appvm-linux-01

webvm-linux-01-nsg

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
300	SSH	22	TCP	Any	Any	Allow
310	AllowAnyHTTPInbound	80	TCP	94.204.16.49	10.0.0.4	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

appvm-linux-01-nsg

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (4)						
300	SSH	22	TCP	Any	Any	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (3)						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Can we access our web server from appvm-linux-01?

Note here we are using the private IP address to access the web server.

```
linuxadmin@appvm-linux-01:~$ curl 10.0.0.4
<!DOCTYPE html>
<html>
<head>
<title>Welcome to nginx!</title>
<style>
html { color-scheme: light dark; }
body { width: 35em; margin: 0 auto;
font-family: Tahoma, Verdana, Arial, sans-serif; }
</style>
</head>
<body>
<h1>Welcome to nginx!</h1>
<p>If you see this page, the nginx web server is successfully installed and
working. Further configuration is required.</p>

<p>For online documentation and support please refer to
<a href="http://nginx.org/">nginx.org</a>.<br/>
Commercial support is available at
<a href="http://nginx.com/">nginx.com</a>.</p>

<p><em>Thank you for using nginx.</em></p>
</body>
</html>
linuxadmin@appvm-linux-01:~$
```

This works because of the default Inbound port rule to allow traffic across the virtual network.

For webvm-linux-01 , let's add a rule to Deny all traffic from anywhere - Normally a Deny rule is added for security purposes.

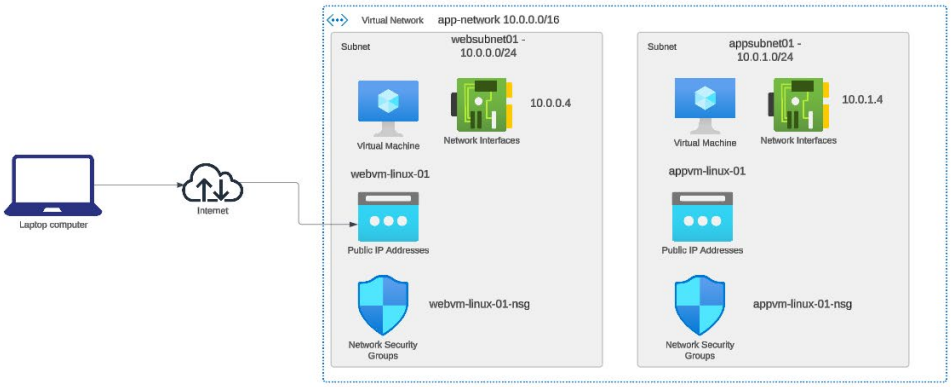
Now try to access the web server from appvm-linux-01

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (6)						
300	⚠ SSH	22	TCP	Any	Any	Allow
310	AllowAnyHTTPInbound	80	TCP	94.204.16.49	10.0.0.4	Allow
320	⚠ DenyAnyCustomAnyInbound	Any	Any	Any	Any	Deny
65000	AllowVnetInBound ⓘ	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound ⓘ	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound ⓘ	Any	Any	Any	Any	Deny
Outbound port rules (3)						
65000	AllowVnetOutBound ⓘ	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound ⓘ	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound ⓘ	Any	Any	Any	Any	Deny

Let's add a rule to only allow traffic from appvm-linux-01 to webvm-linux-01 to access the web server.

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (7)						
300	⚠ SSH	22	TCP	Any	Any	Allow
310	AllowAnyHTTPInbound	80	TCP	94.204.16.49	10.0.0.4	Allow
315	AllowWeb80FromAppvm	80	TCP	10.0.1.4	10.0.0.4	Allow
320	⚠ DenyAnyCustomAnyInbound	Any	Any	Any	Any	Deny
65000	AllowVnetInBound ⓘ	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound ⓘ	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound ⓘ	Any	Any	Any	Any	Deny
Outbound port rules (3)						
65000	AllowVnetOutBound ⓘ	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound ⓘ	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound ⓘ	Any	Any	Any	Any	Deny

Lab - Network Security Groups - Allow ICMP



Can we send a ping request from one machine to another.

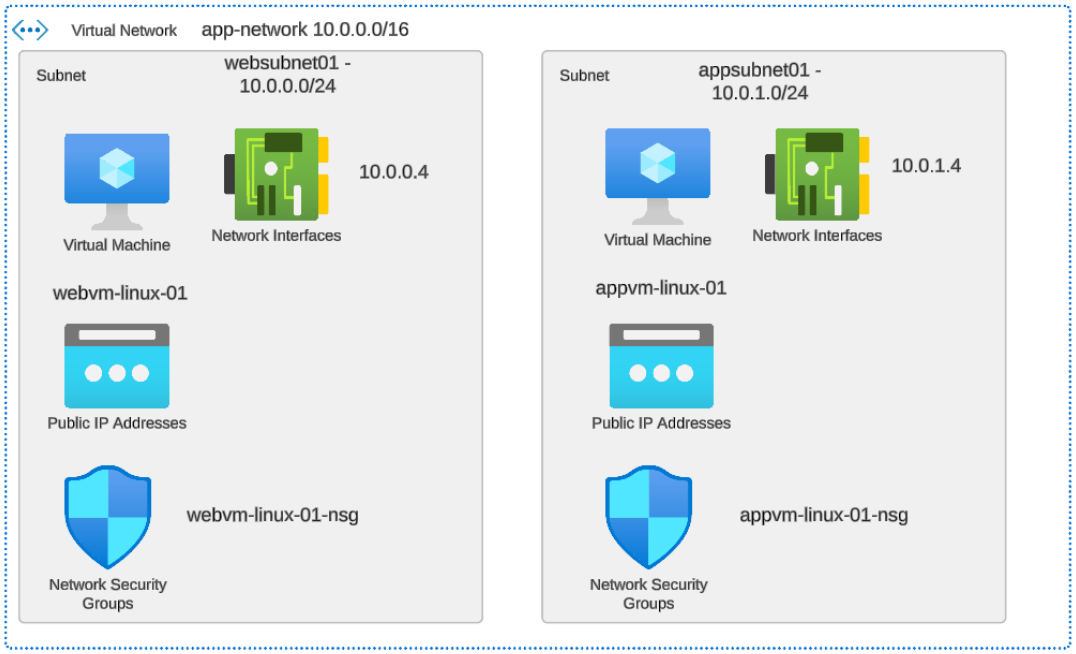
We will need to add rules in order to allow the ping request.

webvm-linux-01-nsg

Priority ↑	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (8)						
300	SSH	22	TCP	Any	Any	Allow
310	AllowAnyHTTPInbound	80	TCP	94.204.16.49	10.0.0.4	Allow
315	AllowWeb80FromAppvm	80	TCP	10.0.1.4	10.0.0.4	Allow
316	AllowICMP	Any	ICMP	10.0.1.4	10.0.0.4	Allow
320	DenyAnyCustomAnyInbound	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound port rules (3)						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

And now the ping request should work.

Lab - Network Security Groups – Subnets



We can also define Network Security Groups at the subnet level.

We can create a new network security group and associate that NSG with both subnets.

We can detach the NSG's at the network interface level.

We can detach the NSG's at the network interface level.

And let's have the following rules

Priority	Name	Port	Protocol	Source	Destination	Action
300	AllowMyIpAddressSSH...	22	TCP	94.204.16.49	10.0.0.4,10.0.1.4	Allow
310	AllowMyIpAddressHTT...	80	TCP	94.204.16.49	10.0.0.4	Allow
315	AllowAppvmHTTPInbo...	80	TCP	10.0.1.4	10.0.0.4	Allow
320	AllowICMPCustomAnyI...	Any	ICMP	10.0.1.4	10.0.0.4	Allow
500	DenyAnyCustomA...	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Lab - Network Security Groups - Multiple NSG's

app-nsg

Let's delete and keep the basic rules for webvm-linux-01-nsg and attach it back to webvm-linux-01

Inbound

appnetwork-nsg

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
300	AllowMyIpAddressSSHi...	22	TCP	94.204.16.49	10.0.0.4,10.0.1.4	Allow
310	AllowMyIpAddressHTT...	80	TCP	94.204.16.49	10.0.0.4	Allow
315	AllowAppvmHTTPInbo...	80	TCP	10.0.1.4	10.0.0.4	Allow
320	AllowICMPCustomAnyI...	Any	ICMP	10.0.1.4	10.0.0.4	Allow
500	DenyAnyCustomA...	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Inbound

webvm-linux-01-nsg

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
320	DenyAnyCustomA...	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

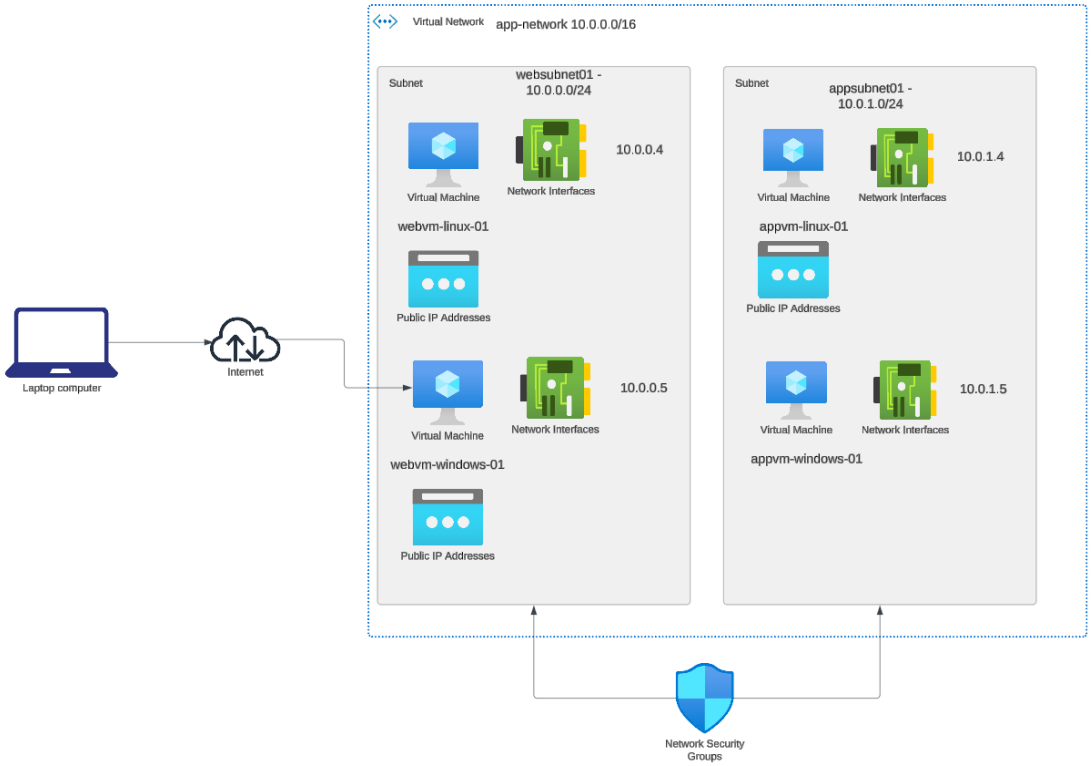
Can we reach the web server running on webvm-linux-01 from our laptop?

The request needs to be allowed both at the subnet layer and the network interface layer.

Let's add a rule for this.

Priority	Name	Port	Protocol	Source	Destination	Action
300	SSH	22	TCP	Any	Any	Allow
315	AllowMyIpAddressHTT...	80	TCP	94.204.16.49	Any	Allow
320	DenyAnyCustomA...	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Lab - Network Security Groups - Windows servers



Let's deploy Azure virtual machines based on Windows Server in both subnets

While creating the virtual machines, let's not create network security groups for the machines.

When creating the Windows machine in appsubnet01 let's not assign a Public IP address also.

Let's view the effective network security groups for each windows-based machine. We should only be having the NSG at the subnet layer.

Let's then RDP into webvm-windows-01 machine from our laptop.

Then from webvm-windows-01 , let's RDP into appvm-windows-01

In order to RDP into webvm-windows-01, we will need to add an inbound port rule.

Priority	Name	Port	Protocol	Source	Destination	Action
300	AllowMyIpAddressSSH···	22	TCP	94.204.16.49	10.0.0.4,10.0.1.4	Allow
310	AllowMyIpAddressHTT···	80	TCP	94.204.16.49	10.0.0.4	Allow
315	AllowAppvmHTTPInbo···	80	TCP	10.0.1.4	10.0.0.4	Allow
316	AllowMyIpAddressRDP···	3389	TCP	94.204.16.49	10.0.0.5	Allow
320	AllowICMPCustomAnyI···	Any	ICMP	10.0.1.4	10.0.0.4	Allow
500	DenyAnyCustomA···	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc···	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Then when logging from webvm-windows-01 to appvm-windows-01, we will use the private IP address of appvm-windows-01.

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound port rules (10)						
300	AllowMyIpAddressSSHInbound	22	TCP	94.204.16.49	10.0.0.4,10.0.1.4	Allow
310	AllowMyIpAddressHTTPInbound	80	TCP	94.204.16.49	10.0.0.4	Allow
315	AllowAppvmHTTPInbound	80	TCP	10.0.1.4	10.0.0.4	Allow
316	AllowMyIpAddressRDPInbound	3389	TCP	94.204.16.49	10.0.0.5	Allow
317	AllowCidrBlockRDPInbound	3389	TCP	10.0.0.5	10.0.1.5	Allow
320	AllowICMPCustomAnyInbound	Any	ICMP	10.0.1.4	10.0.0.4	Allow
500	DenyAnyCustomAnyInbound	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

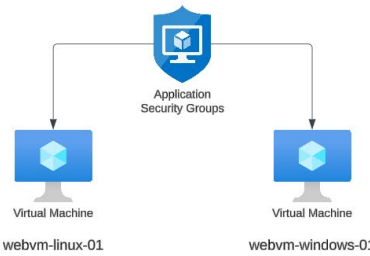
Note - If we did not have the DenyAnyCustomAnyInbound rule, the default AllowVnetInBound rule would allow the RDP traffic into the virtual machine.

Application Security Groups

These helps to group virtual machines together.

Then instead of allowing connections to individual machines in NSG's, we can allow access to Application Security Groups.

Create an Application Security group - appnetwork-asg

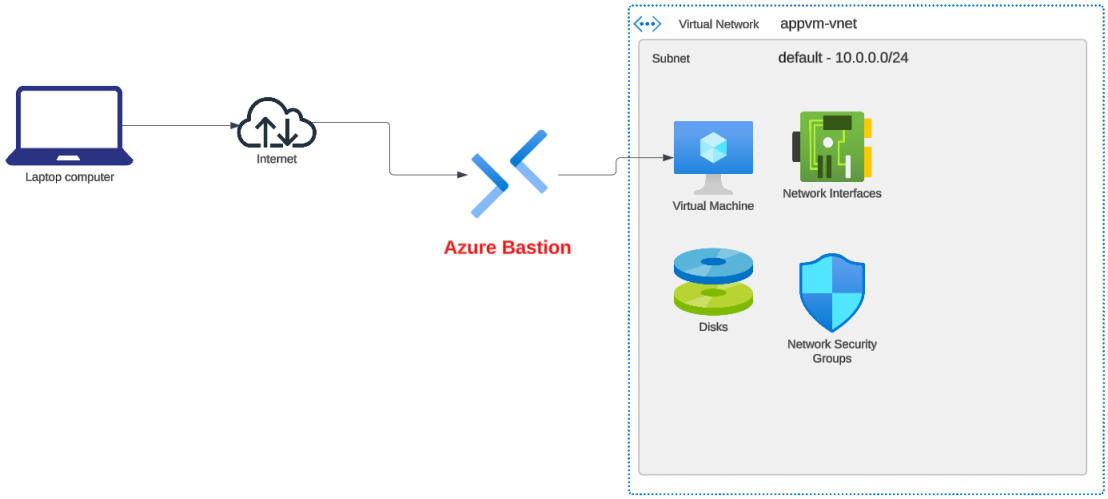


We can then associate the machines in websubnet01 with appnetwork-asg.

Then in the Network Security Group, instead of mentioning IP addresses, we can use the ASG to group virtual machines with the same purpose and use them accordingly.

Priority	Name	Port	Protocol	Source	Destination	Action
300	AllowMyIpAddressSS···	22	TCP	94.204.16.49	10.0.0.4,10.0.1.4	Allow
310	AllowMyIpAddres···	80	TCP	94.204.16.49	appnetwork-asg	Allow
315	AllowAppvmHTTP···	80	TCP	10.0.1.4	appnetwork-asg	Allow
316	AllowMyIpAddressRD···	3389	TCP	94.204.16.49	10.0.0.5	Allow
317	AllowCidrBlockRDPInb···	3389	TCP	10.0.0.5	10.0.1.5	Allow
320	AllowICMPCustomAny···	Any	ICMP	10.0.1.4	10.0.0.4	Allow
500	DenyAnyCustomA···	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan···	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Azure Bastion



This is a fully managed service that provides secure connections to virtual machines without the need of machines needing to have a Public IP address.

You can establish RDP and SSH connections to virtual machines from the Azure Portal.

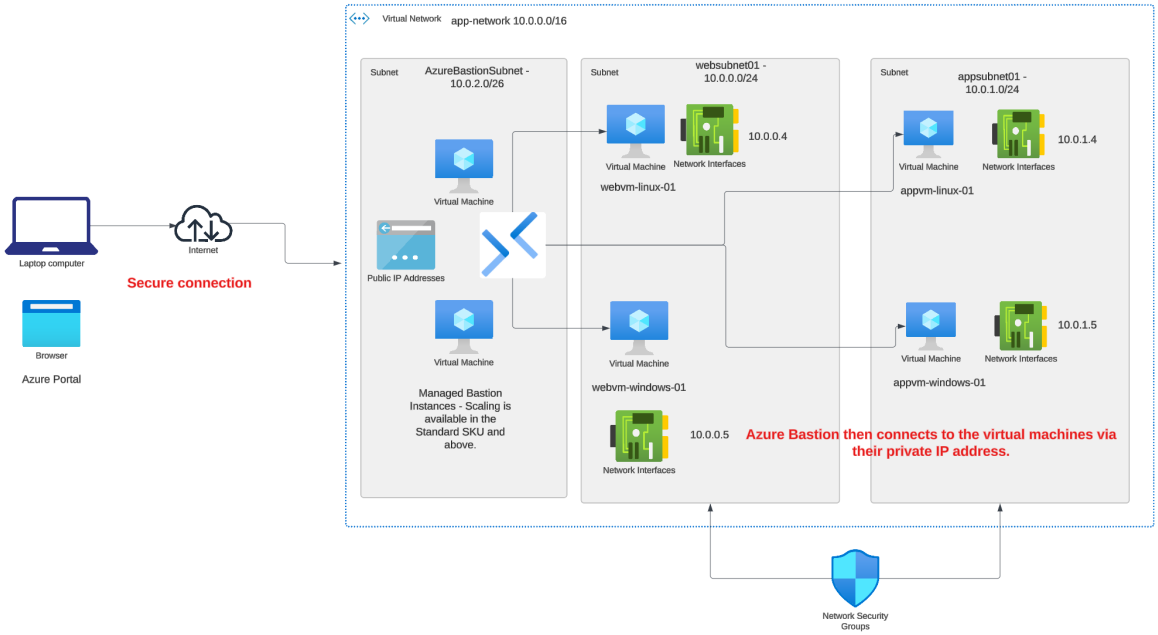
Different SKU's available

Feature	Developer SKU	Basic SKU	Standard SKU	Premium SKU
Connect to target VMs in same virtual network	Yes	Yes	Yes	Yes
Connect to target VMs in peered virtual networks	No	Yes	Yes	Yes
Support for concurrent connections	No	Yes	Yes	Yes
Access Linux VM Private Keys in Azure Key Vault (AKV)	No	Yes	Yes	Yes
Connect to Linux VM using SSH	Yes	Yes	Yes	Yes
Connect to Windows VM using RDP	Yes	Yes	Yes	Yes
Connect to Linux VM using RDP	No	No	Yes	Yes
Connect to Windows VM using SSH	No	No	Yes	Yes
Specify custom inbound port	No	No	Yes	Yes
Connect to VMs using Azure CLI	No	No	Yes	Yes
Host scaling	No	No	Yes	Yes

Reference - https://learn.microsoft.com/en-us/azure/bastion/bastion-overview

	Price[2]
Azure Bastion Developer	Free
Azure Bastion Basic	$0.19 per hour
Azure Bastion Standard	$0.29 per hour
Additional Standard Instance[1]	$0.14 per hour
Azure Bastion Premium	$0.45 per hour
Additional Premium Instance[1]	$0.22 per hour

Reference - https://azure.microsoft.com/en-us/pricing/details/azure-bastion/



We need to deploy a new subnet to the virtual network. This subnet needs to have the name of AzureBastionSubnet.

