Contents

[CLOUD CONCEPTS 3](#_Toc87022216)

[RESOURCE GROUP 3](#_Toc87022217)

[CREATING A RESOURCE GROUP 3](#_Toc87022218)

[REGION AND ZONES 3](#_Toc87022219)

[VIRTUAL MACHINE 5](#_Toc87022220)

[AZURE’S VIRTUAL MACHINE SERVICE 5](#_Toc87022221)

[AZURE VIRTUAL MACHINE – KEY CONCEPTS 5](#_Toc87022222)

[DEPLOYING A VIRTUAL MACHINE 5](#_Toc87022223)

[DEPLOYING WINDOWS VM 6](#_Toc87022224)

[DEPLOYING LINUX VM 11](#_Toc87022225)

[INSTALLING SOFTWARES IN VM 12](#_Toc87022226)

[AVAILABILITY 13](#_Toc87022227)

[INCREASING THE AVAILABILITY 14](#_Toc87022228)

[AVAILABILITY SETS 14](#_Toc87022229)

[AVAILABILITY ZONES 15](#_Toc87022230)

[NOTES ON AVAILABILITY ZONES AND SET 16](#_Toc87022231)

[VIRTUAL MACHINE SCALE SETS 16](#_Toc87022232)

[AZURE DEDICATED HOST 16](#_Toc87022233)

[AZURE SPOT INSTANCES 16](#_Toc87022234)

[WORKLOAD 16](#_Toc87022235)

[IMPORTANT USE CASES AND SOLUTIONS 17](#_Toc87022236)

[AZURE VIRTUAL NETWORK 17](#_Toc87022237)

[CREATING A VIRTUAL NETWORK 18](#_Toc87022238)

[CREATING A SUBNET IN VIRTUAL NETWORK 18](#_Toc87022239)

[CREATING A VIRTUAL MACHINE IN VIRTUAL NETWORK 19](#_Toc87022240)

[COMMUNICATION ACROSS VIRTUAL MACHINES IN A VIRTUAL NETWORK 20](#_Toc87022241)

[NETWORK SECURITY GROUP 20](#_Toc87022242)

[APPLICATION SECURITY GROUP 21](#_Toc87022243)

[NETWORK CONNECTIVITY OPTIONS 21](#_Toc87022244)

[VIRTUAL NETWORK PEERING 21](#_Toc87022245)

[POINT-TO-SITE VPN CONNECTION 22](#_Toc87022246)

[SITE-TO-SITE VPN CONNECTION 22](#_Toc87022247)

[AZURE EXPRESS ROUTE 23](#_Toc87022248)

[AZURE CORE SERVICES 23](#_Toc87022249)

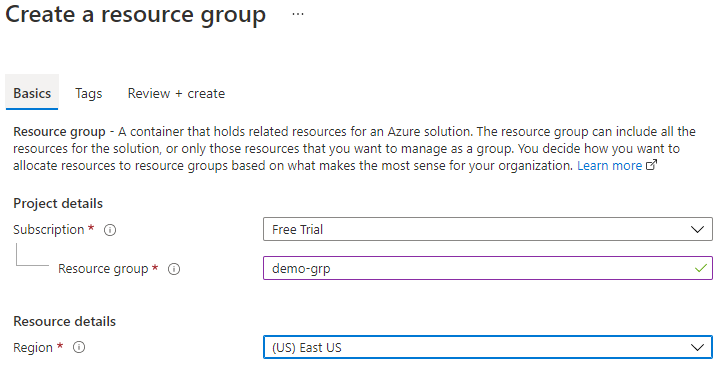
[AZURE STORAGE 24](#_Toc87022250)

# CLOUD CONCEPTS

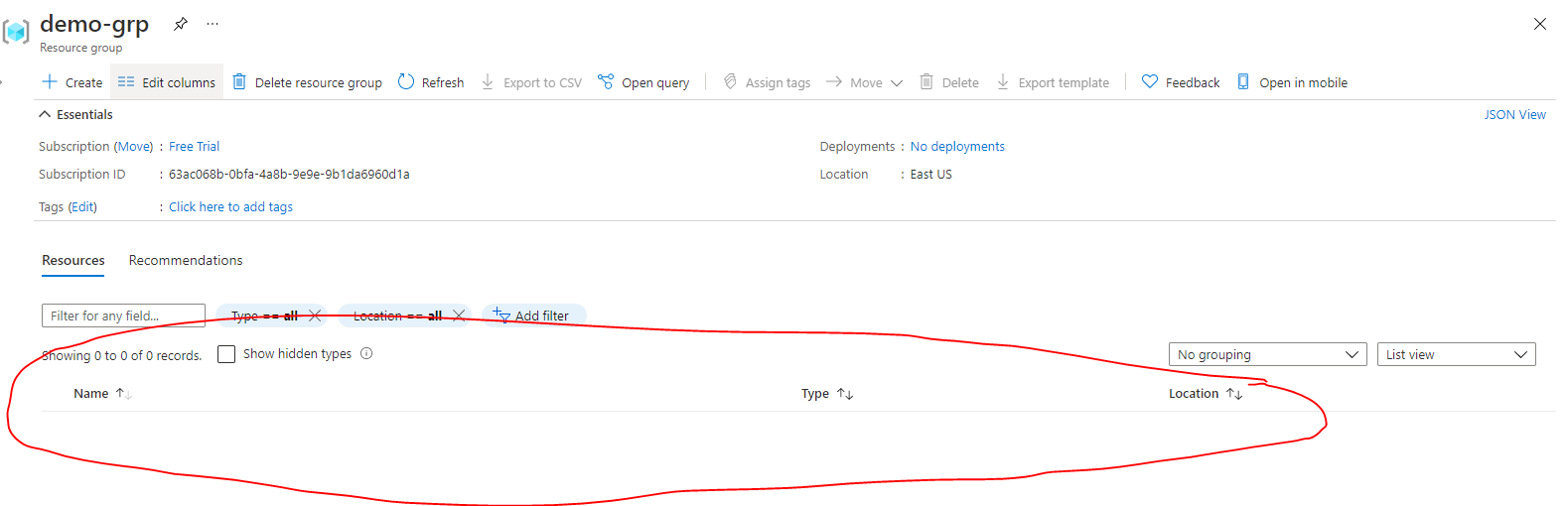
# RESOURCE GROUP

* Resource Group can be considered as a logical container/separation of resources. For example – For an organization resource group can be separated based resources a department of an organization is using.
* Every resource we create in Azure platform must be a part of resource group.
* There is no cost involved in creation of resource group.