The Azure Bastion managed instances are deployed to this subnet.

The Azure Bastion host will have a public IP address.

We can diassociate the Public IP addresses from the virtual machines.

Note:- If we disassociate the Public IP address from the VM hosting the web server , we will not be able to reach the web server from the Internet.

Also ensure that we don't have any NSG's attached to the network interfaces.

From an NSG perspective we need to ensure a rule is present to allow the Azure Bastion host to access the virtual machines.

The minimum size of AzureBastionSubnet needs to be /26

We don't need the SSH and RDP rules from my Public IP address to the machines, because now we need to connect via the Bastion Host.

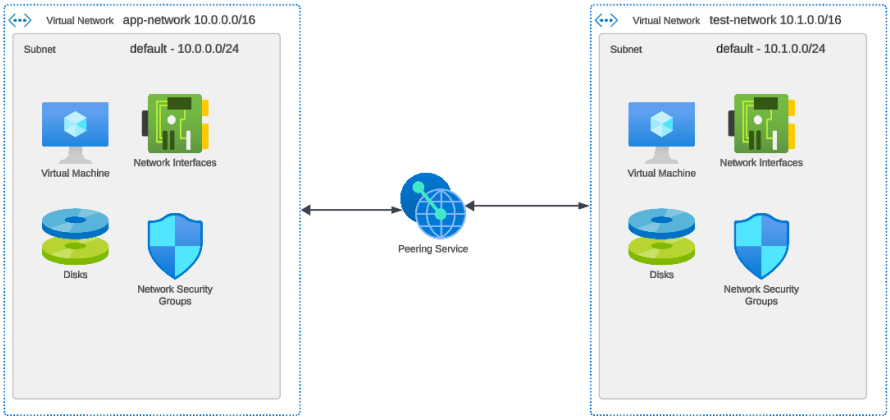
Also for the sake of simplicity let's delete other rules and only have the rules which are required for connectivity purposes.

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
300	AllowMyIpAddressSS...	22	TCP	94.204.16.49	10.0.0.4,10.0.1.4	Allow
310	AllowMyIpAddres...	80	TCP	94.204.16.49	appnetwork-asg	Allow
315	AllowAppvmHTTP...	80	TCP	10.0.1.4	appnetwork-asg	Allow
316	AllowMyIpAddressRD...	3389	TCP	94.204.16.49	10.0.0.5	Allow
317	AllowCidrBlockRDPInb...	3389	TCP	10.0.0.5	10.0.1.5	Allow
320	AllowICMPCustomAny...	Any	ICMP	10.0.1.4	10.0.0.4	Allow
500	DenyAnyCustomA...	Any	Any	Any	Any	Deny
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Priority	Name	Port	Protocol	Source	Destination	Action
Inbound Security Rules						
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound Security Rules						
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

If you do decide to have an NSG associated with the Azure Bastion Subnet, below are the NSG rules required.

Virtual Network Peering

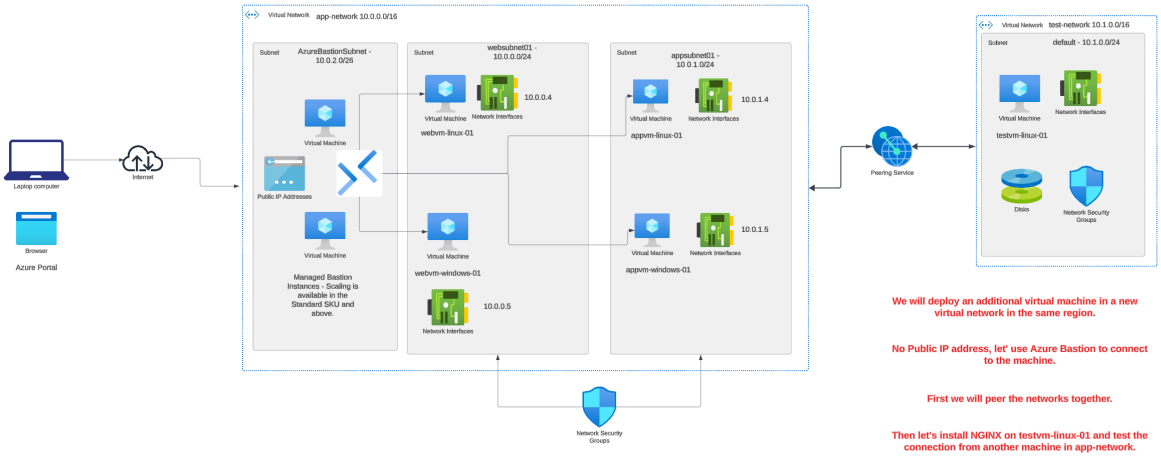


This services allows you to connect virtual networks together.

The traffic across the virtual machines uses the Microsoft backbone network.

You can connect Azure virtual networks in the same region or across regions.

When peering virtual networks together, they cannot have overlapping CIDR blocks.



User Defined Routes

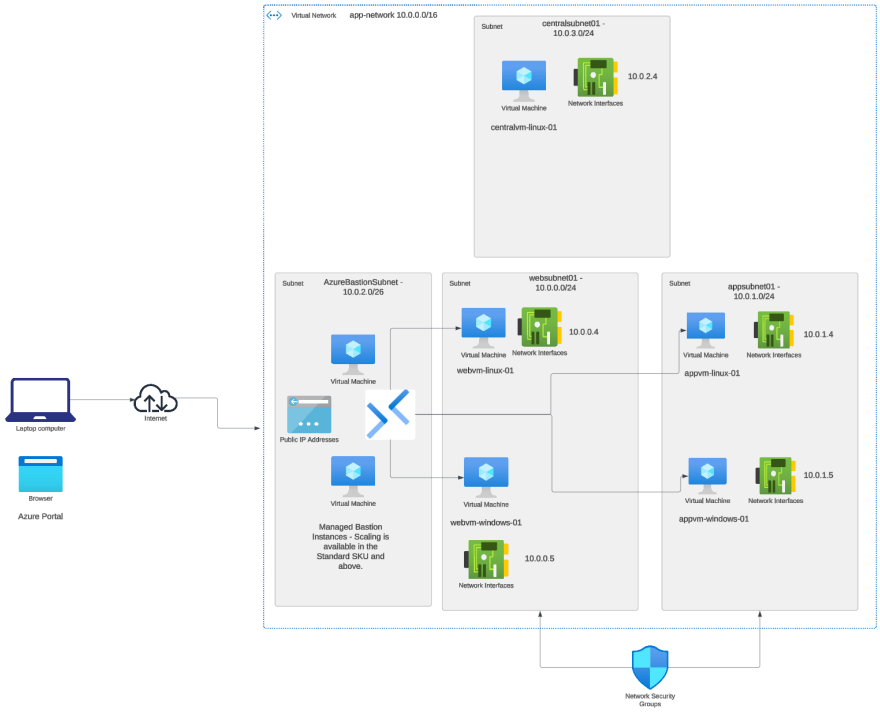
By default there are system routes in place which ensures the traffic is routed correctly across subnets in a virtual network.

But let's say that your company has a virtual machine that is hosting a virtual appliance - Firewall.

And all traffic in the virtual network needs to be routed through the virtual appliance.

We can define a user-defined route that makes sure all traffic is routed through the firewall appliance device.

Lab - User Defined Routes



Let's say that all traffic needs to be routed via a new virtual machine named centralvm-linux-01.

Let's create that new environment first.

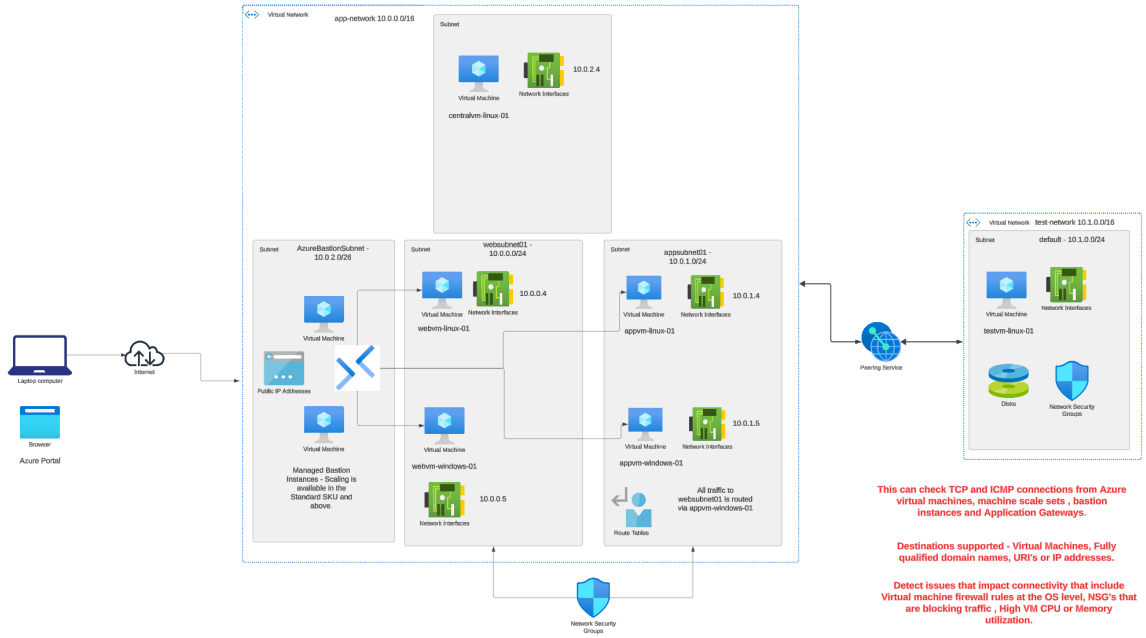
Then we will create a new route table.

Then create a route that routes all traffic for websubnet01 via centralvm-linux-01.

We then need to associate the route table with appsubnet01

In order to route requests we now need to implement 2 aspects
Enable IP forwarding on the network interface for centralvm-linux-01 and at the OS level.

Network Watcher - Connection Troubleshoot

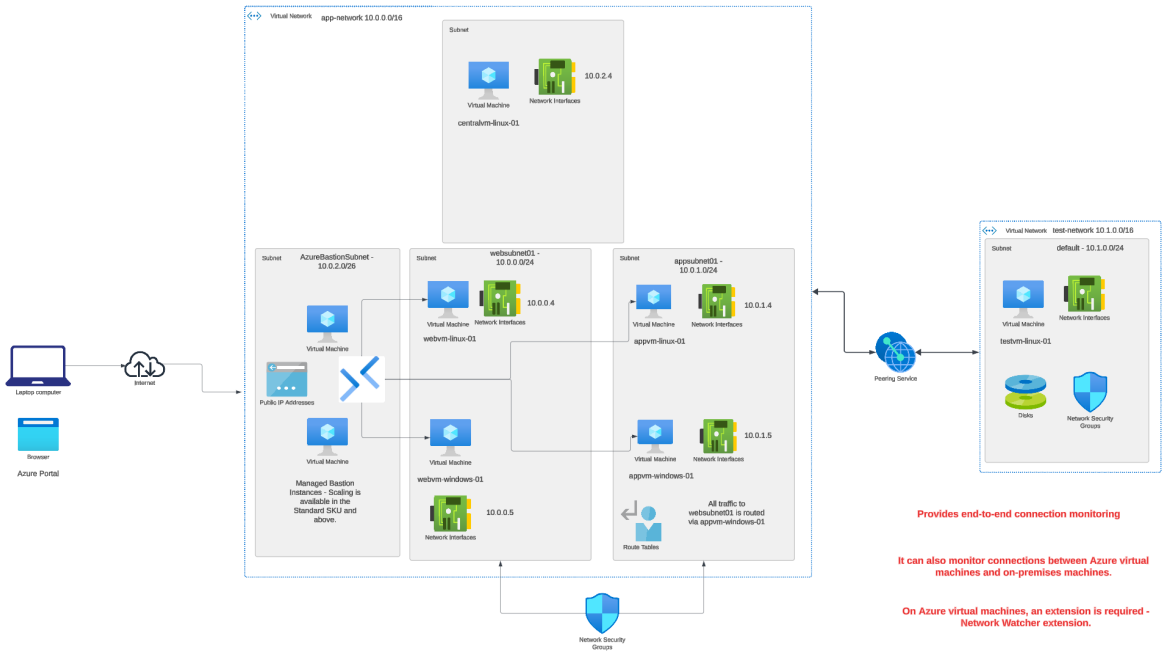


This can check TCP and ICMP connections from Azure virtual machines, machine scale sets , bastion instances and Application Gateways.

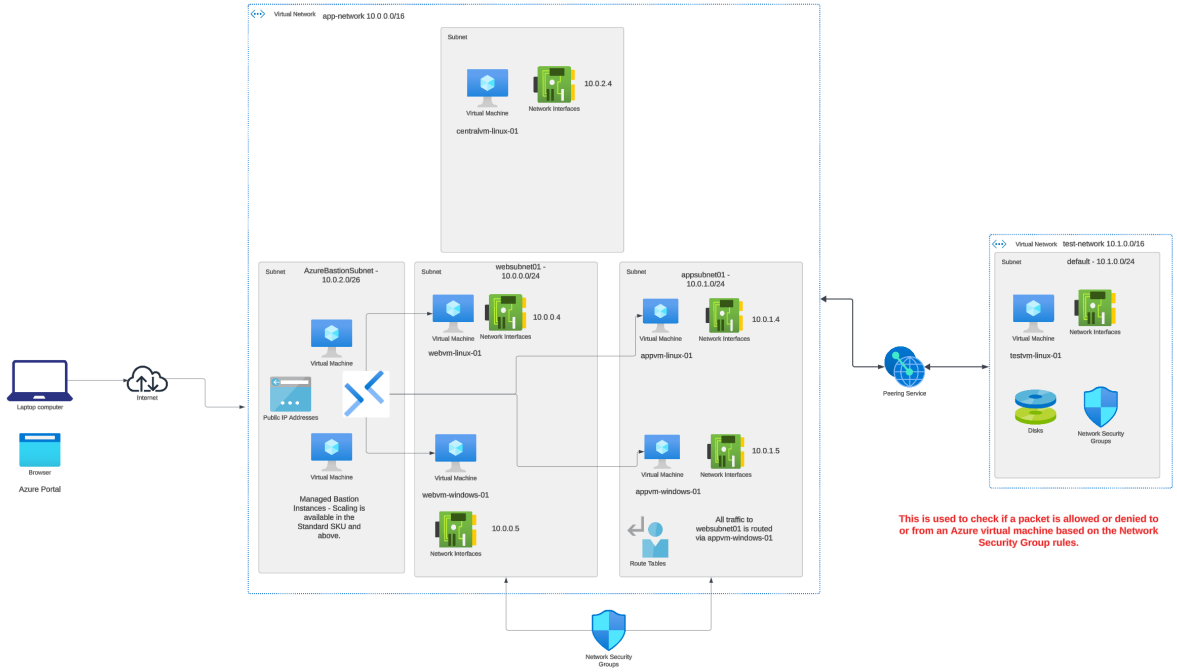
Destinations supported - Virtual Machines, Fully qualified domain names, URI's or IP addresses.

Detect issues that impact connectivity that include Virtual machine firewall rules at the OS level, NSG's that are blocking traffic , High VM CPU or Memory utilization.

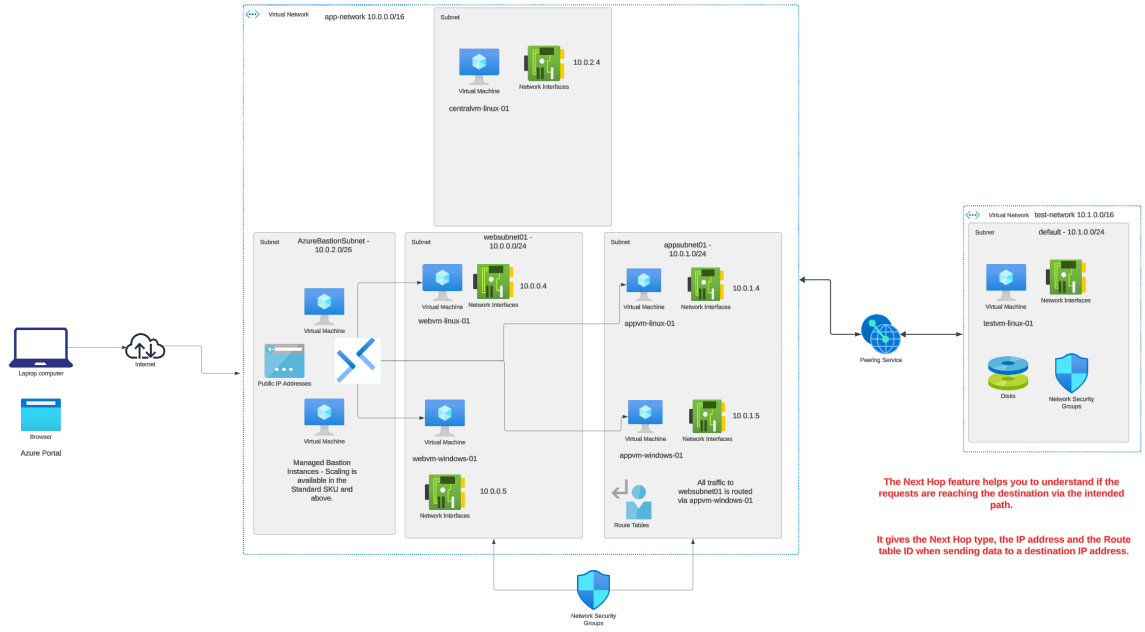
Network Watcher - Connection Monitor



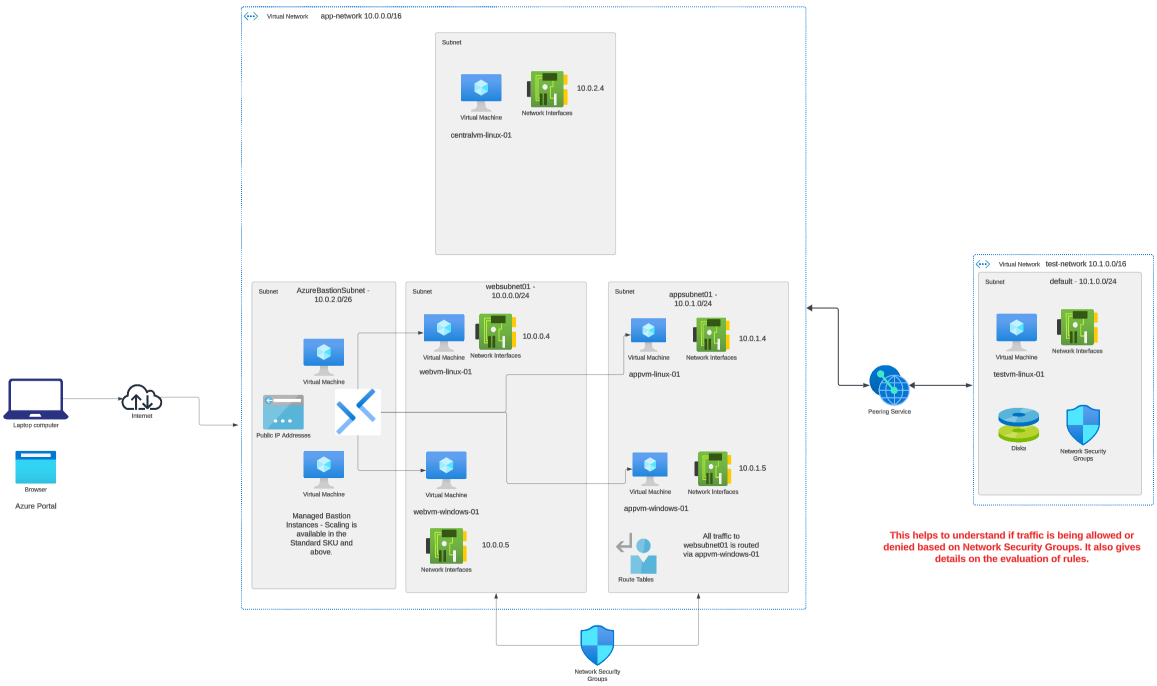
Network Watcher - IP Flow Verify



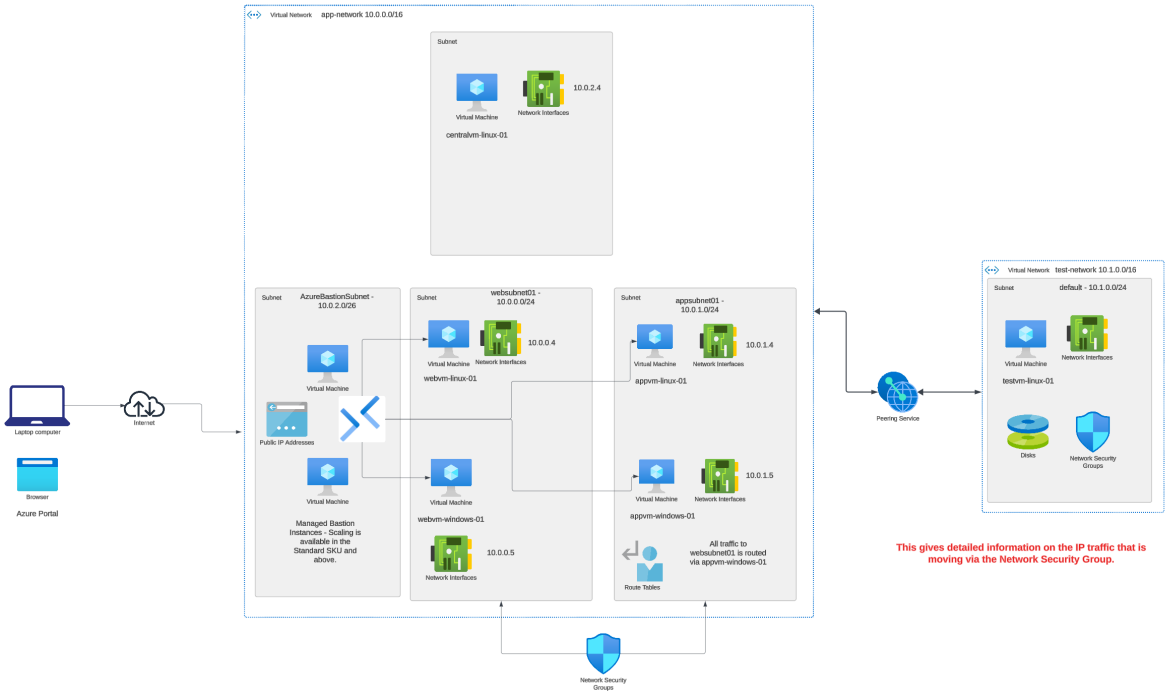
Network Watcher - Next hop



Network Watcher - NSG Diagnostic



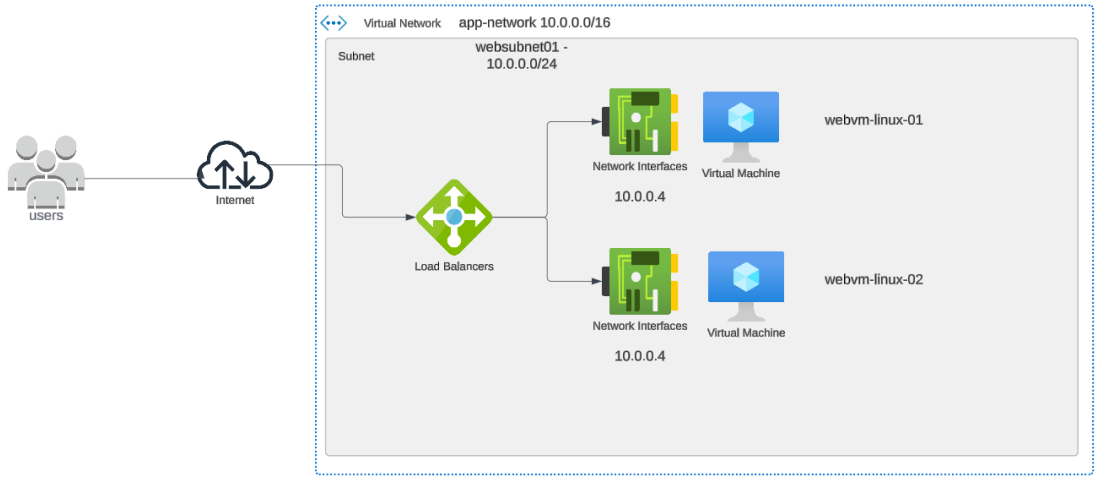
Lab - Network Watcher - NSG Flow logs



The Azure Load Balancer Service

Azure Load Balancer

A load balancer is used to distribute the incoming network traffic across a set of backend servers.



You can have an application hosted on a set of machines.

You want user traffic to be distributed equally across the machines.

For this we can make use of the Azure Load Balancer service.

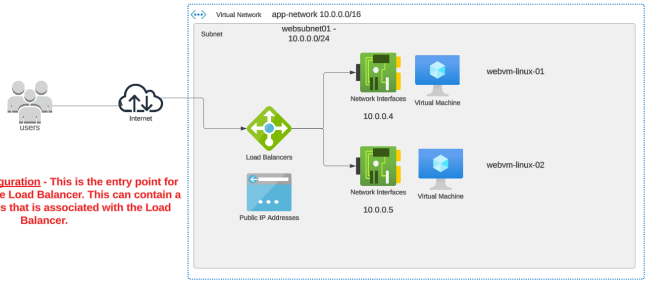
Here the Azure Load Balancer can distribute traffic across the private IP addresses of the backend machines.

Load Balancer SKU's - The Basic SKU is going to retire on September 30, 2025

	Standard Load Balancer	Basic Load Balancer
Scenario	Equipped for load-balancing network layer traffic when high performance and ultra-low latency is needed. Routes traffic within and across regions, and to availability zones for high resiliency.	Equipped for small-scale applications that don't need high availability or redundancy. Not compatible with availability zones.
Backend type	IP based, NIC based	NIC based
Protocol	TCP, UDP	TCP, UDP
Backend pool endpoints	Any virtual machines or virtual machine scale sets in a single virtual network	Virtual machines in a single availability set or virtual machine scale set
Health probes	TCP, HTTP, HTTPS	TCP, HTTP
Health probe down behavior	TCP connections stay alive on an instance probe down **and** on all probes down.	TCP connections stay alive on an instance probe down. All TCP connections end when all probes are down.
Availability Zones	Zone-redundant, zonal, or non-zonal frontend IP configurations can be used for inbound and outbound traffic	Not available
Type	Internal, Public	Internal, Public
Frontend IP configuration	When using a Public Standard Load Balancer, the SKU of the public IP must be Standard. Basic Public IPs are not supported on Standard LB	When using a Public Basic Load Balancer, the SKU of the public IP must be Basic. Standard Public IPs are not supported on Basic LB
Diagnostics	Azure Monitor multi-dimensional metrics	Not supported
HA Ports	Available for Internal Load Balancer	Not available
Secure by default	Closed to inbound flows unless allowed by a network security group. Internal traffic from the virtual network to the internal load balancer is allowed.	Open by default. Network security group optional.
Outbound Rules	Declarative outbound NAT configuration	Not available
TCP Reset on Idle	Available on any rule	Not available
Multiple front ends	Inbound and outbound	Inbound only
Management Operations	Most operations < 30 seconds	60-90+ seconds typical
SLA	99.99%	Not available
Global VNet Peering Support	Standard Internal Load Balancer is supported via Global VNet Peering	Not supported
NAT Gateway Support	Both Standard Internal Load Balancer and Standard Public Load Balancer are supported via Nat Gateway	Not supported

Reference - https://learn.microsoft.com/en-us/azure/load-balancer/skus

Components



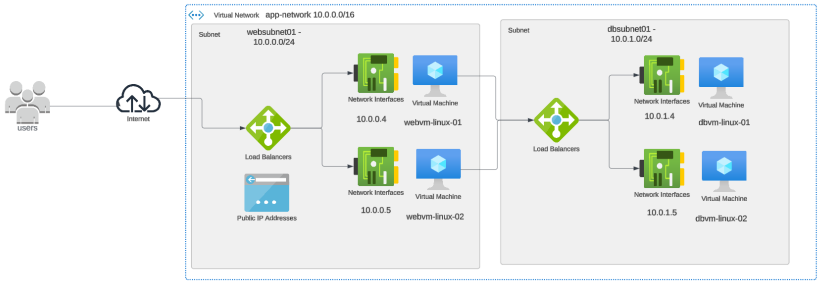
Frontend IP configuration - This is the entry point for the clients onto the Load Balancer. This can contain a Public IP address that is associated with the Load Balancer.

Backend Pool - These are the backend virtual machines that will be used to serve the client requsts.

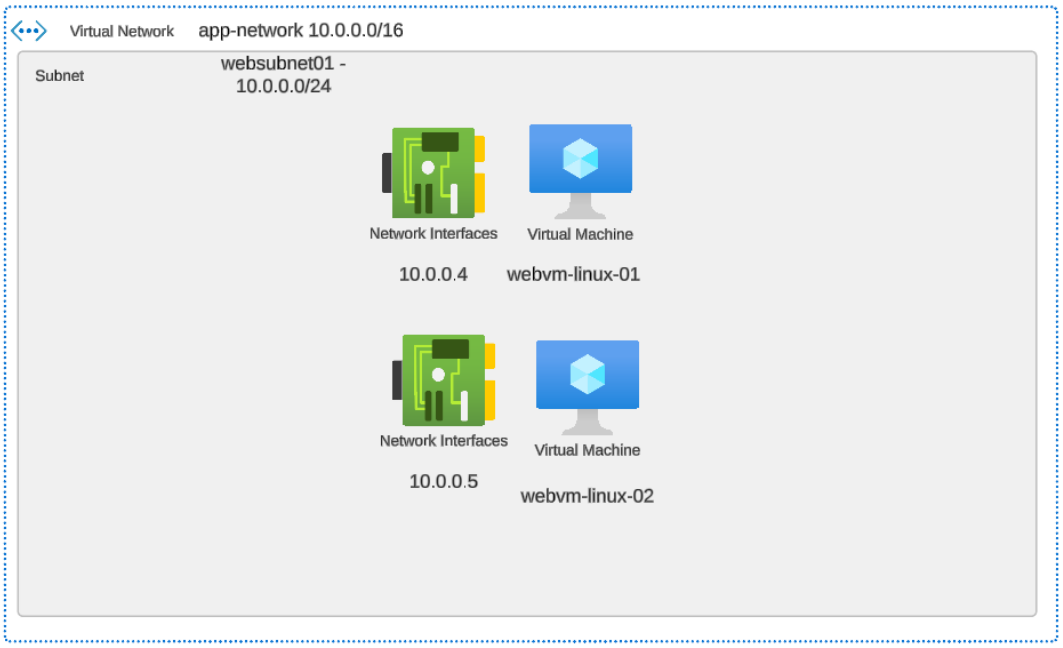
Health Probe - This is used to determine if the backend machines are healthy or not.

Load Balancer Rules - These are used to determine how the requests from the clients are routed to the backend instances.

We can also create a Public facing or a Private Load Balancer



Lab - Basic Load Balancer – Setup



Let's first create 2 virtual machines based on Ubuntu Linux.

Install the NGINX server on both machines.

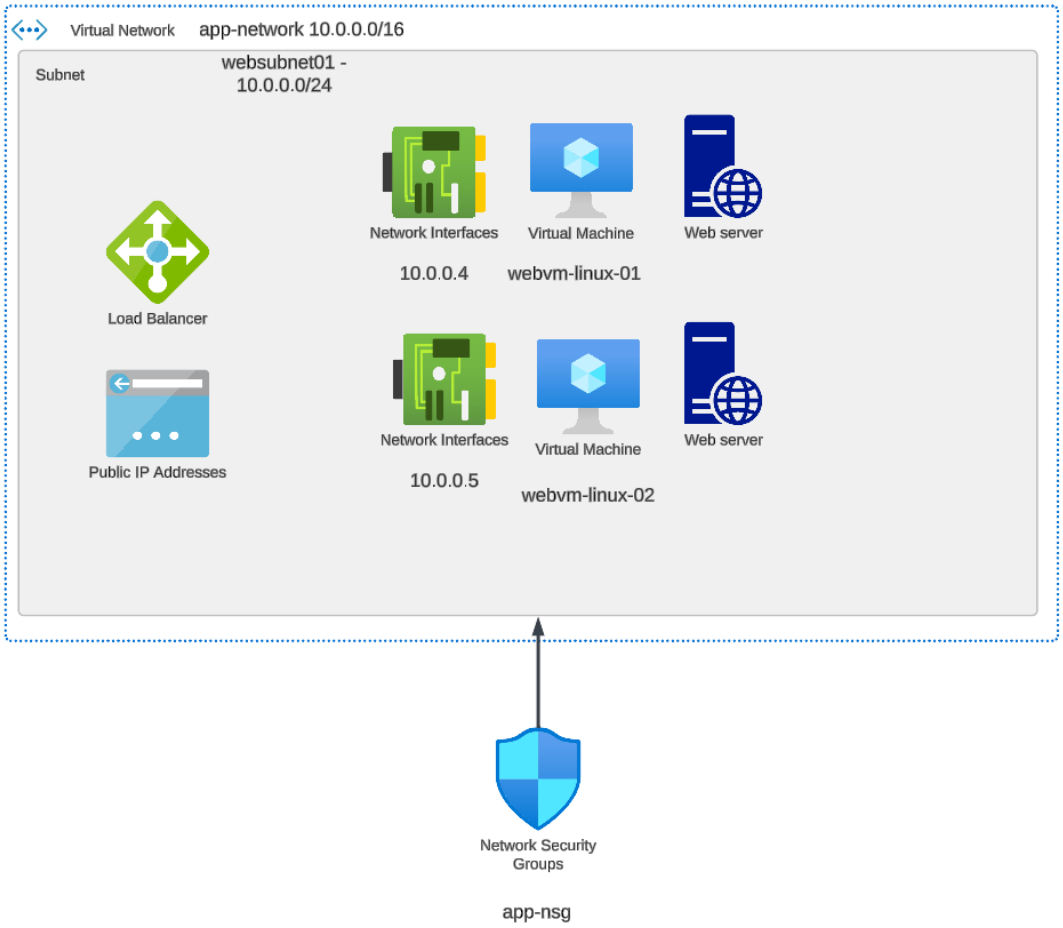
Initially let's have a Public IP address for both machines to perform the installation.

Later on we can disassociate the IP addresses and delete them.

We will also ensure that no NSG's are created for the virtual machines.

Let's create an NSG at the subnet layer.

Lab - Basic Load Balancer – Deployment

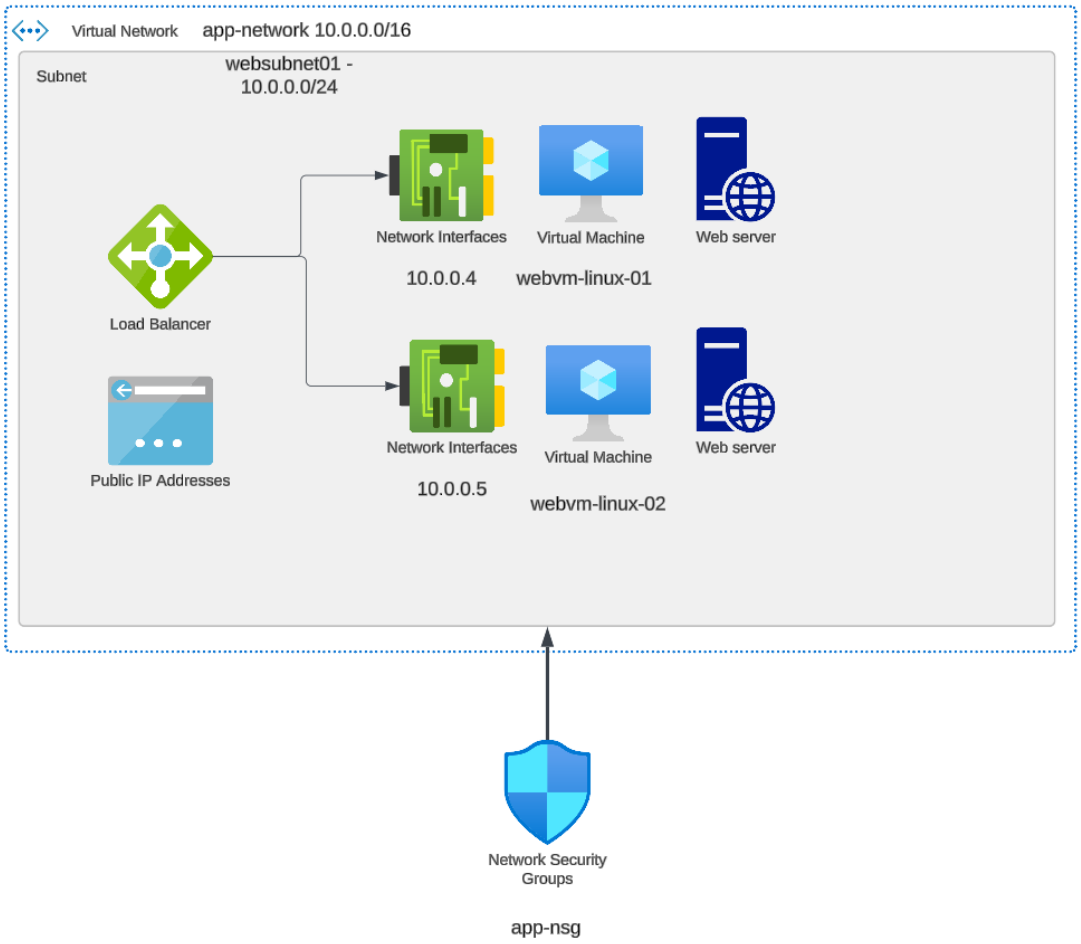


Let's deploy a Load Balancer - Public and off the Basic SKU.

While creating the load balancer, we will configure the backend pool with the virtual machines.

We will also configure a Frontend IP config which will have a Public IP address for the Load Balancer.