## CREATING A RESOURCE GROUP



* All the resources are tied to a subscription for billing aspects.
* The resource group must associate to a region.
* Initially there will be no resource in the resource group. When we start adding resources to the resource group it will show up in the below table



# REGION AND ZONES

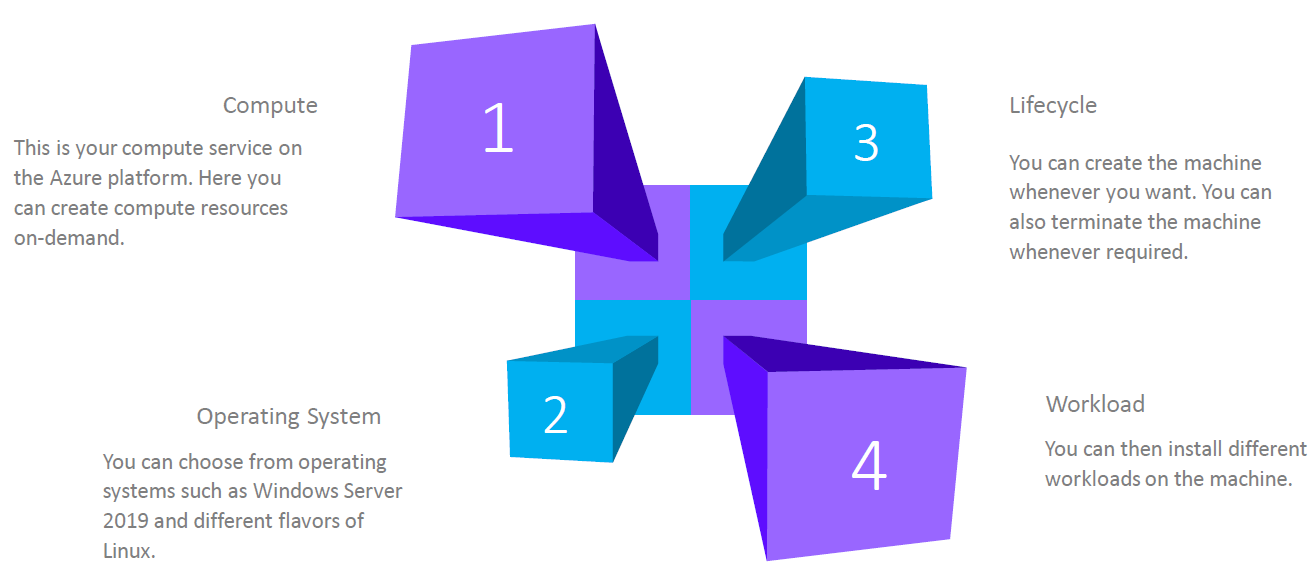
|  |  |
| --- | --- |
|  | CASE 1: SINGLE DATA CENTER IN A REGION  Imagine that your application is deployed in a data center in London  WHAT WOULD BE THE CHALLENGES?   * Challenge 1: Slow access for users from other parts of the world (high latency) * Challenge 2: What if the data center crashes?   *Your application goes down (low availability)* |
|  | CASE 2: MULTIPLE DATA CENTER IN A REGION  Let's add in one more data center in London  WHAT WOULD BE THE CHALLENGES?   * Challenge 1: Slow access for users from other parts of the world * Challenge 2 (SOLVED) : What if one data center crashes?   *Your application is still available from the other data center*   * Challenge 3: What if entire region of London is unavailable?   *Your application goes down*  16 |
| CASE 3: MULTIPLE REGION – MULTIPLE DATA CENTER    Let's add a new region: Mumbai  WHAT WOULD BE THE CHALLENGES?   * Challenge 1 (PARTLY SOLVED): Slow access for users from other parts of the world   *You can solve this by adding deployments for your applications in other regions*   * Challenge 2 (SOLVED) : What if one data center crashes?   *Your application is still live from the other data centers*   * Challenge 3 (SOLVED) : What if entire region of London is unavailable?   *Your application is served from Mumbai*  ADVANTAGES:   * *High Availability* * *Low Latency* * *Global Footprint* * *Adhere to government regulations* | |

# VIRTUAL MACHINE

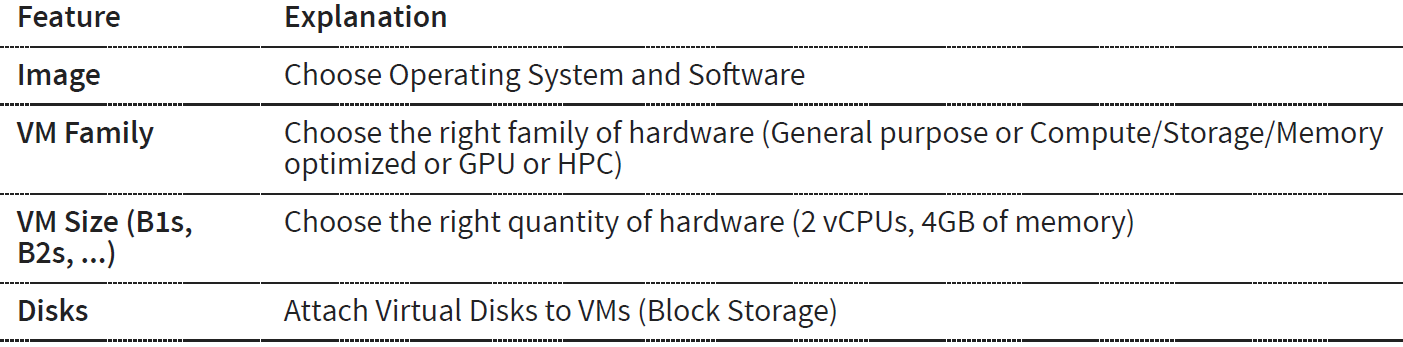
* It is a computer file typically called as an image which behaves like an actual computer.
* It runs in windows, Linux etc. This gives you a flexibility that can run multiple machines in a physical computer.
* Each system can have a different operating system.
* Each of these virtual machines provides its own virtual hardware which includes CPUs, memory, hard drives, network interfaces and other such devices.

## AZURE’S VIRTUAL MACHINE SERVICE

* In corporate data centers, applications are deployed to physical servers, but we deploy applications in the cloud by renting(provisioning) virtual servers (Virtual Machine)

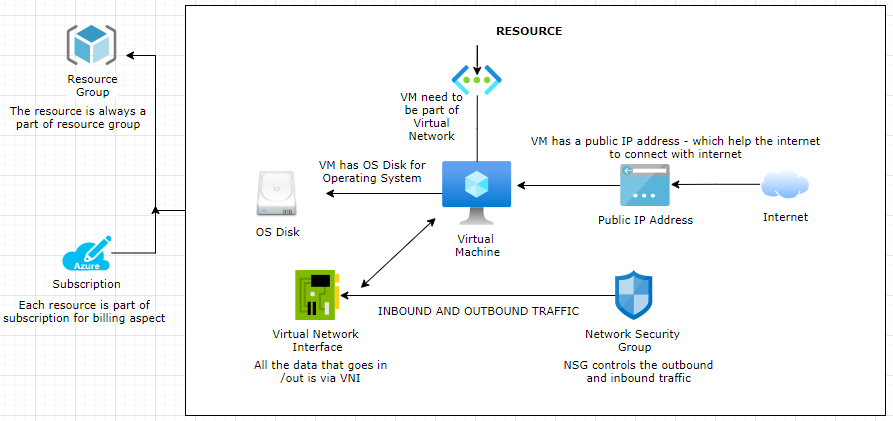


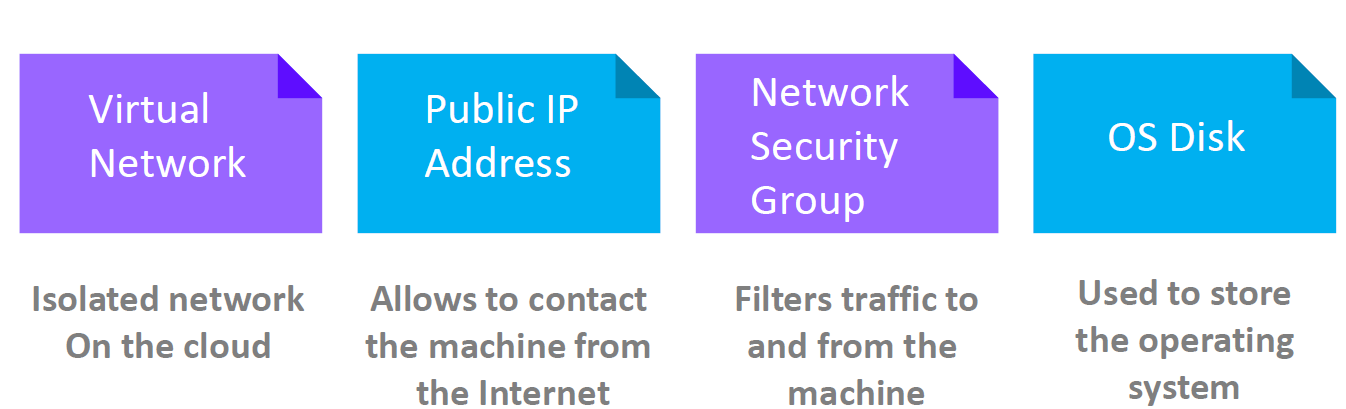
### AZURE VIRTUAL MACHINE – KEY CONCEPTS



## DEPLOYING A VIRTUAL MACHINE

* When we deploy a virtual machine – there are other aspects also get deployed with it.
* VM is a compute resource in Azure Platform. It is an Infrastructure as a service in azure platform





#### OS DISK

* The virtual machine has OS Disk where operating system can be installed
* Addition disk can be added too

#### VIRTUAL NETWORK INTERFACE

* Virtual Network Interface is like network interface card
* All the data that goes in or out go via Virtual Network Interface