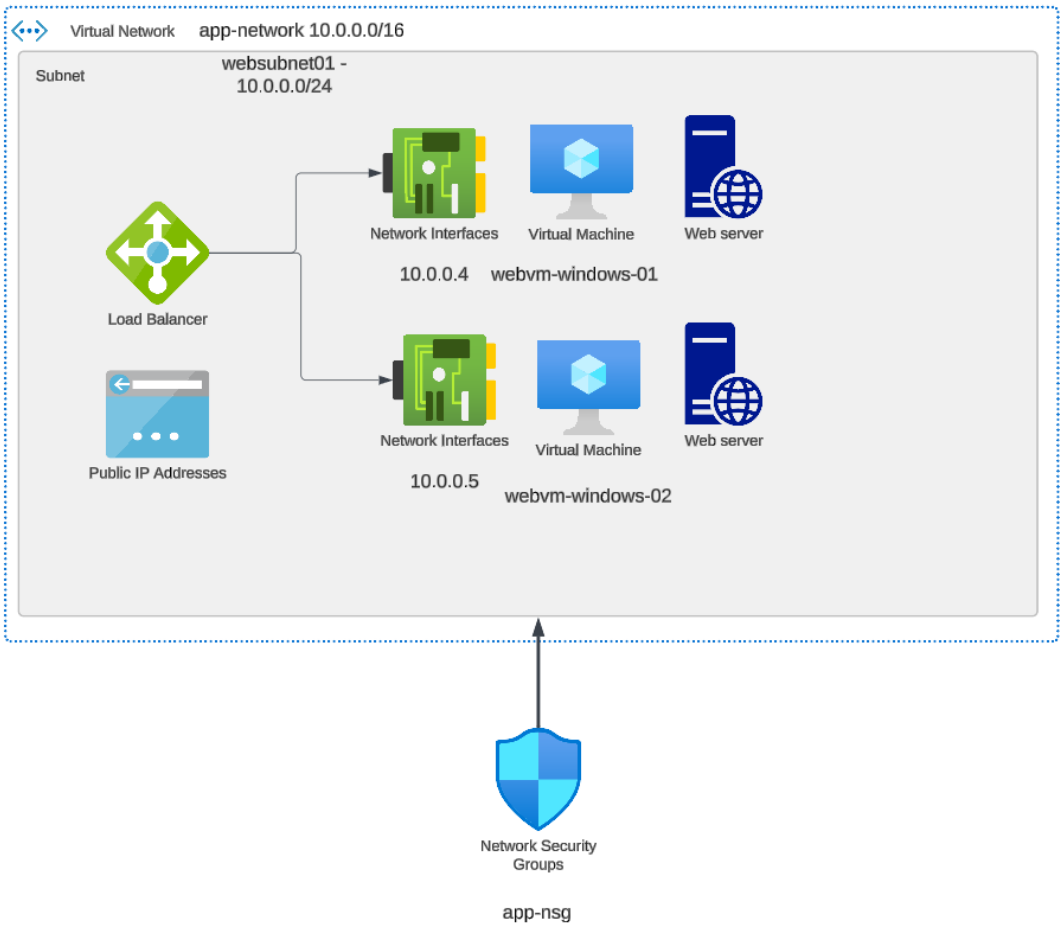
Lab - Basic Load Balancer – Configuration



Once we have the Load Balancer in place, lets first define a health probe.

And then define a Load Balacing Rule.

Lab - Azure Load Balancer - Standard SKU - Setup

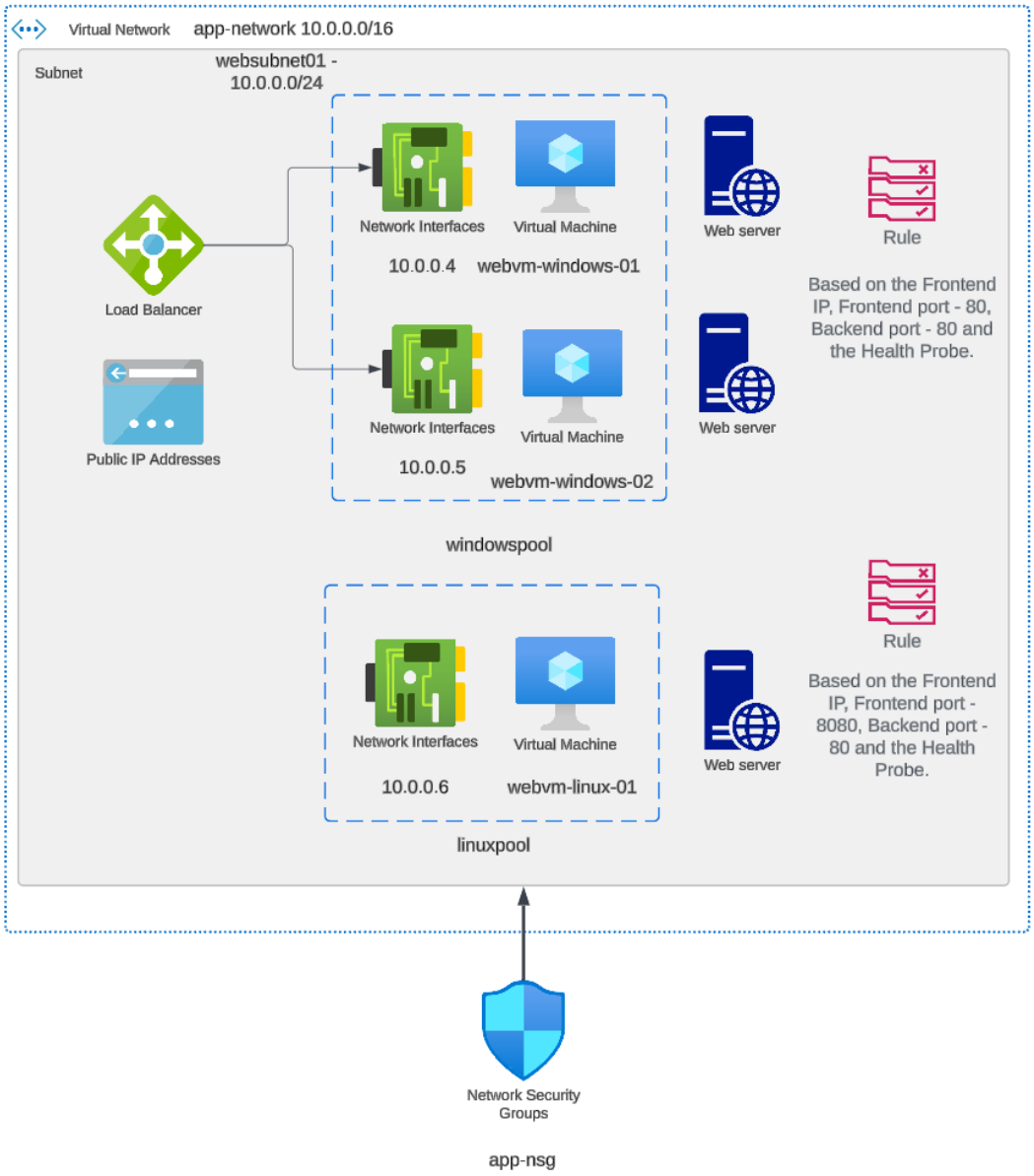


This time we will create machines that are not part of any Availability set.

These will be based on Windows and will have IIS in place.

And perform the same deployment of a Load Balancer, but this time it will be based on the Standard SKU.

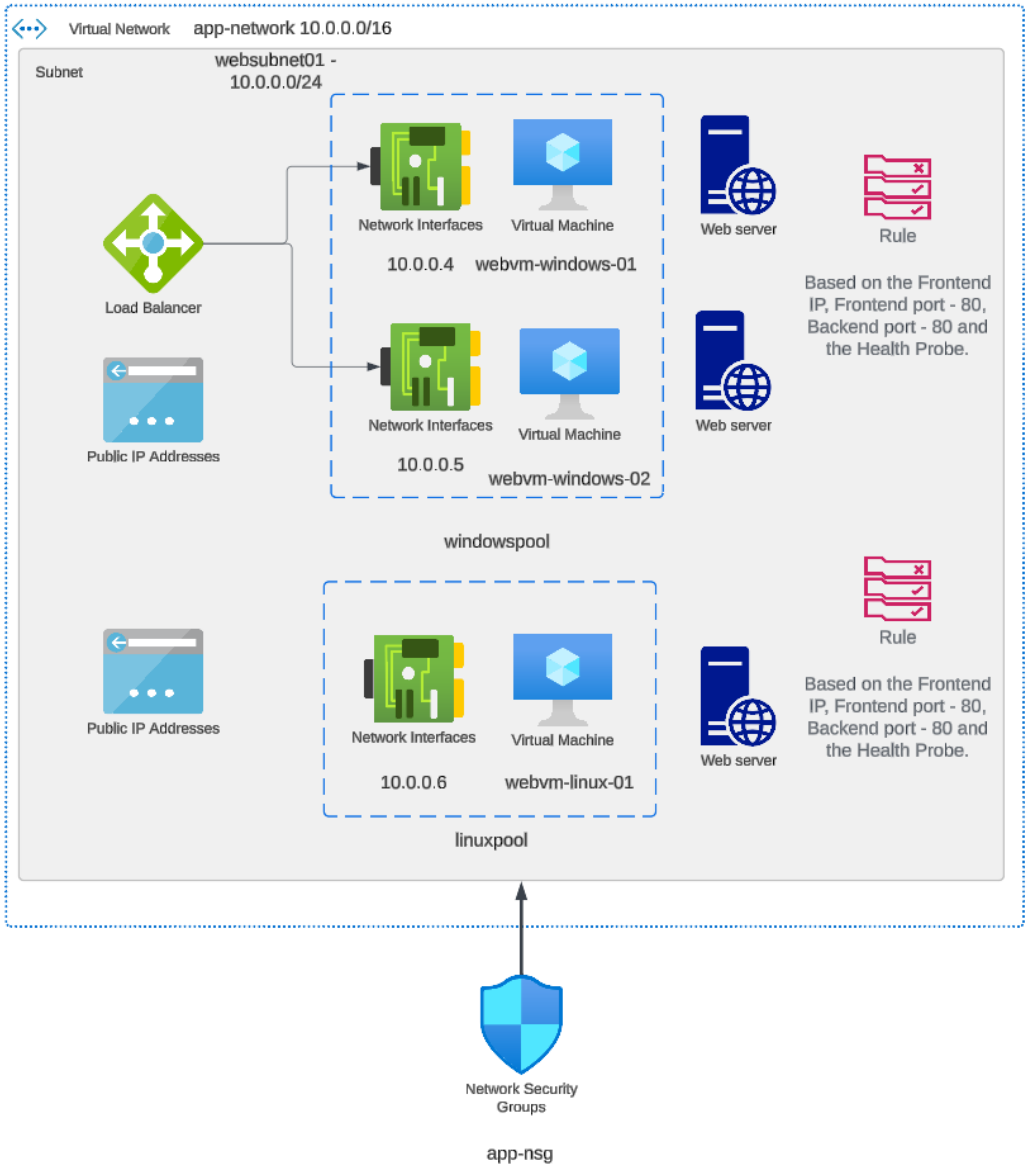
Lab - Standard Load Balancer - Multiple Backend Pools



Let's add another machine to the backend pool. This time lets deploy a Linux machine with NGINX installed.

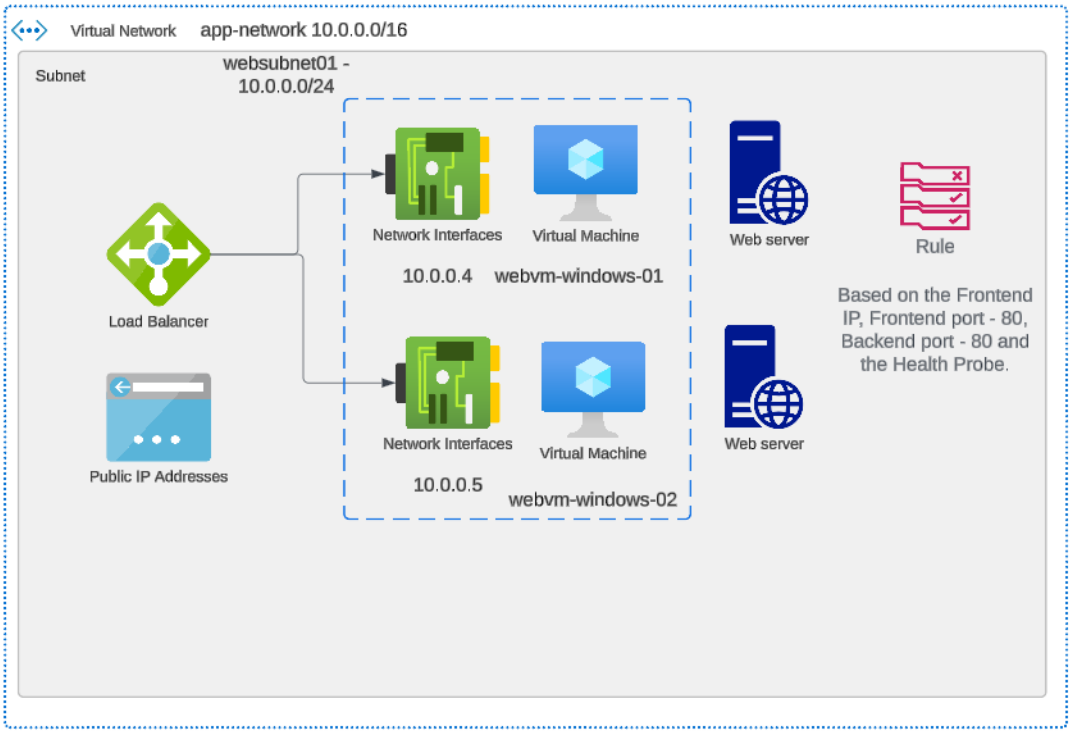
We will make this machine part of another backend pool.

Lab - Standard Load Balancer - Multiple FrontEnd IP address



Another way is to define another Public IP address along with another Frontend IP config and access the backend pool via the new Frontend IP config.

Azure Application Gateway



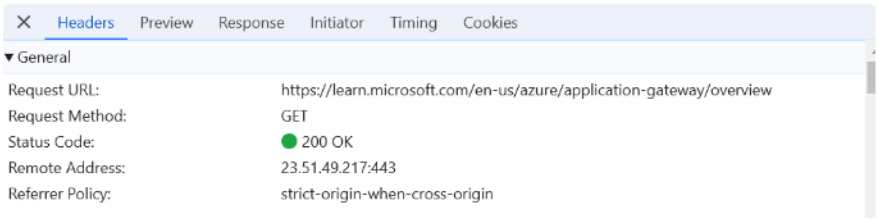
Here routing is carried out at the network level. The routing is faster because it just forwards the request to the desired backend pool.

The Azure Load Balancer will route the traffic based on the IP address and the port number.

Azure Application Gateway

The Azure Application Gateway is a Layer 7 load balancer. Here the routing decisions can also be made based on the details of the HTTP request.

When you make a request for a URL, there are a lot of attributes associated with the HTTP request.



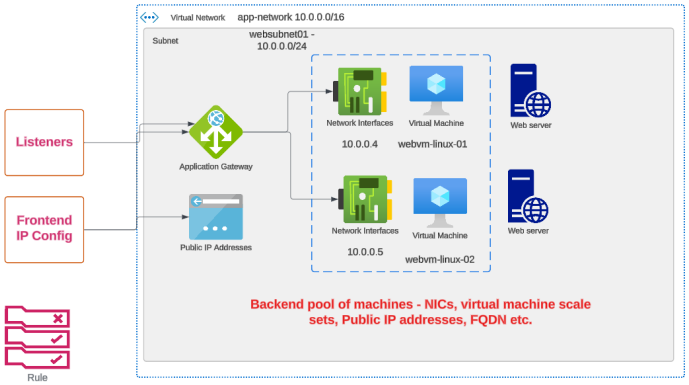
The Azure Application Gateway can parse the HTTP request and route the request accordingly.

The different components

The Listener listens for incoming client connections. Listeners are based on the protocol, port, hostname and IP address.

The Application Gateway has a Frontend IP address. All client requests are routed to the frontend ip configuration.

You can have a Public or Private IP address attached to the Front End IP configuration.



The rules are used to route requests to the backend targets. This is based on the listener, the backend server pool and the HTTP settings.

The Health Probe can be used to monitor the health of the backend resources.

Here you have settings such as the port number, protocol and encryption.

Lab - Azure Application Gateway - URL Routing – Setup

First let's define machines based on Ubuntu Linux that will become target resources in the backend pool for the Azure Application Gateway.

The machines will initially have a public IP address to install the web server. Later on we can disassociate the Public IP addresses.

The machines will have NGINX and html pages in place.

We will have a Network Security Group attached to the subnet.

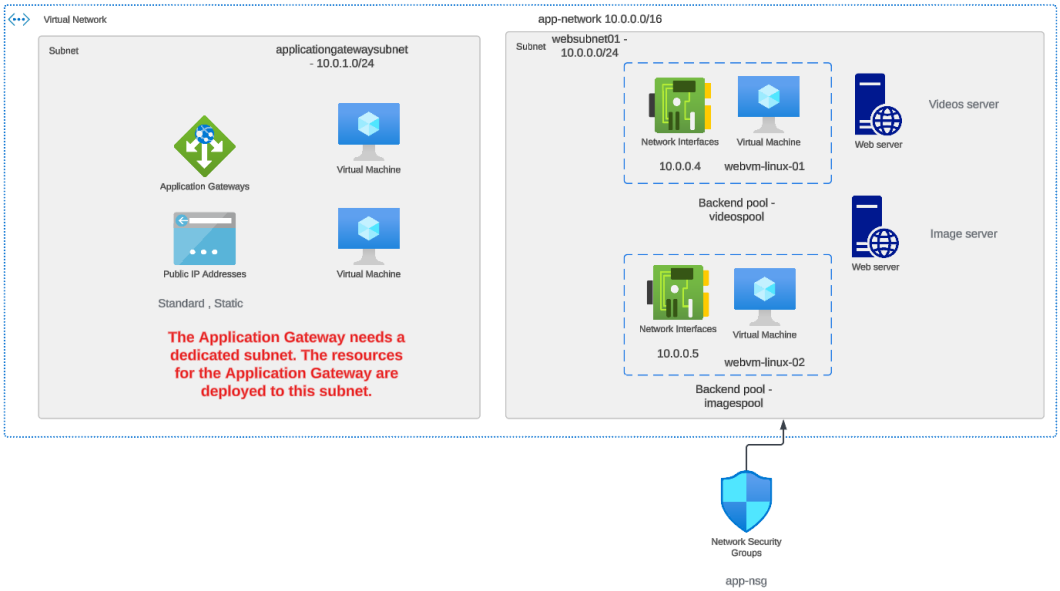
Priority	Name	Port	Protocol	Source	Destination	Action
300	AllowMyIpAddressSS···	22	TCP	94.204.16.49	10.0.0.4,10.0.0.5	Allow
310	AllowTagHTTPInbound	80	TCP	Internet	10.0.0.4,10.0.0.5	Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalan···	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInBound	Any	Any	Any	Any	Deny

Lab - Azure Application Gateway - URL Routing – Implementation

We want to base the routing of requests based on the URL.

If the URL contains /videos then the request needs to be directed to the backend pool that contains the videos server.

If the URL contains /images then the request needs to be directed to the backend pool that contains the images server.



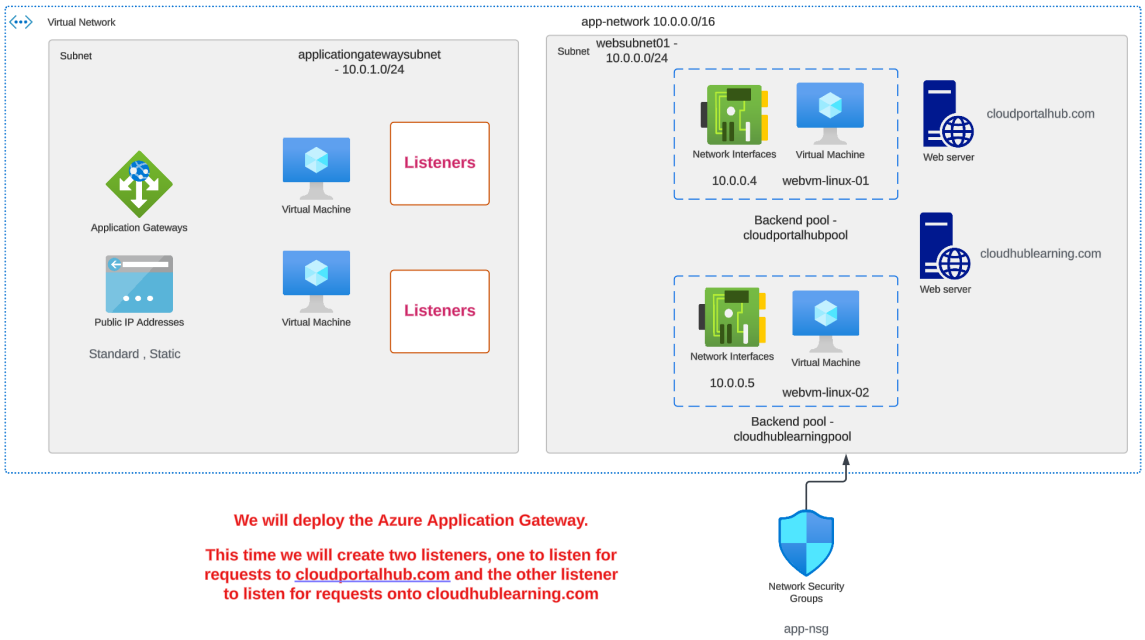
Lab - Azure Application Gateway - Multiple Sites - Gateway setup

We now want to use the Application Gateway to route requests based on different sites.