#### NETWORK SECURITY GROUP

* It controls all the inbound and outbound traffic

#### VIRTUAL NETWORK

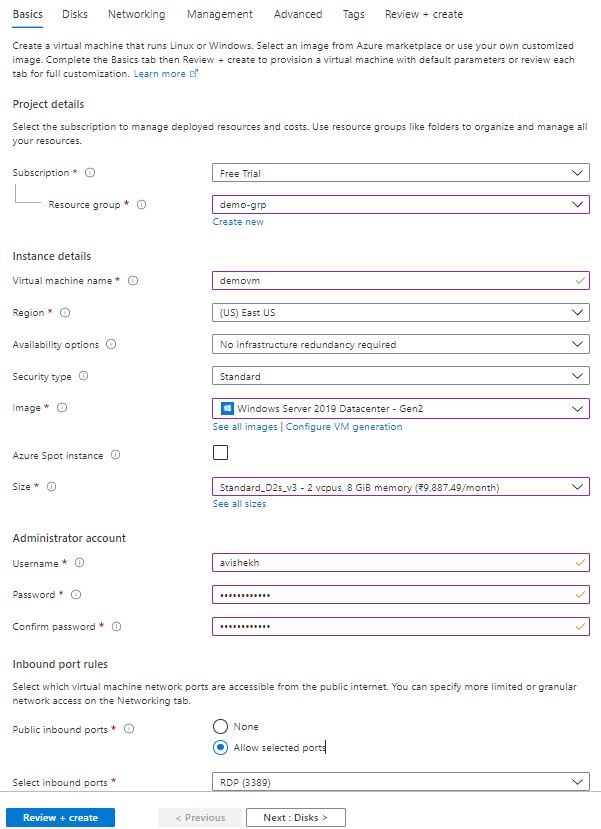
* Every VM is part of a Virtual Network.

#### PUBLIC IP ADDRESS

* The VM are always associated to a public ip address –through which the internet can connect with the VM.

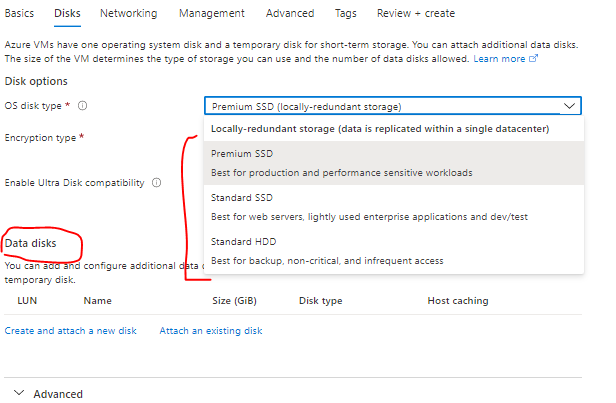
### DEPLOYING WINDOWS VM

#### BASIC



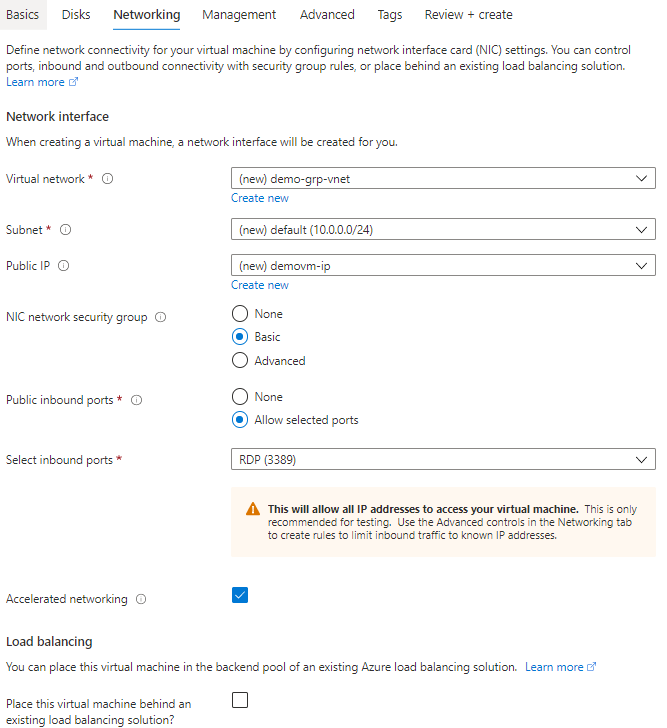
|  |  |
| --- | --- |
| RESOURCE GROUP | The resource group of the VM |
| VM NAME | Name of the Virtual machine |
| REGION | Region in which this VM will be created |
| IMAGE | This is the name of the image – which will be used to set-up OS in the VM. |
| SIZE | This defines the size of the resources in the VM like CPUs and RAM |
| SELECT INBOUND PORTS | This defines on which port the inbound traffic to VM is allowed. For window we user RDP(Remote Desktop) at port 3389 |

#### DISK



|  |  |
| --- | --- |
| OS DISKTYPE | * This is the disk which will be used for the storage of data |
| DATA DISK | * When we configure the VM – by default we get the OS disk . For additional disk we can add as a Data disk to the VM |

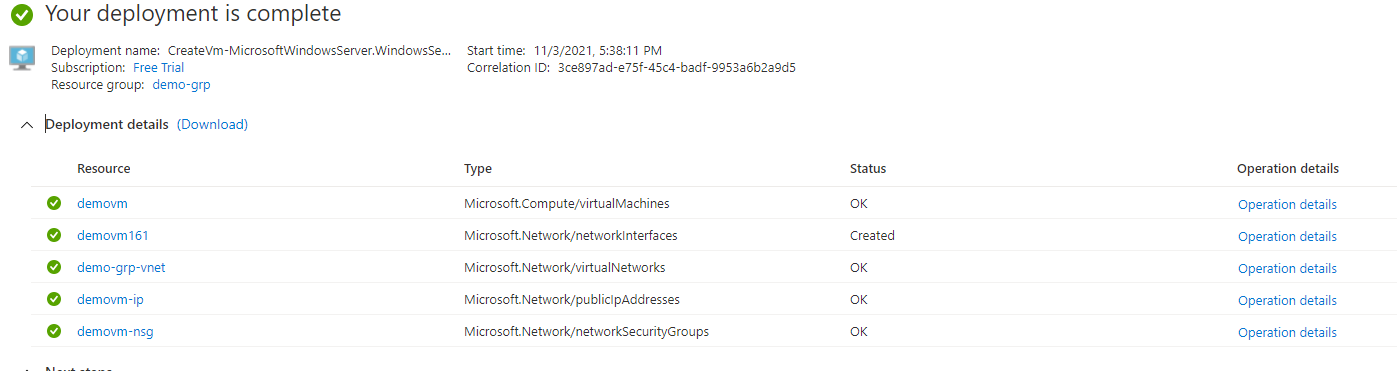
#### NETWORKING



|  |  |
| --- | --- |
| VIRTUAL NETWORK |  |
| SUBNET |  |
| PUBLIC IP ADDRESS | The VM can be accessed on Internet using its public IP address |

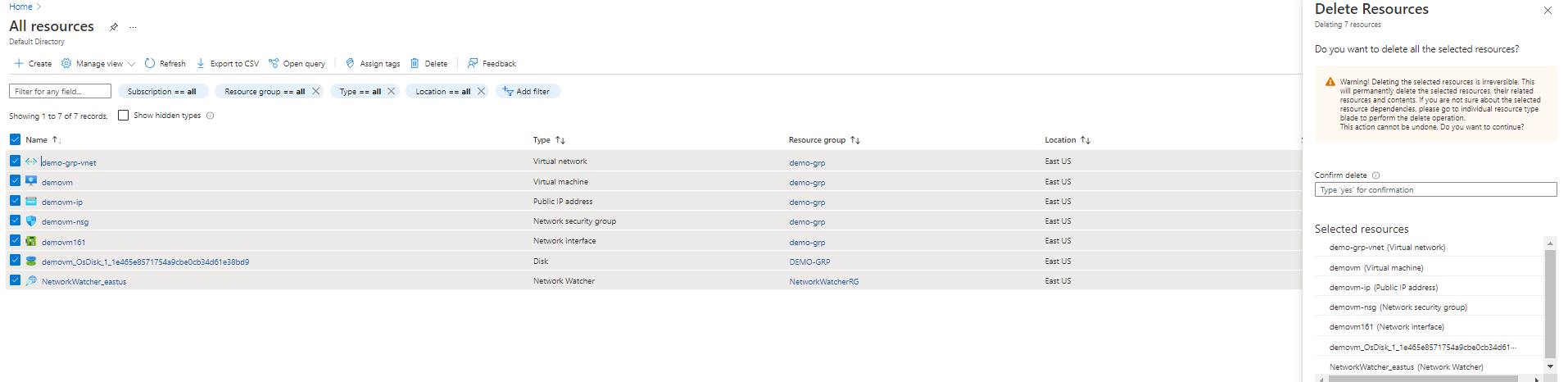
#### VM CREATED

* The below diagram shows the created VM and other related resources which are created with the VM like NIC, VM , NSG and public IP address.



#### DELETING A VM

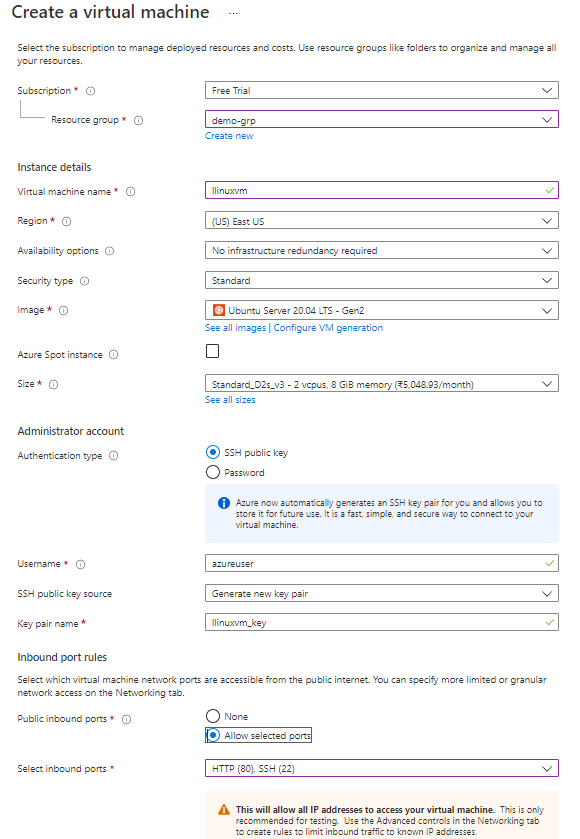
* From the *menu 🡪 All Resources*. Select all the resources which are related to the VM 🡪 Type yes and Delete



#### CONNECTING TO VM (WINDOWS) USING RDP

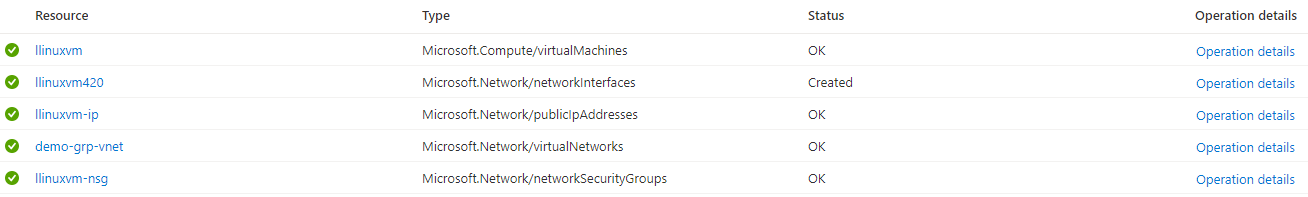
|  |  |
| --- | --- |
|  | * To connect with Windows based VM we use RDP * SSH is used to connect to Linux based VM |
|  | * To connect to the windows VM- download the RDP file * Open the downloaded RDP and Enter the username/password (used while creating the VM) |