If a request is for www.cloudportalhub.com, they are directed to webvm-linux-01. And if the request is for www.cloudhublearning.com , then the request is directed to webvm-linux-02.

We will just create simple Default.html pages in the default /var/www/html folder for each server.

Lab - Azure Application Gateway - Multiple Sites – Implementation



We will deploy the Azure Application Gateway.

This time we will create two listeners, one to listen for requests to cloudportalhub.com and the other listener to listen for requests onto cloudhublearning.com

Understanding the domain name system

50.47.100.20

You have a web application located on a machine.

In order to send a request to the machine hosting the application, you need to contact the machine via its IP address.

In the browser , https://50.47.100.20

Users cannot easily remember IP addresses. Hence we have domain names which are user friendly to remember. They can be linked to IP addresses.

We can map a domain of cloudportalhub.com to 50.47.100.20 so users can type https://cloudportalhub.com in their browser.

There are many DNS servers on the Internet.

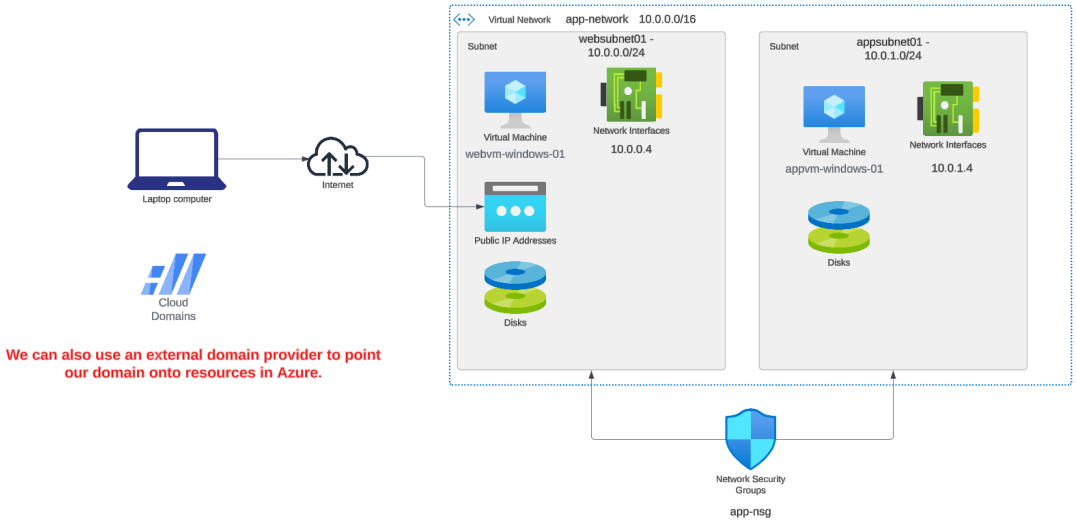
Your request for cloudportalhub.com first needs to be resolved to the IP address of the machine

A request is made from your machine onto the Internet via the various DNS servers on the Internet to fist find out the IP address mapped to cloudportalhub.com.

Once a response comes back , then the laptop will make a connection via the Internet onto the machine hosting the web application.

50.47.100.20

Using DNS for Azure virtual machines



We can also use an external domain provider to point our domain onto resources in Azure.

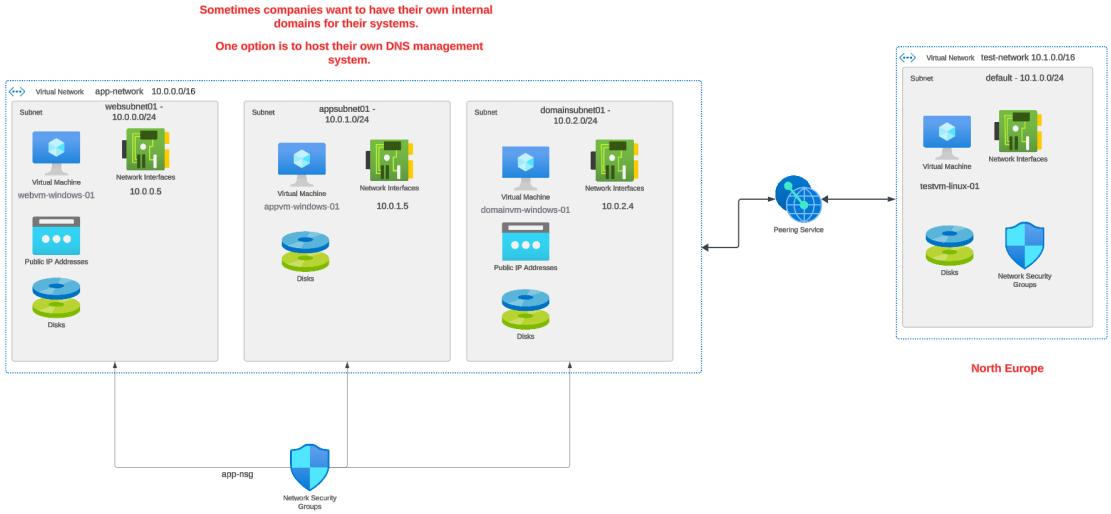
Azure provides their own in-built DNS that manages the DNS zones and records.

Azure also provides internal name resolution for virtual machines.

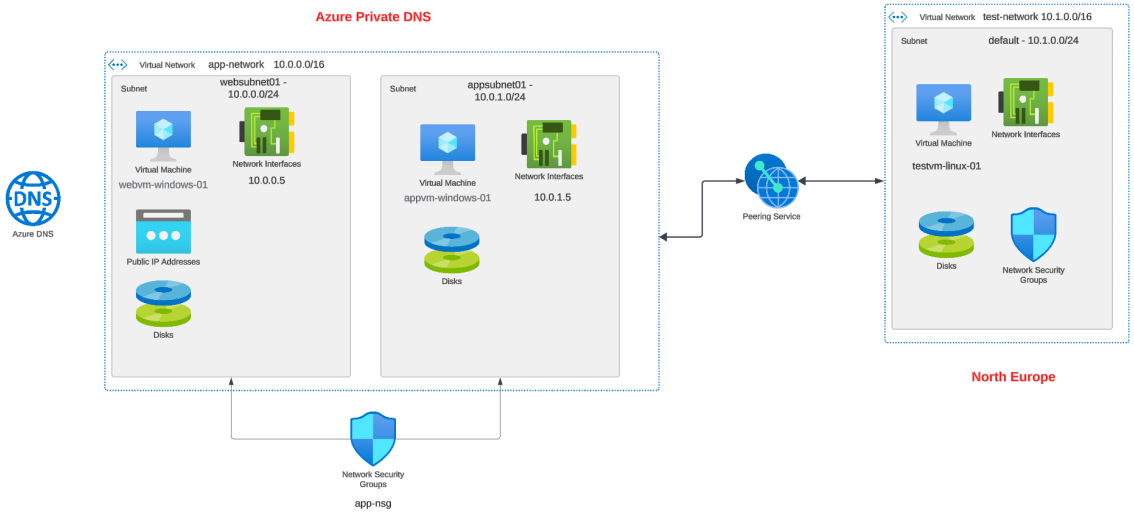
We can assign a DNS name for the public IP address and access the web server via the public-based DNS name.

Each virtual machine also gets an internal DNS name. Internally we can access the machines via the internal DNS name.

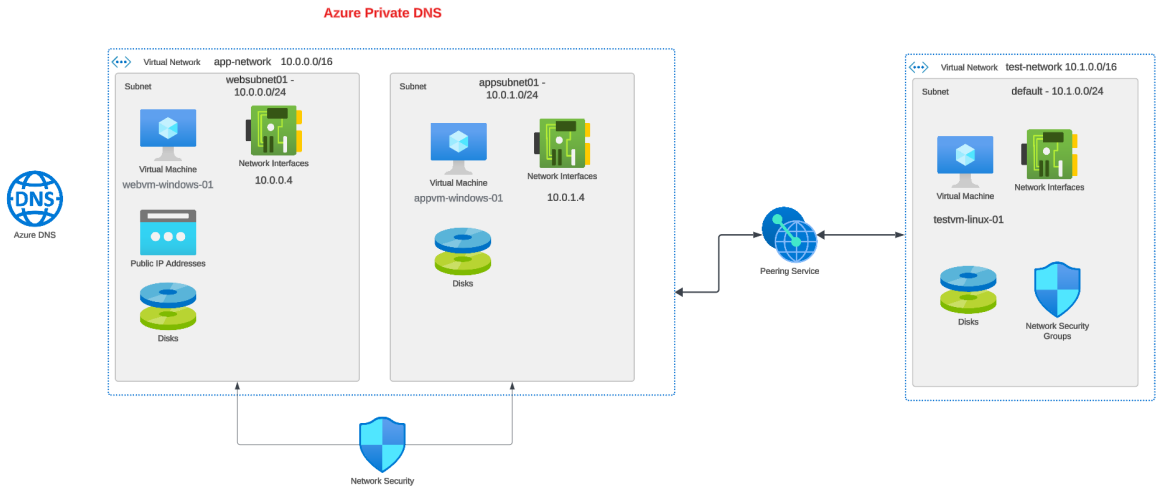
Overview of setting up a Local DNS



Lab - Azure Private DNS



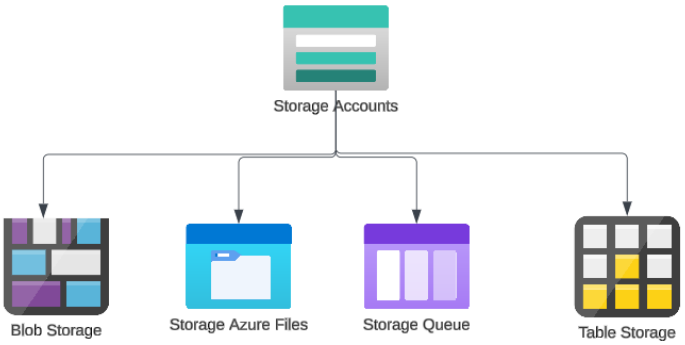
Lab - Azure DNS - Peered network



Implement and manage storage

What are storage accounts

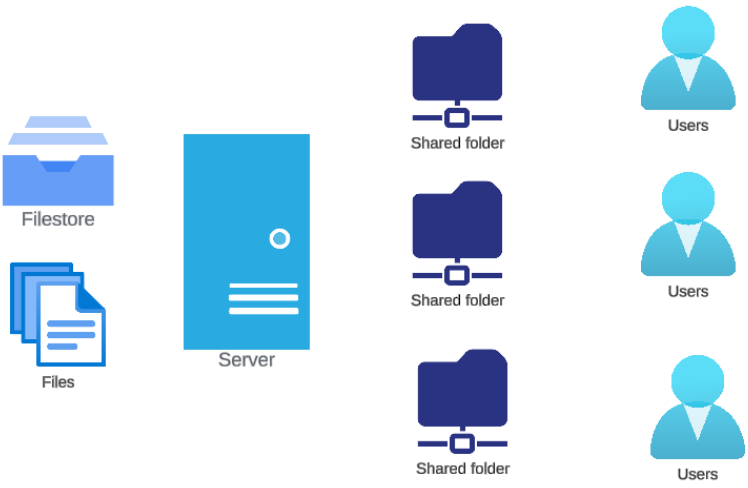
Azure Storage Accounts - This is storage on the Azure cloud for your blob objects, files, queues and tables.



Azure Storage Accounts provides 4 services.

This is used for storing a large amount of unstructured data. Suitable for storing images, documents, video and audio files.

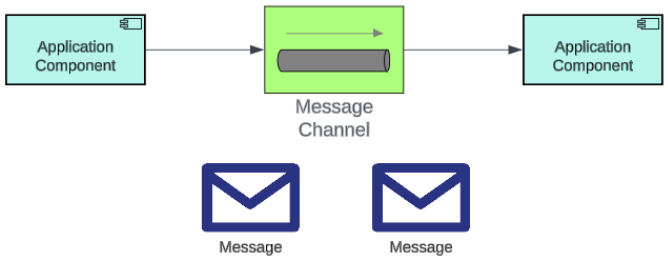
The video and audio files could be stored in an Azure storage account.



Here you need to maintain the file server and ensure enough storage is in place.

Instead you can create file shares using the Azure File share service. Here the storage is managed for you.

If messages need to be shared across multiple application components. Here you need to have the message software and maintain it.



Instead we can make use of the Queue service which provides the basic messaging service.

If an application needs to store data (non-relational structured data), like let's say data about users.

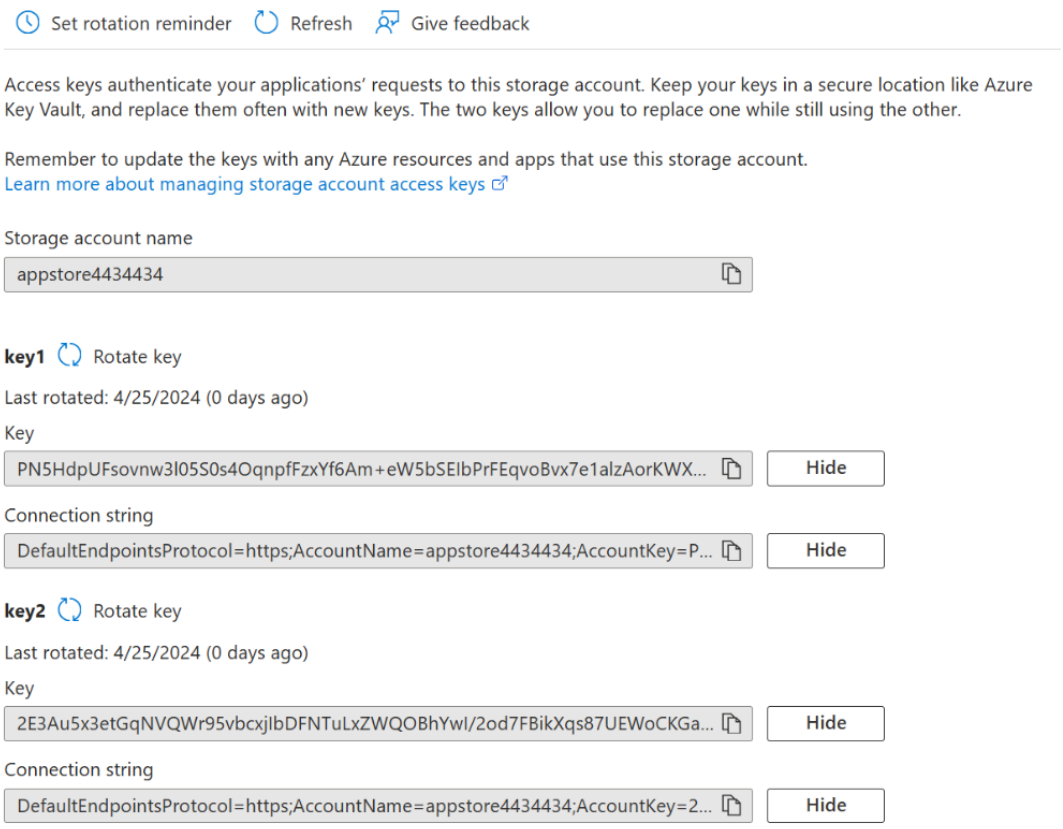
Azure Storage Accounts - Different authorization techniques

Let's say you are using an Azure Storage account to store images via the use of the Blob service.

One way to give access is to enable anonymous access. But this gives access to the Blobs at the container level.

Another broader way of giving access is via the use of Access Keys.

This gives access to all services in the storage account.



Another way of granting access is via the use of Shared Access Signatures.

Here you can put more restrictions on the access - You can also grant time limited access.

Azure Storage Accounts - Data Redundancy

How does Azure maintain high availability of your data stored in Azure Storage Accounts.

Service Credit – hot blobs in LRS, ZRS, GRS and RA-GRS (write requests) Accounts and blobs in LRS Block Blob Storage Accounts:

Uptime Percentage	Service Credit
< 99.9%	10%
< 99%	25%

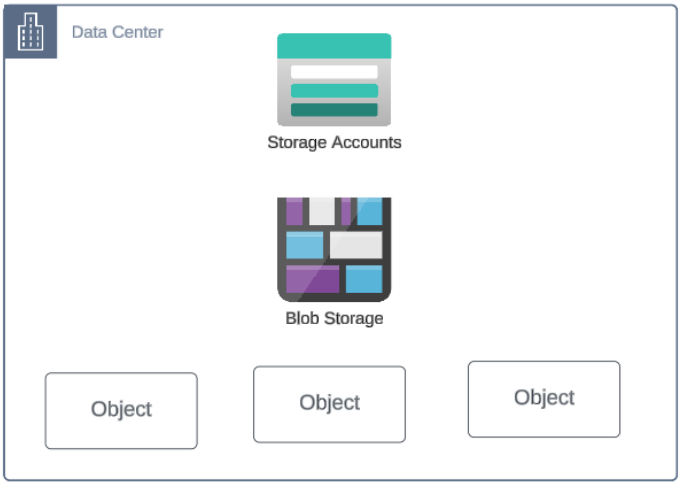
Service Credit – hot blobs in RA-GRS (read requests) Accounts:

Uptime Percentage	Service Credit
< 99.99%	10%
< 99%	25%

There are different data redundancy options in place.

Locally redundant storage

Here three copies of your data are made within a single data center.

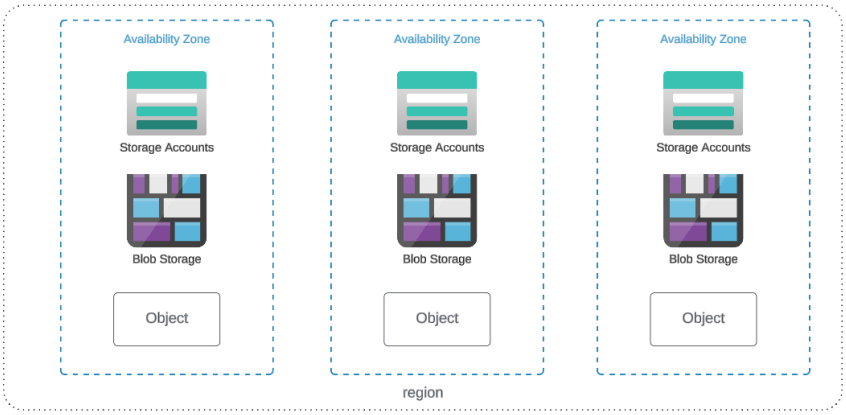


East US

Zone redundant storage

What happens if the data center goes down. Then you don't have access to your objects.

Here the data is replicated synchronously across three Azure Availability zones in the primary region.

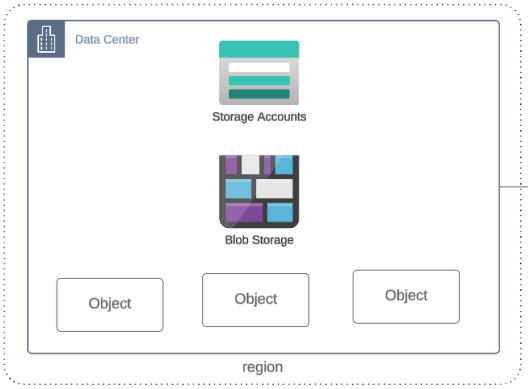


East US

But what happens if the entire region goes down. All of the Availability zones are not available.