### DEPLOYING LINUX VM



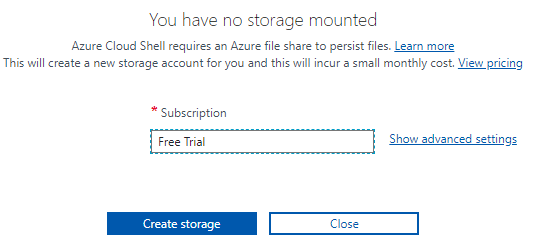
|  |  |
| --- | --- |
|  | * This will show a pop- up to download the SSH key * Download the SSH key – This key will be used to login to VM using SSH. * Note to connect with Linux VM we use SSH. |

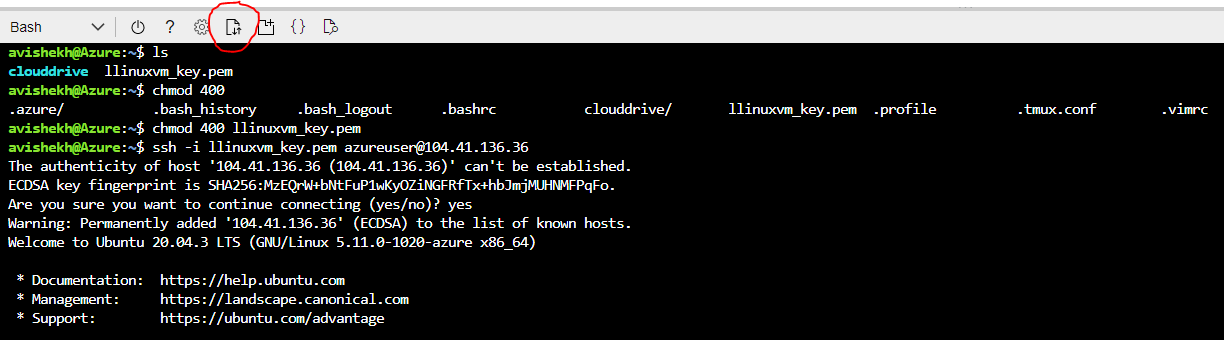
**RESOURCES CREATED WITH VM**



#### CONNECTING TO VM (SSH)

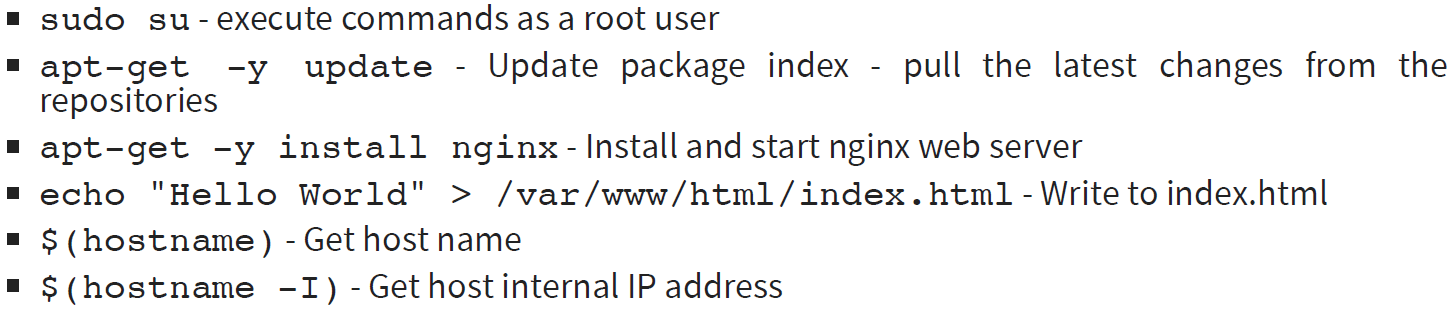
* Open the Cloud Shell and choose Bash
* Select the subscription 🡪 Create Storage



* Upload the SSH key using upload option 
* Navigate to VM 🡪 Connect 🡪SSH . Follow the steps to SSH the VM

### INSTALLING SOFTWARES IN VM

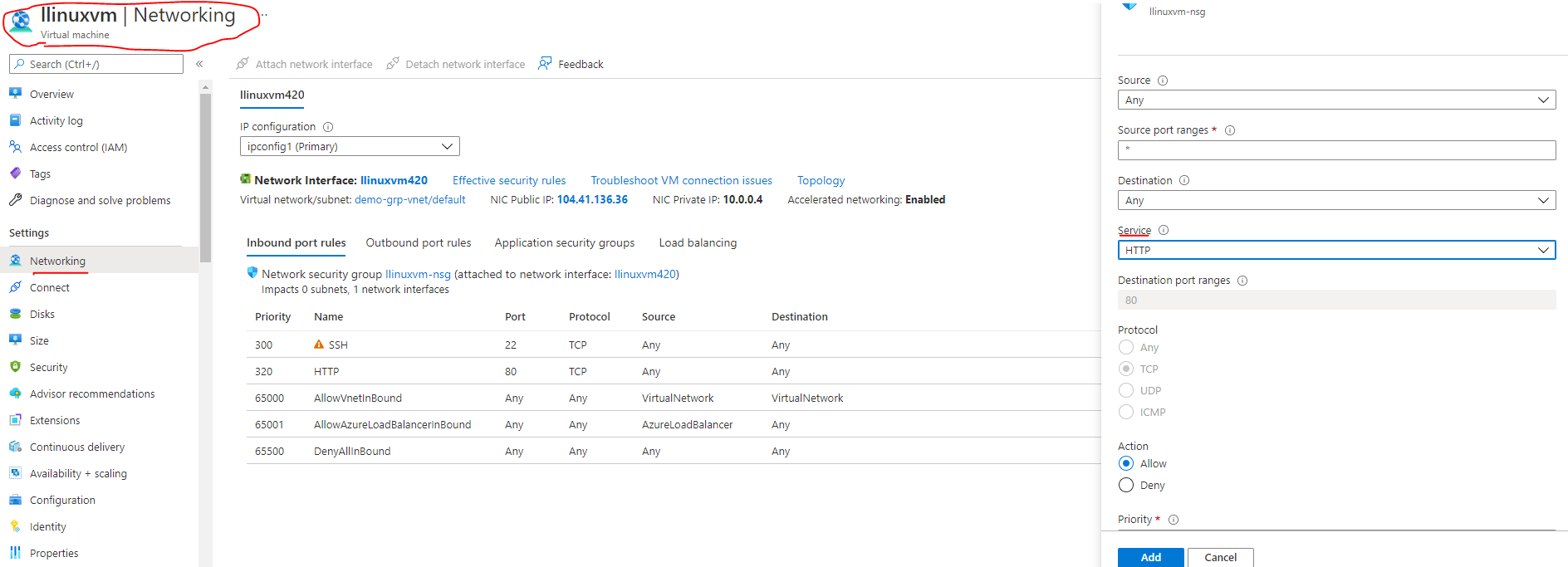
#### INSTALLING NGINX (HTTP SERVER)



* The nginx webserver can be accessed using the public IP address of the VM(<http://104.41.136.36/> )

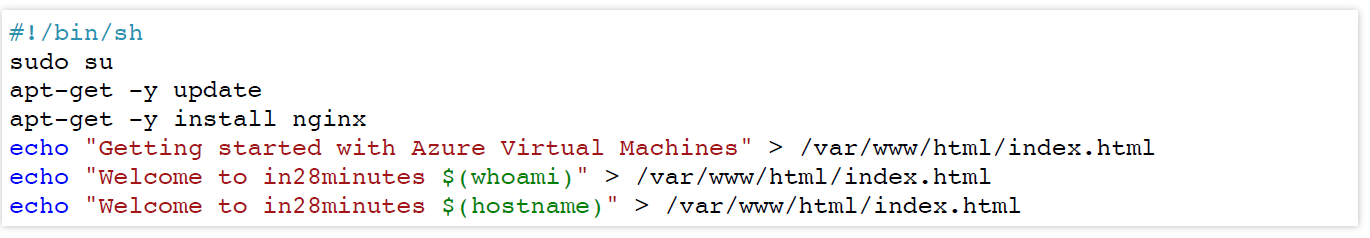
##### ADDING INBOUND PORT RULE

* We can add the inbound port rule to accept the incoming request. For example – we can enable the HTTP service at port 80 by adding a new inbound port rule.
* The same can be done while creating the VM (***Basic 🡪 Select inbound port***)

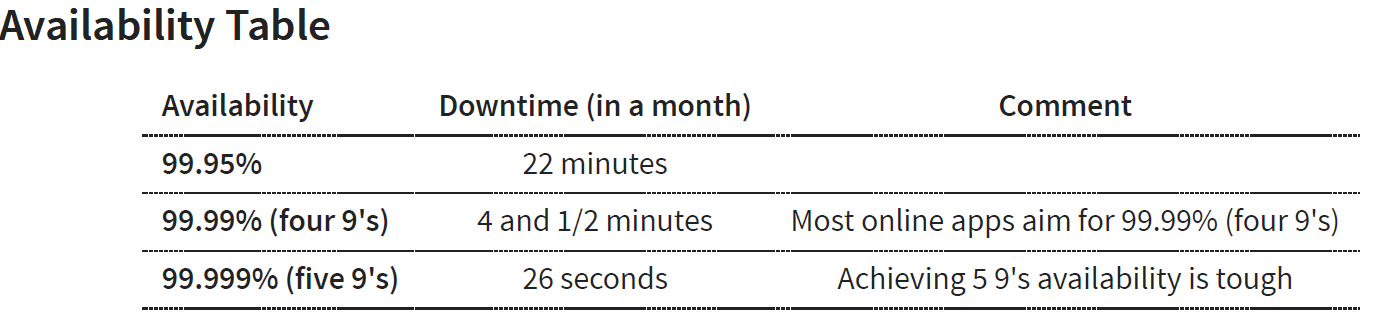


#### USING CLOUD INIT

* In the above steps – We first created the VM and the installed the nginx server. We did all by doing the “***ssh***” and running command from cloud shell.
* Just In case if we want to run a specific set of command after the VM start up – we can write the series of command in “Advanced Tab” 🡪 Cloud init as a bash script. As show below.



## AVAILABILITY



### INCREASING THE AVAILABILITY

* **SINGLE INSTANCE VM:** If we are using single instance VM we can use a specific disk type . Below is the availbility – when we select a spefic disk type(from Disk Tab)

|  |  |
| --- | --- |
| **DISK TYPE** | **AVAILABILITY** |
| Premium SSD or Ultra Disk | 99.9% |
| Standard SSD Managed Disks | 99.5% |
| Standard HDD Managed Disks | *95%* |

Two or more instances in same Availability Set: 99.95%

* Availability set is a logical grouping of VMs
  + **FAULT DOMAINS**: Group of VMs sharing a common power source and network switch. We can create upto 3 fault domains
  + **UPDATE DOMAINS**: Group of VMs that are rebooted (updated) at the same time.We can create up to 20 update domains
* Two or more instances in two or more Availability Zones in the same Azure region: 99.99%
* ***Summary: Create multiple instances in multiple AZs if you want high availability***