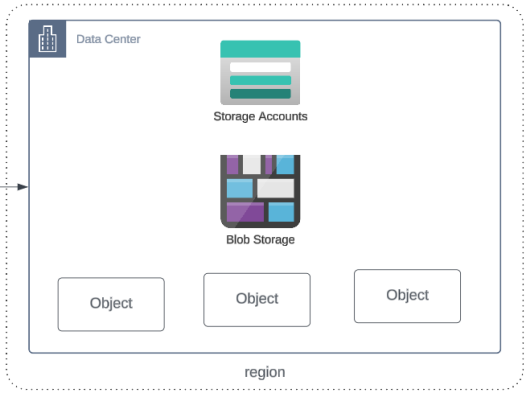
Geo-redudant storage

Three copies of your data are made to a single physical location in the primary region using LRS



East US

Three copies of your data are made to a single physical location in the secondary region using LRS

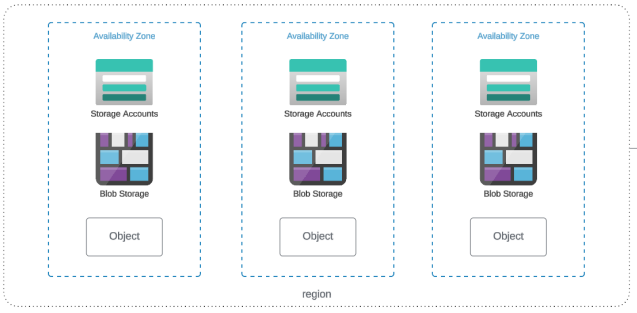


West US

Your data is replicated to a secondary region.

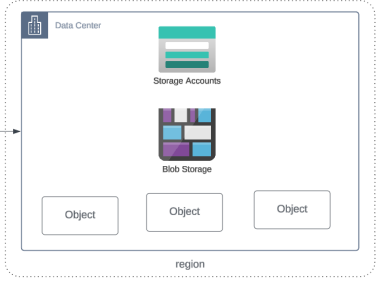
Geo-zone-redudant storage

Here the data is replicated synchronously across three Azure Availability zones in the primary region.



East US

Three copies of your data are made to a single physical location in the secondary region using LRS



West US

Storage Accounts - Access Tiers

A company can look towards millions of objects in an Azure Storage Account.

Data storage prices pay-as-you-go	Premium	Hot	Cool	Archive
First 50 terabyte (TB) / month	$0.15 per GB	$0.018 per GB	$0.01 per GB	$0.00099 per GB
Next 450 TB / month	$0.15 per GB	$0.0173 per GB	$0.01 per GB	$0.00099 per GB
Over 500 TB / month	$0.15 per GB	$0.0166 per GB	$0.01 per GB	$0.00099 per GB

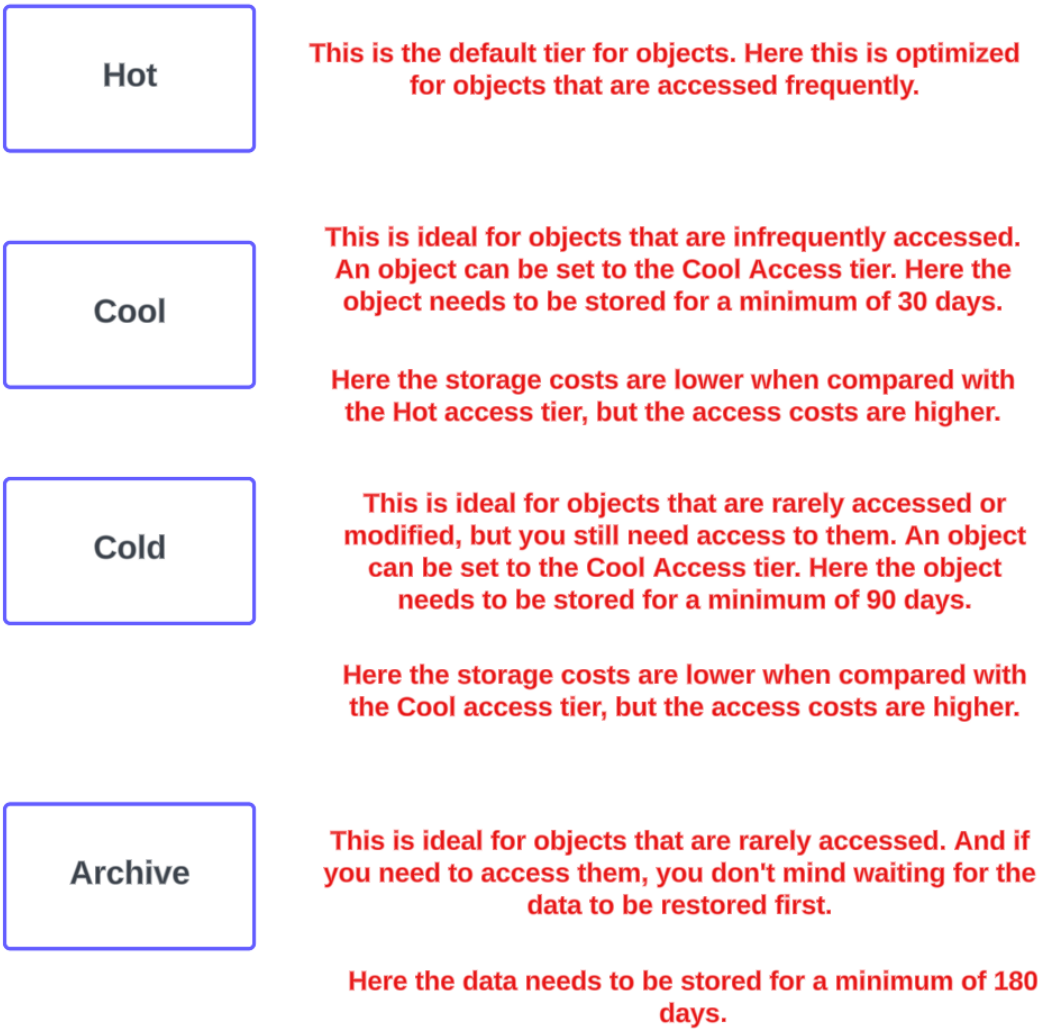
A company would want to monitor their storage costs.

An this can especially be the case if objects are not being used.

A thousand images have been uploaded on a particular day. During the first week the images are being used regularly.

But after a week the images are not being accessed. Should be still pay the same when it comes to storage costs.

We can use Access tiers to help in this regard.



Lab - Azure Storage Accounts - Object Replication

Object replication - Block Blobs

Here objects can be replicated asynchronously between a source and destination storage account.

You create a replication policy to replicate the objects.

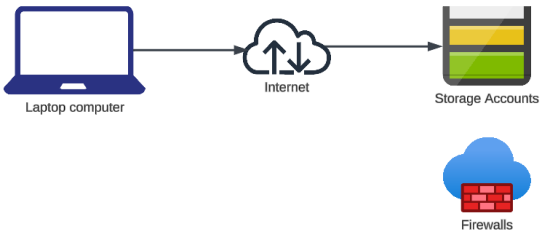
Source and destination storage accounts - General Purpose V2 or Premium block blob accounts.

Source and destination storage accounts - Blob versioning needs to enabled.

Source storage accounts - Change feed is enabled.

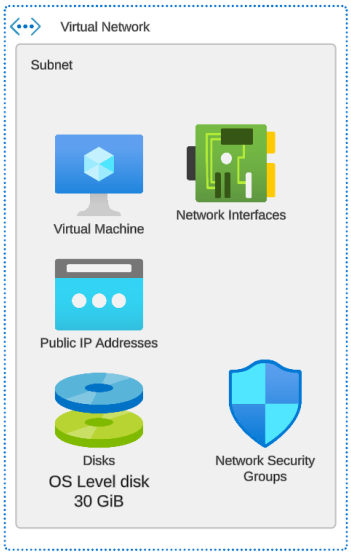
Lab - Firewall and Network settings – Setup

The Storage account service is a public service.



We can also restrict the storage account service to only be accessible from within the Virtual Network only.

This is done via the use of Virtual Network Service Endpoints.



Note on Premium storage accounts

Azure Premium Storage Account

Storage Accounts

Here your data is stored on high performance hardware via the use of solid-state drives. These are optimized for low latency.

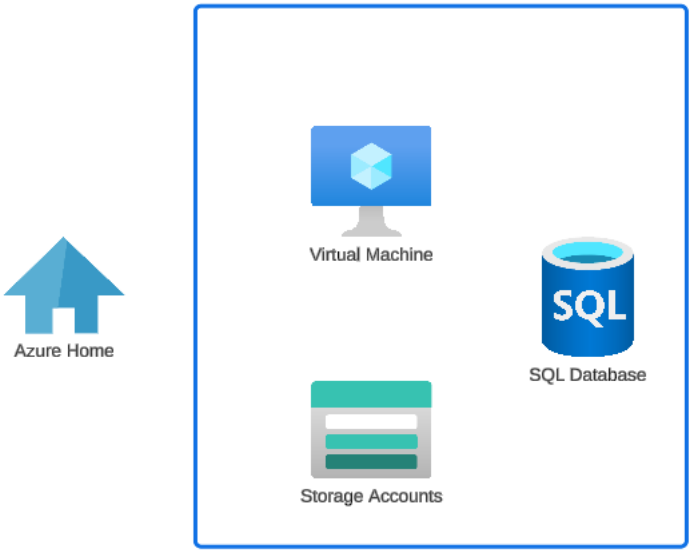
If your applications need fast access to data.

Here you have higher storage costs and lower transaction costs when compared with normal storage accounts.

These storage accounts are available for Block blobs, Page blobs and File shares.

Manage Azure identities and governance

What is Microsoft Entra ID



So far we have been working with Azure resources with our Azure Admin Account.

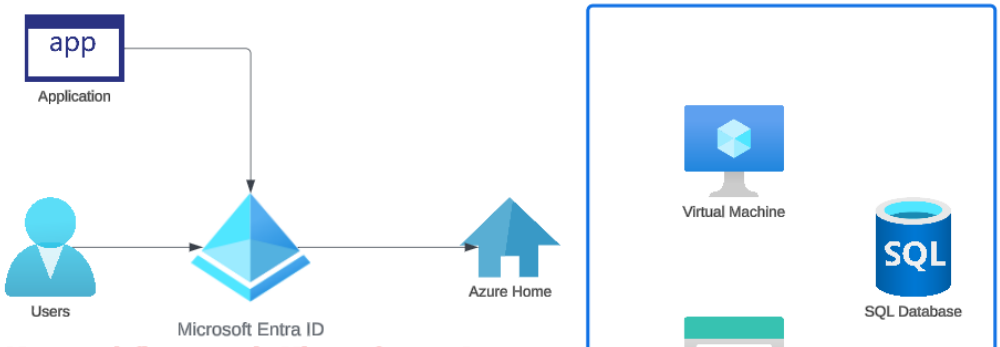
But in an organization, you want to have users who can access and manage resources.

Who has permission to create resources. Who has permission to access resources.

We need to create users and be able to assign permissions.

Microsoft Entra ID - This is a cloud-based identity and access management service. This identity service can be used for Azure, Microsoft 365 and even other Software-as-a-service applications.

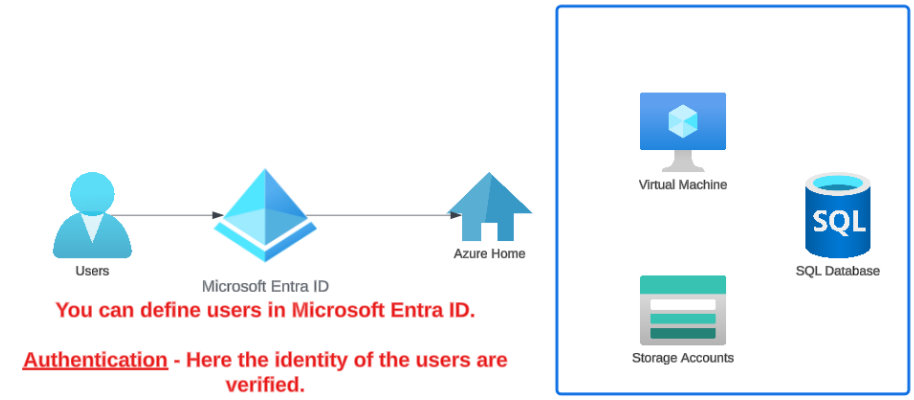
Even Applications can be linked to identities and be given access accordingly.



You can define users in Microsoft Entra ID.

Authentication - Here the identity of the users are verified.
Authorization - Here the permissions are checked for the users.

Introduction to Role Based Access Control



You can define users in Microsoft Entra ID.

Authentication - Here the identity of the users are verified.
Authorization - Here the permissions are checked for the users.

Role-based access control

We can assign different roles to a user.

There are many in-built roles.

You can also define your own custom roles.

Role-based access control

We can assign different roles to a user.

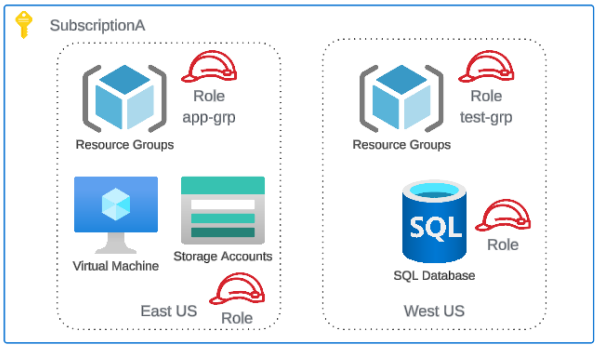
There are many in-built roles.

You can also define your own custom roles.

You can assign a role at the subscription level.

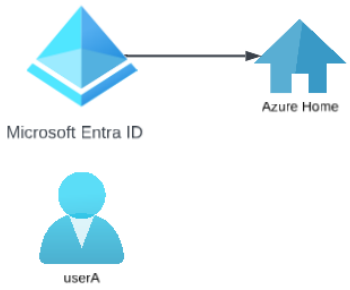
You can assign a role at the resource group level.

You can assign a role at the resource level.

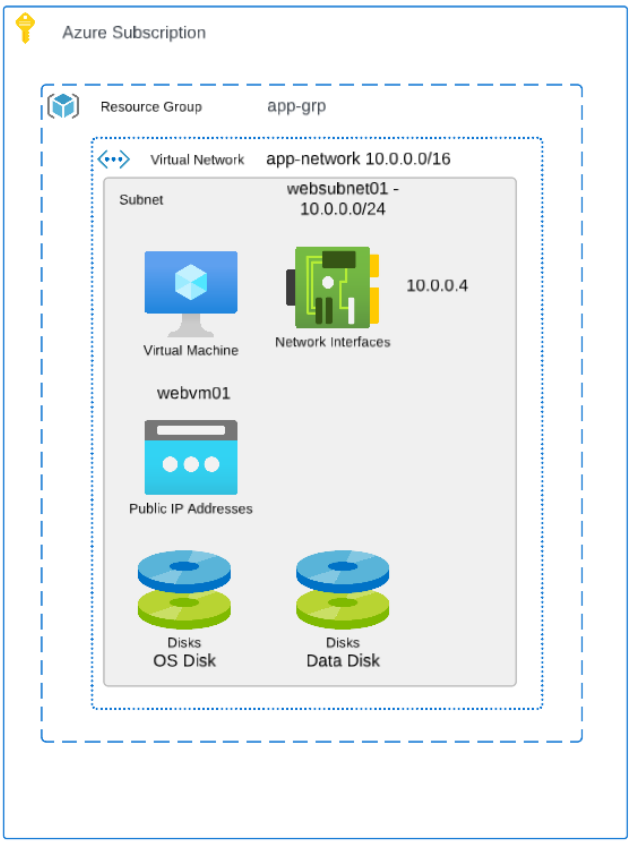


Owner Role	Contributor Role	User Access Administrator Role	Reader Role
Here the user would have complete access and be able to manage the resources. The user can also delegate access to other users.	Here the user would have complete access and be able to manage the resources.	Here the user would be able to delegate access to other users.	Here the user would be just be able to read the properties for the resources.

Lab - Role-based assignments - Resource level

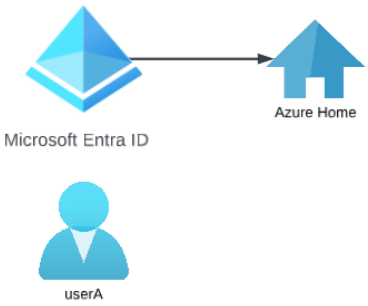


Let's give userA the reader role to the Azure virtual machine.



We will notice that we cannot see the other aspects of the virtual machine such as the virtual network etc.

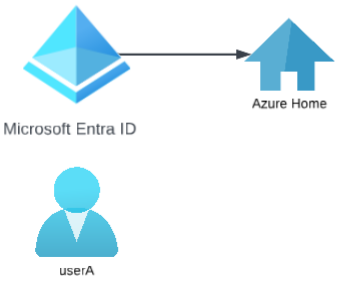
Lab - Role-based assignments - Resource group level



Now let's give UserA the Reader role at the resource group level.

Well now we can view the other resources but can be stop the virtual machine?

Lab - Role-based assignments - Contributor Role

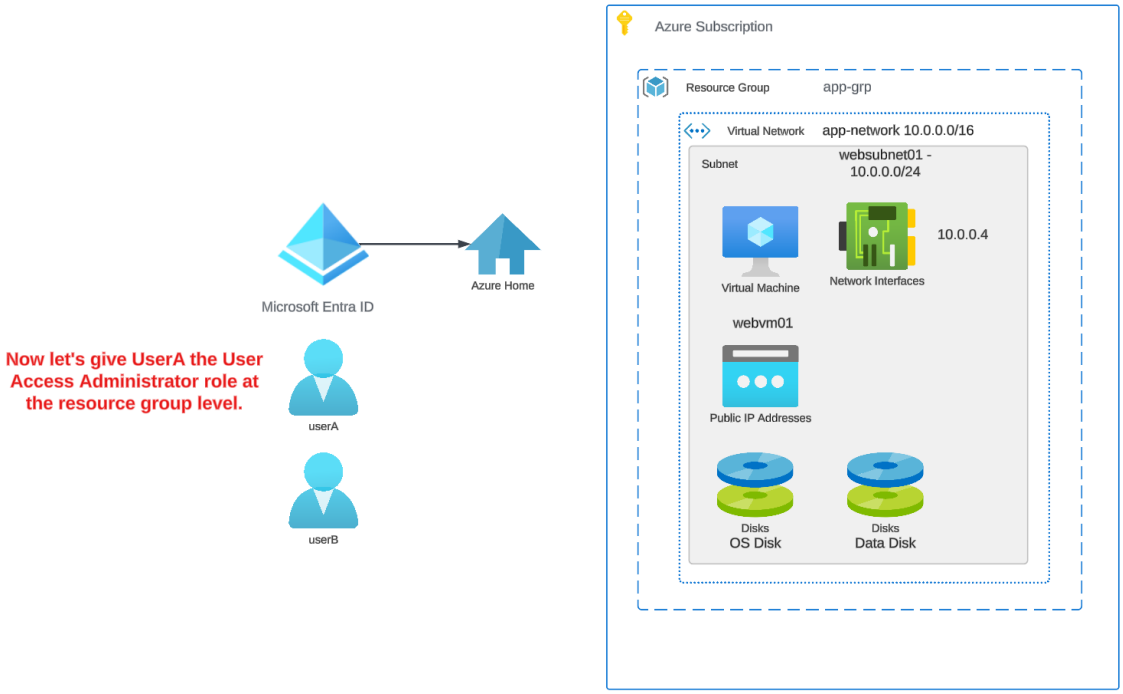


Now let's give UserA the Contributor role at the resource group level.

So now we can stop the virtual machine.

Can we create a new resource in the resource group such as an Azure Storage Account.

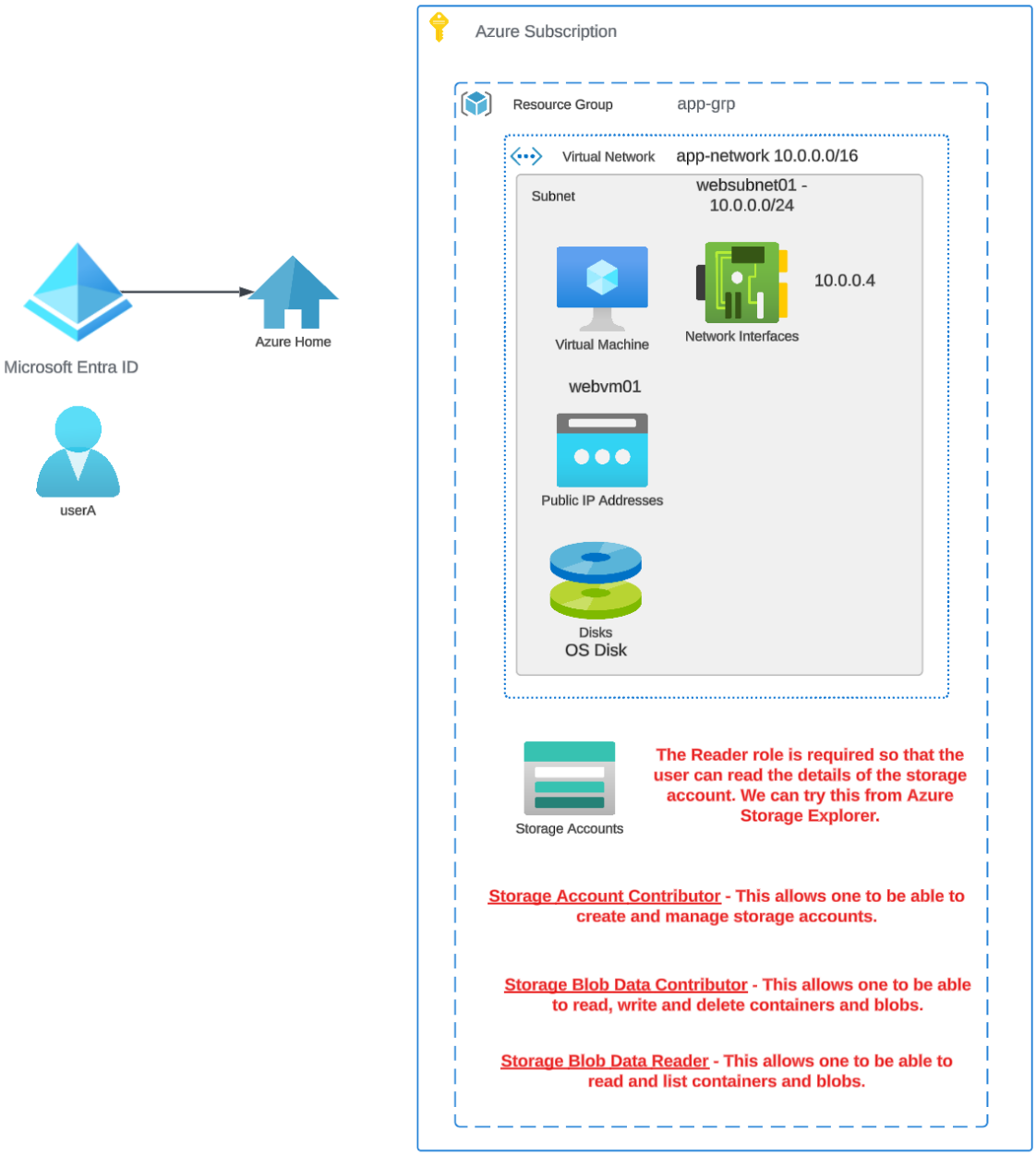
Lab - Role-based assignments - User Access Administrator Role



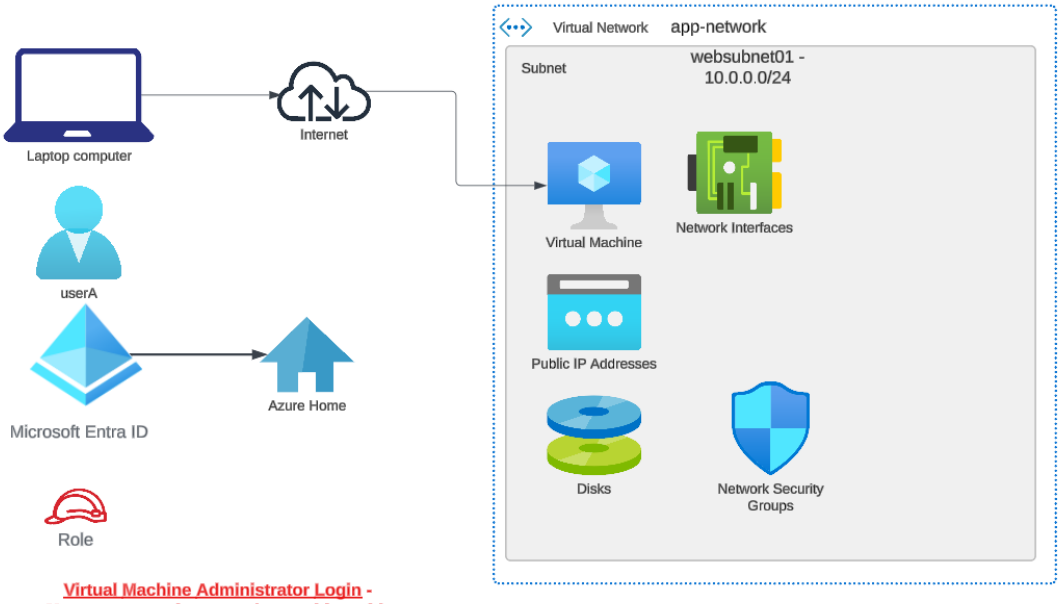
Now let's give UserA the User Access Administrator role at the resource group level.

UserA should now be able to delegate roles to other users as well.

Lab - Role assignments for Azure Storage Accounts



Lab - Role assignments for Azure virtual machines



Virtual Machine Administrator Login - Here users can log onto the machine with admin privileges.

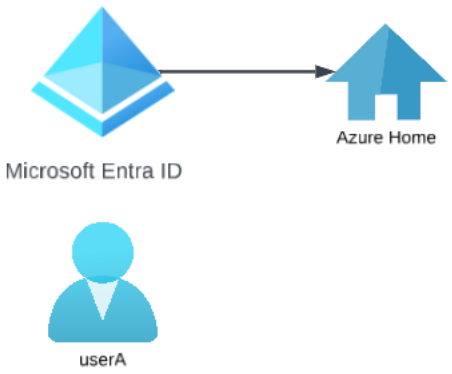
Virtual Machine User Login - Here users can log onto the machine with regular user privileges.

Virtual Machine Contributor - Here users can create and manage virtual machines, manage the disks.

Login with Microsoft Entra ID credentials is supported for Windows Server 2019 Datacenter or later, Windows 10 1809 or later.

The machine needs to be registered with Microsoft Entra ID.

Microsoft Entra ID Roles



Microsoft Entra ID Roles

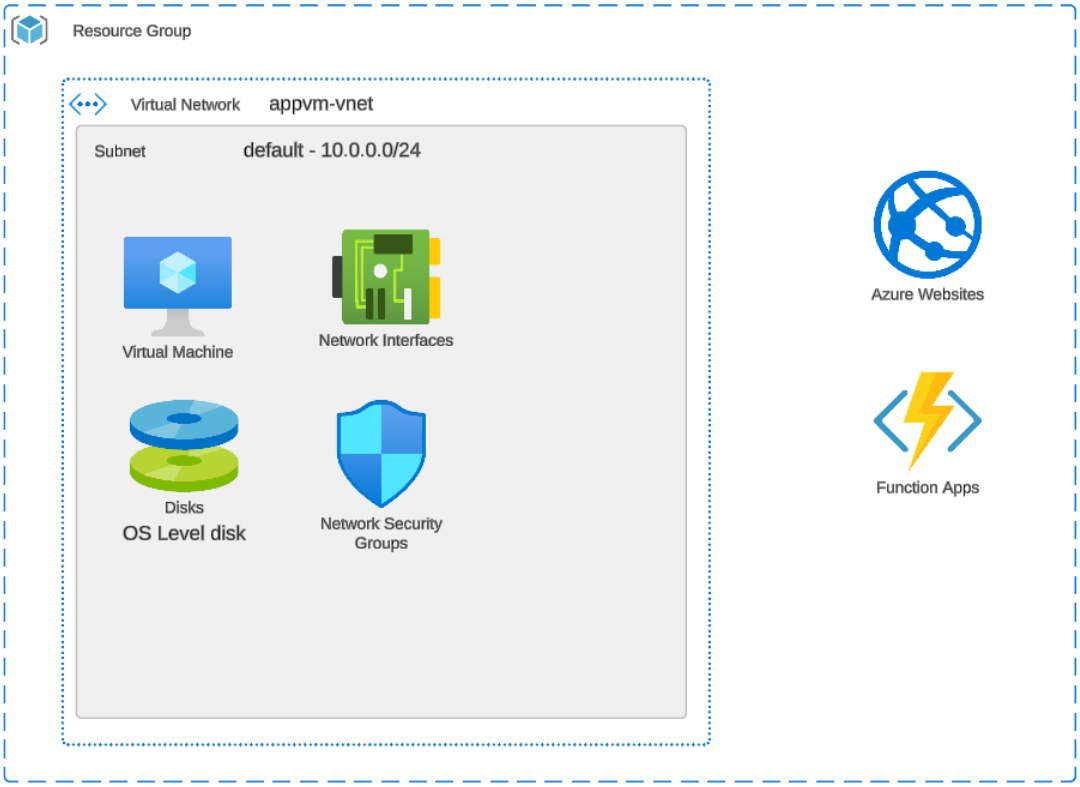
This gives users permissions to carry out operations within Microsoft Entra ID.

This is different from permissions given to resources to an Azure subscription.

Resource tags

Resource tags

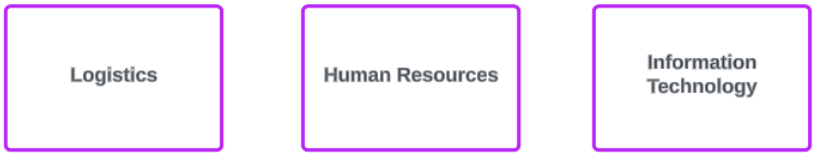
Resource groups help to logically group resources.



If we want to filter resources based on resource group that can be done.

If we want to filter costs based on resource group that is also possible.

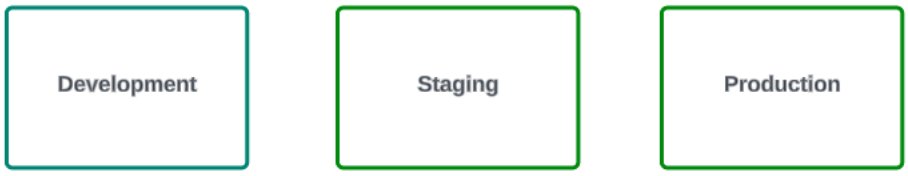
A company might have different departments



A company might have different Applications

Applications could have diferent tiers

Applications could have different Environments



Companies want to be able to discern the different resources via these different attributes.

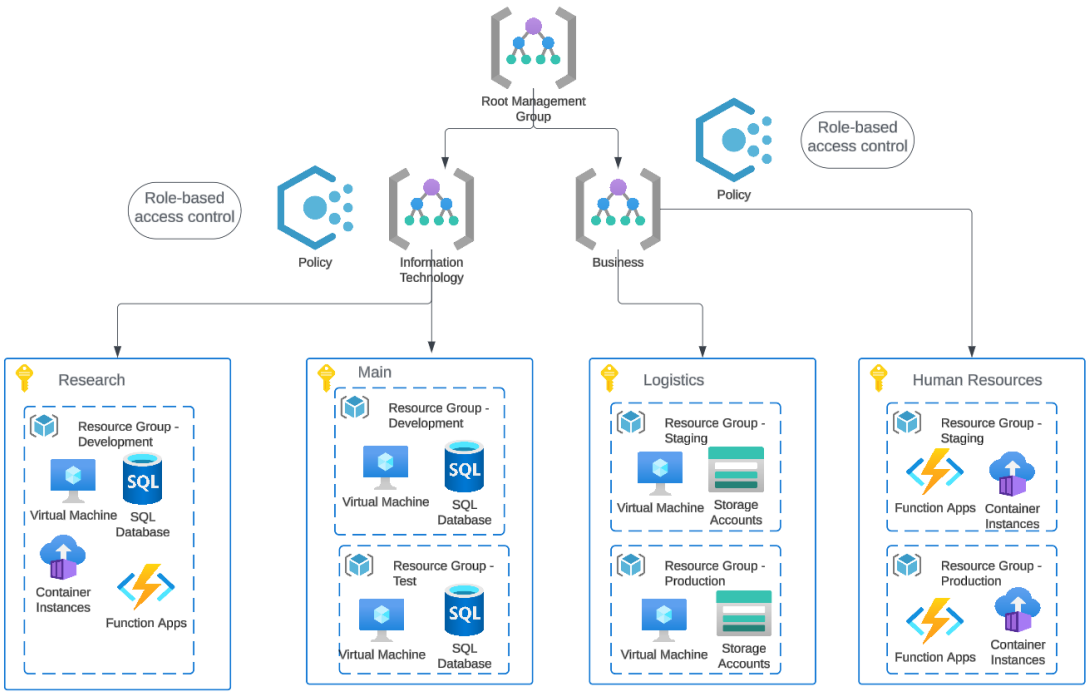
You can add tags to resources, this is extra metadata added to the resources.

It just gives an extra way to organize resources. Even from a billing aspect you can filter resources based on resource tags.

Management Groups

Management Groups

This helps to manage different subscriptions

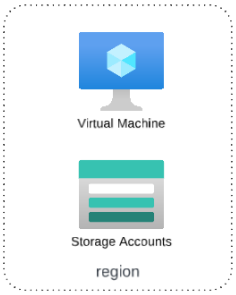


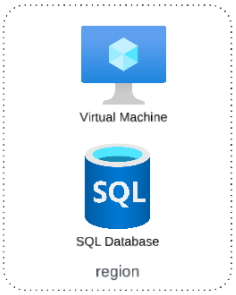
Monitor and backup Azure resources

What is the Azure Monitor Service

This service allows you to collect data for your resources in Azure and your on-premises resources as well.

You can analyze and work on the analyzed data.





You can look at the metrics collected for various resources

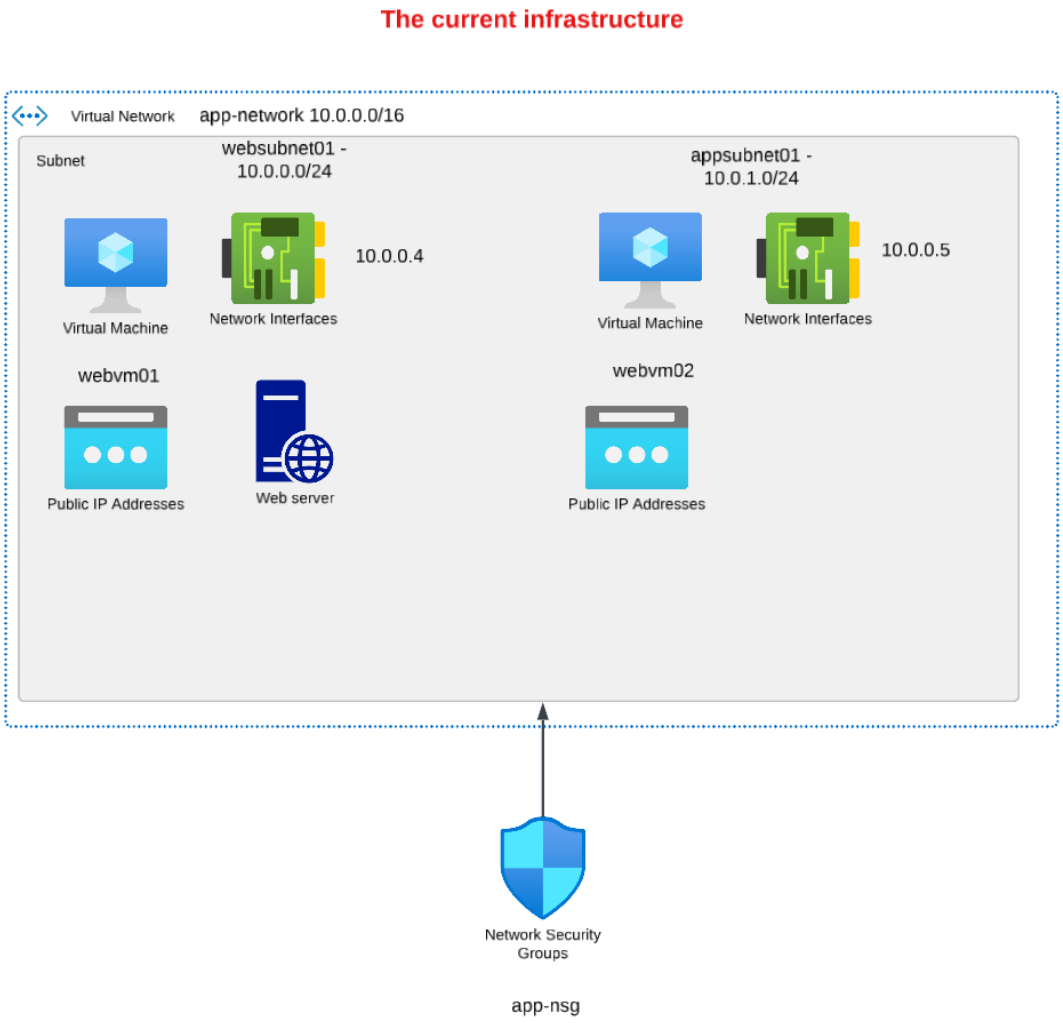
Alerts can be generated if metrics for resources go beyond a particular threshold.

You can also collect logs for various resources.

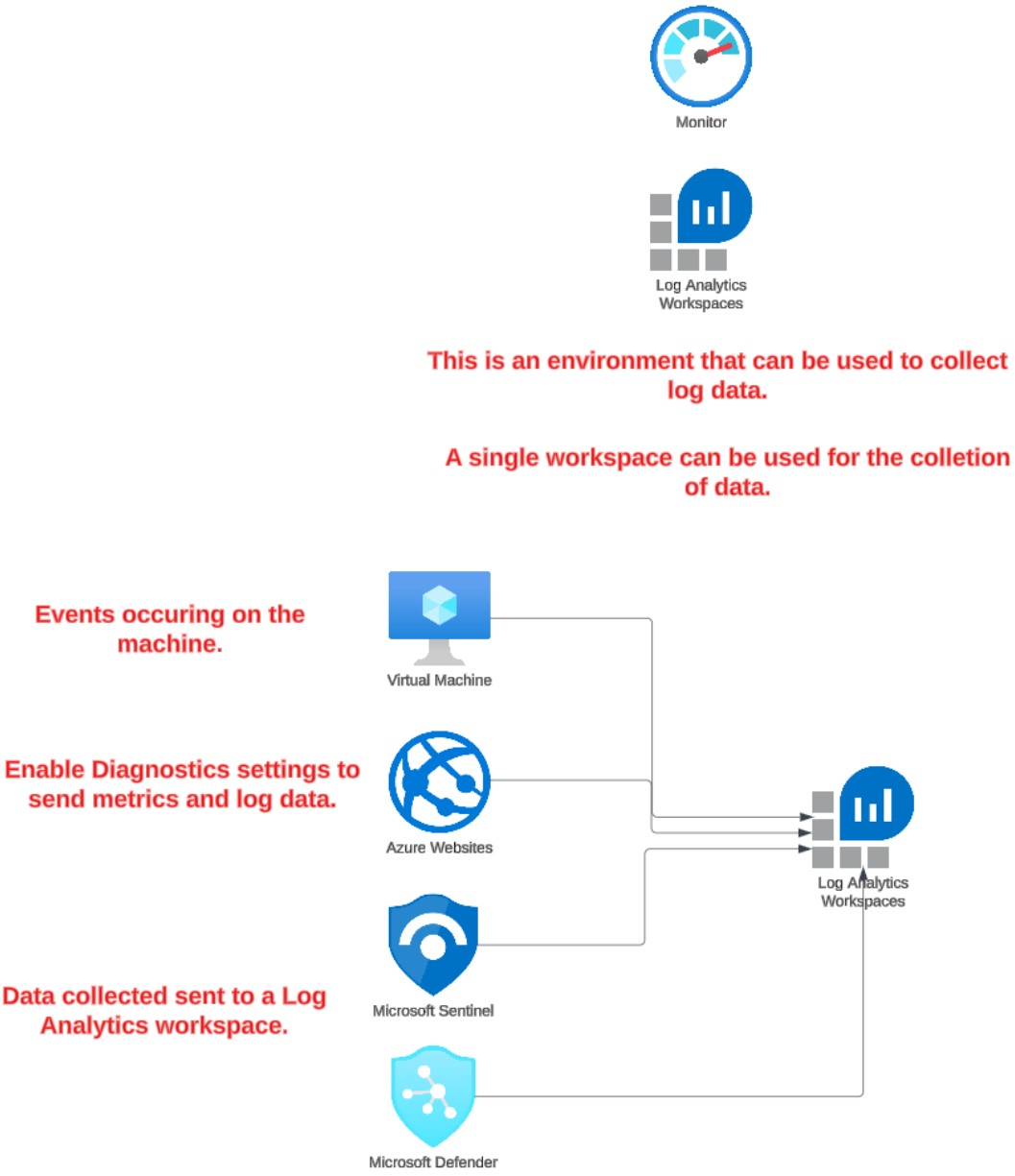
You can get insights when it comes to resources such as Virtual Machines

You can get reports and even Visualize the data.

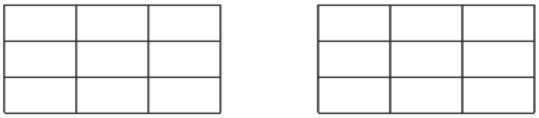
Quick look at Azure Monitor



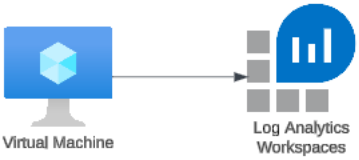
What is a Log Analytics Workspace



Within the Log Analytics workspace, the data is collected into tables that have rows of data.



You are charged for the data that is ingested into the workspace and for how long you plan to retain the data.

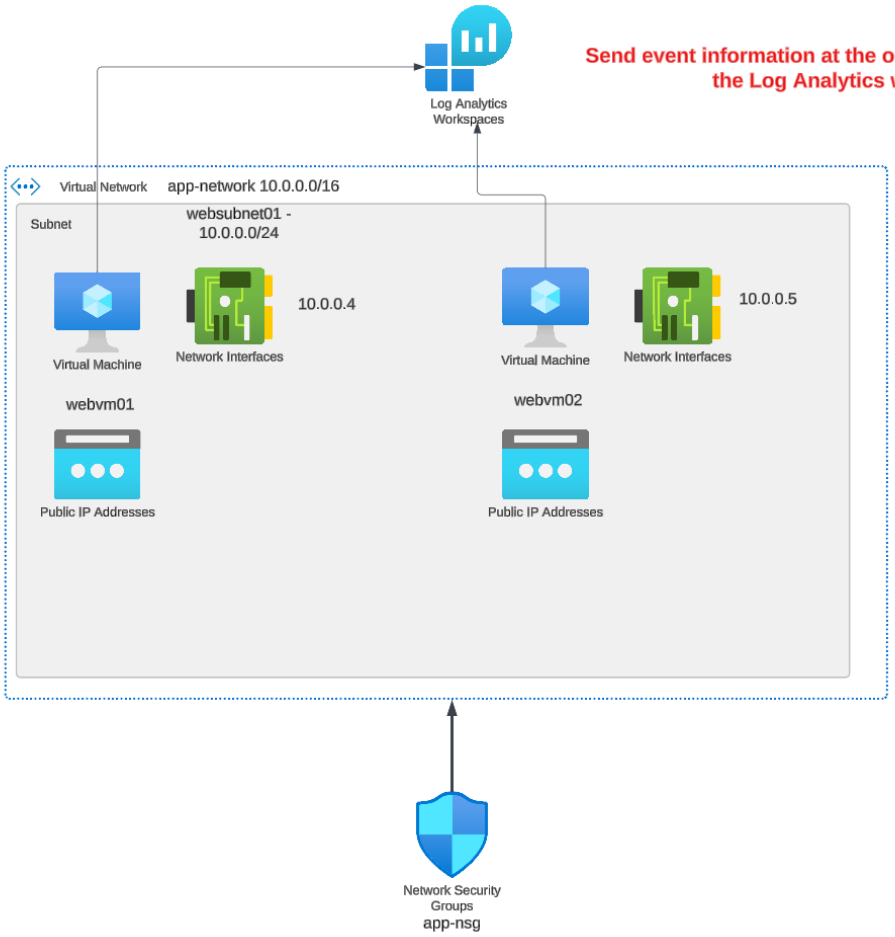


You can have multiple virtual machines that send data to a Log Analytics workspace.

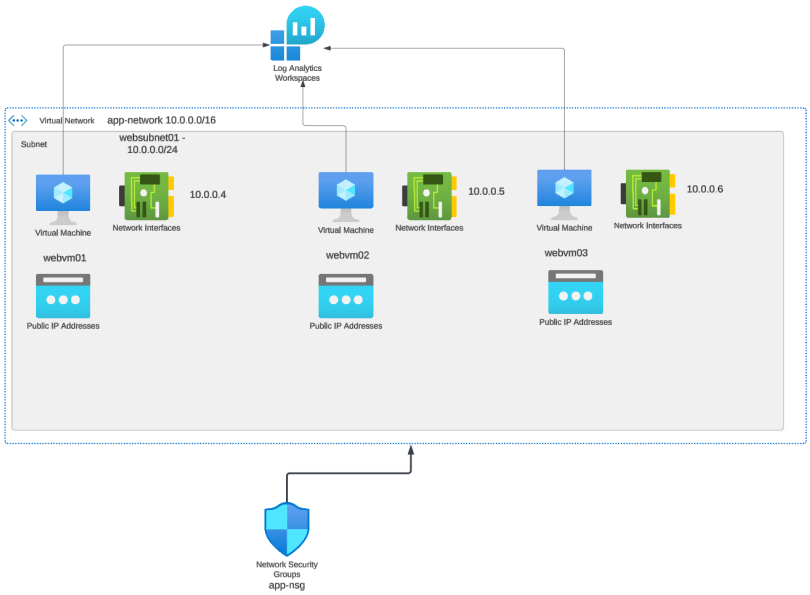
For collecting data from Azure virtual machines , we need to define a data collection rule.

In the rule, we can define the source when it comes to what is the data we need to collect. And then define where to deliver the content to.

Lab - Connecting virtual machines to the workspace



Lab - Sending Custom Logs

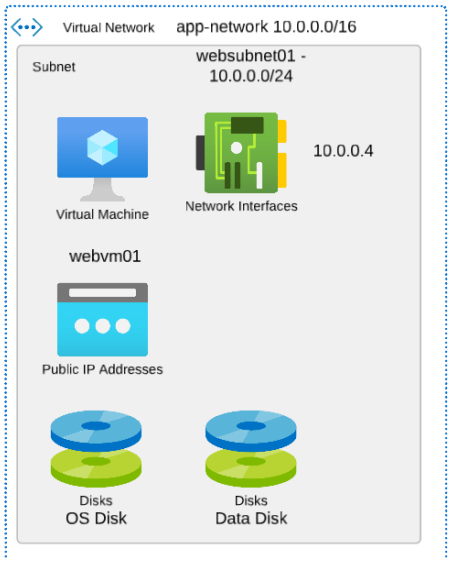


Have a Linux machine in place with NGINX installed.

Create a data collection endpoint.

Create a custom path for the collection of log data of NGINX onto the Log Analytics workspace.

Lab - Azure Virtual Machine – Backup



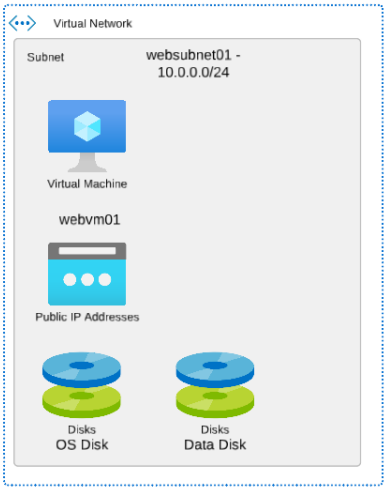
The backup's for a virtual machine are stored in a recovery services vault.

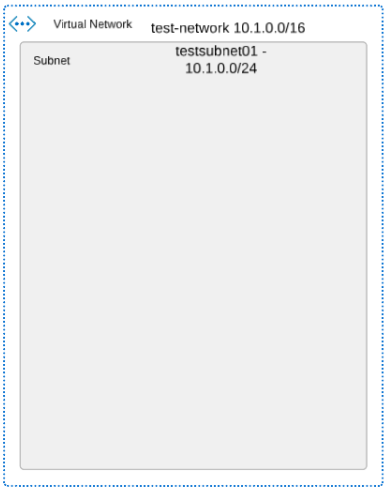
During the backup process, a snapshot is first taken and stored on the VM itself.

For a Windows-based VM, an app-consistent snapshot is taken. If you want , you can perform a quick restore based on the snapshot taken.

For Azure VM backup, the virtual machine and the recovery services vault need to be in the same region.

Lab - Azure Backup - VM Restore





We have a restore point for the Azure VM in the Recovery services vault.

We need to have an Azure Storage account in the same region as the VM and the Recovery services vault.

Restore option

Create a new VM - Here we can create a new virtual machine , but this needs to be created in the same region as the source virtual machine.

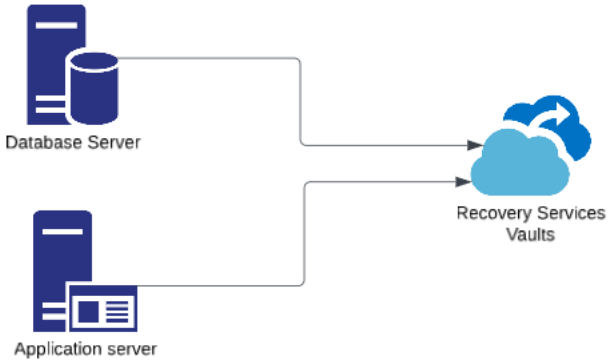
We can restore a VM Disk to create a new VM.

We can restore a disk and use it to replace a disk on the existing VM.

Let's create an Azure storage account a new virtual network. Let's restore the VM to the new virtual network.

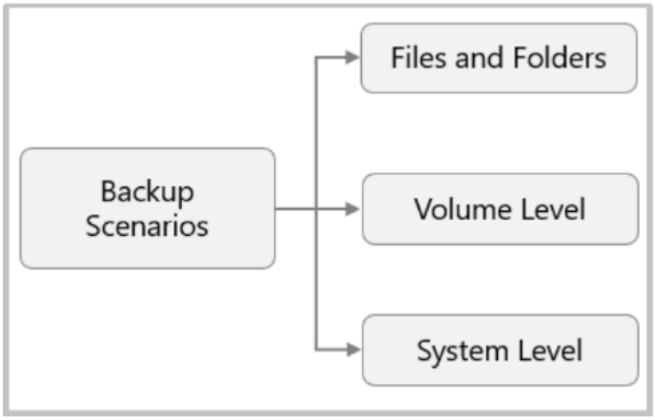
Lab - Azure Backup - MARS agent

You might want to backup individual files and folders from your on-premises servers onto Azure.



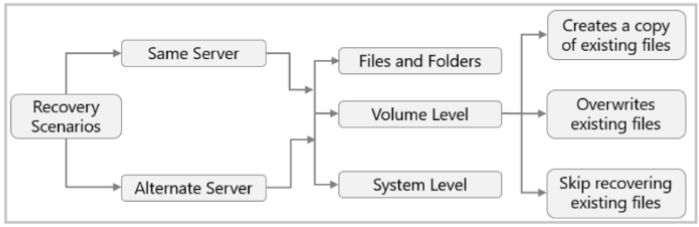
For this we can use the Microsoft Azure Recovery Services agent to take backups and send them onto the Recovery Services vault.

The MARS agent supports the following backup scenarios:

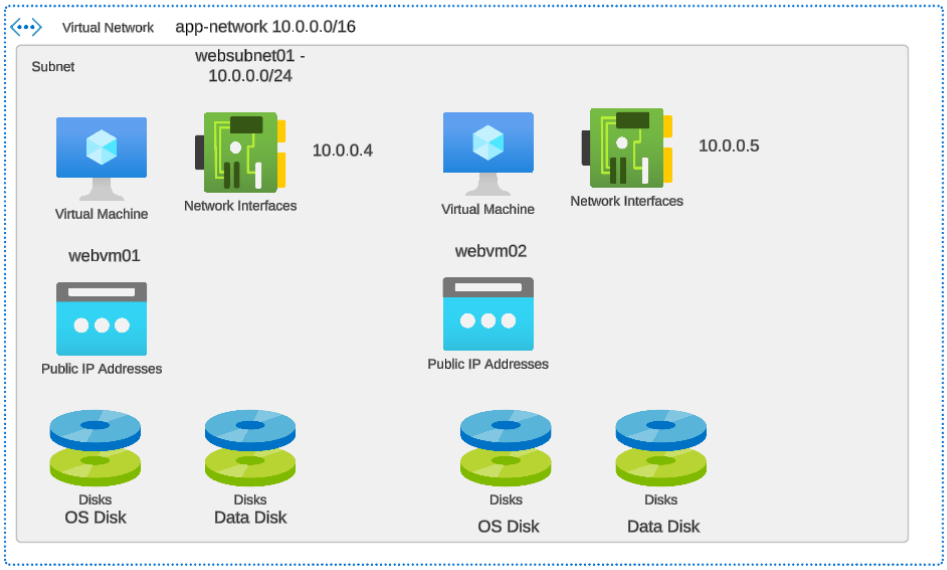


Recovery scenarios

The MARS agent supports the following recovery scenarios:



Reference - https://learn.microsoft.com/en-us/azure/backup/backup-azure-about-mars



We will first install the MARS agent onto an Azure virtual machine - webvm01. Let's imagine that the virtual machine is an on-premises machine.

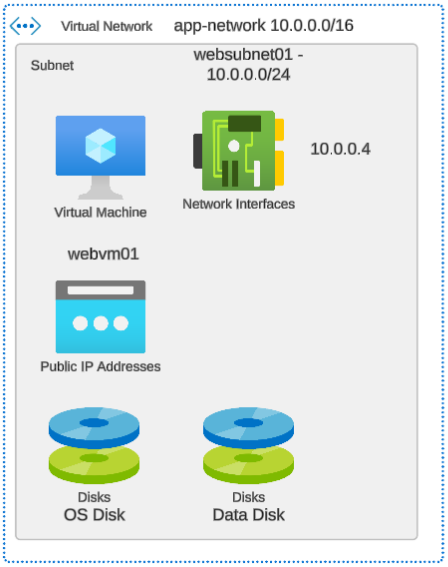
We need to register the MARS agent with a Recovery Services Vault.

We can then schedule a backup of files on webvm01

We will then install the MARS agent on webvm02 and register the agent with the Recovery Services Vault.

We can then recover data onto webvm02.

Azure backup Reports



You can configure Azure Backup reports to audit the backups and restores.

All of log data for the vault can be sent onto a Log Analytics workspace.

The workspace does not need to be in the same region as the Recovery Services Vault.

It can take a day or two before you can start seeing the backup reports.

Azure Site Recovery

Azure Site Recovery is used to replicate workloads that run on physical and virtual machines.

Virtual Machine

Application server

You have an application running in one region on some infrastructure.

The Infrastructure running the application goes down, then the application is no longer available.

If the application is critical , any downtime could result in a loss of revenue for the business.

With Azure Backup, it takes time to perform a restore. It could take hours to get the infrastructure back in place.

Also the backups are taken at specific points in time, so you don't have data till the most recent timestamp.

Azure Site Recovery helps to mitigate such issues by replicating data from one region onto another continuously.

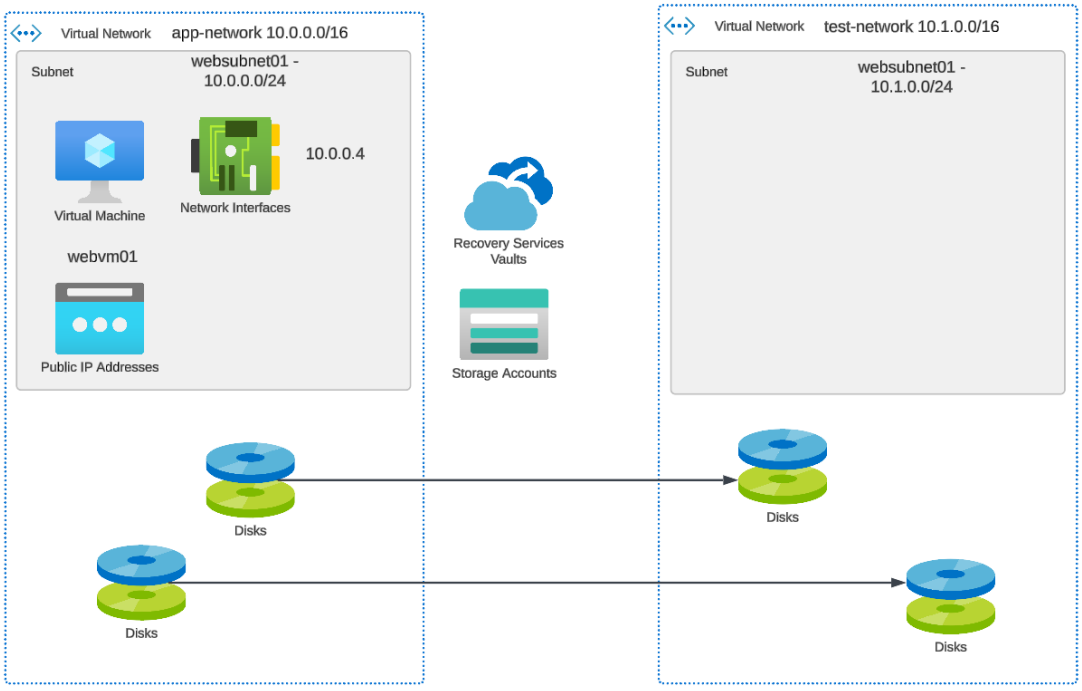
So if the primary infrastructure does go down, you have your setup running in the secondary location.

The costs of maintaining this setup is higher than that of a backup option, but it all depends on the loss of revenue incase of an outage in your infrastructure.

You can replicate Azure virtual machines from one region to another.

You can replicate on-premises VMware or Hyper-V machines to another site.

Azure Site Recovery - Azure VM – Overview



North Europe

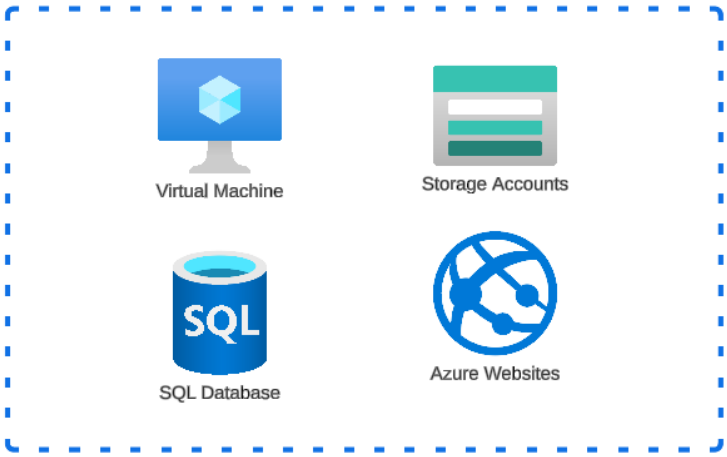
Target region - UK South

The Azure storage account is used as a cache storage account. During the replication process, the VM changes are first stored in the cache before they are sent to the target store.

The disks are replicated to the destination.

Azure Resource Manager Templates

What are Azure Resource Manager templates



Test Environment

We need to rebuild the Test environment everytime a new testing cycle starts.

We want to have a repeatable and reliable way to build the resources everytime.

Templates

We can build an ARM (Azure Resource Manager) template that has the resources defined.

We then submit the template to Azure and the resources will be deployed accordingly.

This is also known as Infrastructure as code.

You can also use Bicep which is a domain-specific language developed by Microsoft that can be used to define the infrastructure that needs to be deployed to Azure.