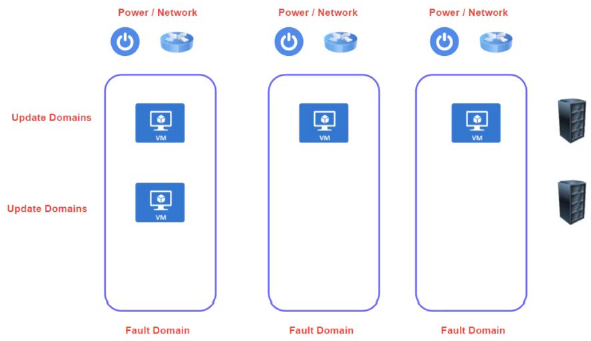
### AVAILABILITY SETS

|  |  |
| --- | --- |
|  | * When we deploy the application is multiple VMs – these VM are actually created in phycial server in Azure Data Center. * The phycial server has its dedicated power source and networking. * When we spin-up a VM – we cannot control in which phycial server the VMs are created. * Just in case the physical server goes down (may be duethe power source) , then both VMs will go down and hence the application. * To solve this option Azure platform has offers “Availability Set” |

* When a VM is created it is configured to be part of Fault Domain and Update Domain.
* This feature helps to protect your machines against infrastructure level failures.
* An unplanned event wherein the underlying infrastructure fails unexpectedly. The failures could be attributed to network failures , local disk failures or even rack failures
* Planned maintenance events , wherein Microsoft needs to make planned updates to the underlying physical environment. In such cases , a reboot might be required on your virtual machine
* You can increase the availability of your application by making use of availability sets. Each virtual machine that is assigned to the availability set is assigned a separate fault and update domain.

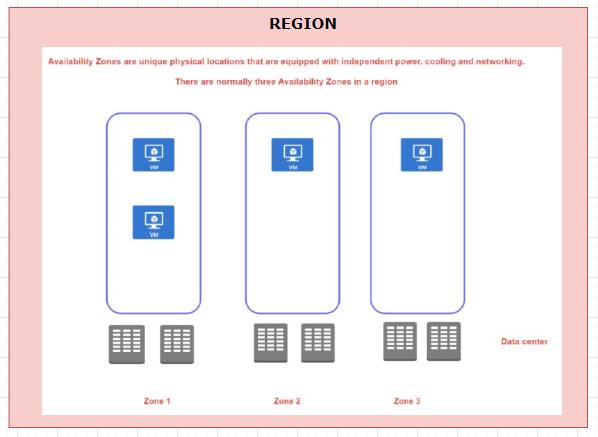
|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **UD1** | **VM1** | **VM3** | | **UD2** | **VM2** | **VM4** | |  | **FD1** | **FD2** | | * In the following matrix diagram – Virtual Machine VM1 & VM2 belong to a Fault Domain (FD1)and VM3 and VM4 belong to fault domain FD2 * VM1 and VM3 belong to update domain UD1 and VM2 an VM4 belong to update domain UD2 |

* As the fault domain shares the common power source and network switch – Just in case some goes wrong with this fault domain – then the application will be still available via VM3 and VM4 and vice versa.
* When the physical server needs an update – It will be updated based on update domain. Hence – if update domain UD1 is getting updated then applicatiomn will be available via VM2 and VM4.



### AVAILABILITY ZONES

* In a specific zone – we have multiple zones and each zone is a collection of data centers.
* Availability zones are unique physical location that are equiped with independent power , colling and networking.
* This features help provides better availability for your application by protecting them from datacenterfailures
* Each Availability zone is a unique physical location in an Azure region
* Each zone comprises of one or more data centersthat has independent power, cooling, and networking
* Using Availability Zones, you can be guaranteed an availability of 99.99% for your virtual machines. You need to ensure that you have 2 or more virtual machines running across multiple availability zones.



* When we create a VM in a availability zone – It is in turn mapped to the data center in that availability zone.
* The advantage we get with availability zone is that – if a data centers in a zone goes down – the application will eb up and running from other zones in a specific region.

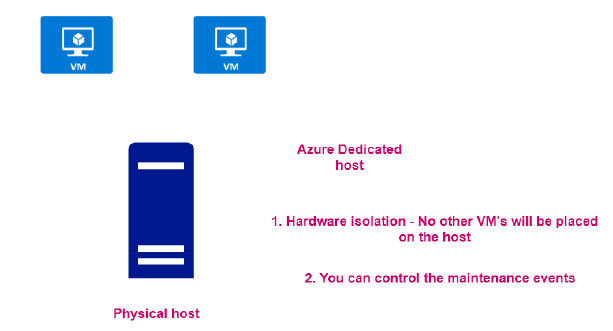
### NOTES ON AVAILABILITY ZONES AND SET

* There is no extra cost involved in creating availability zone or sets. But the is a costing aspect – when it comes to VM communication between the Zones. But this cost is not applicable when it comes to availability set as those VM are part of same physical data center.
* When we create a VM is availability zone or set – it our responsibility to sync the application in all the newly created VMs- To achieve the sync we can make use of extension of custom script called “Cloud Init Script”.

## VIRTUAL MACHINE SCALE SETS

* Virtual machine scale set simplify the creation and management of multiple VMs(group of VMs)
* VM scale set also allow as to add a load balancer
* Supports manual and auto scaling
* Distribute VM instances across multiple Availability Zones
* Supports 1000 VM instances in a single scale set.

## AZURE DEDICATED HOST



* When we create VMs, they are get created in physical server/ host in the azure data center
* In Azure – it come with a capability to assign the entire physical host as a resource. Note this capability are usually leveraged by large scale organization.

#### ADVANTANGE OF DEDICATED HOST

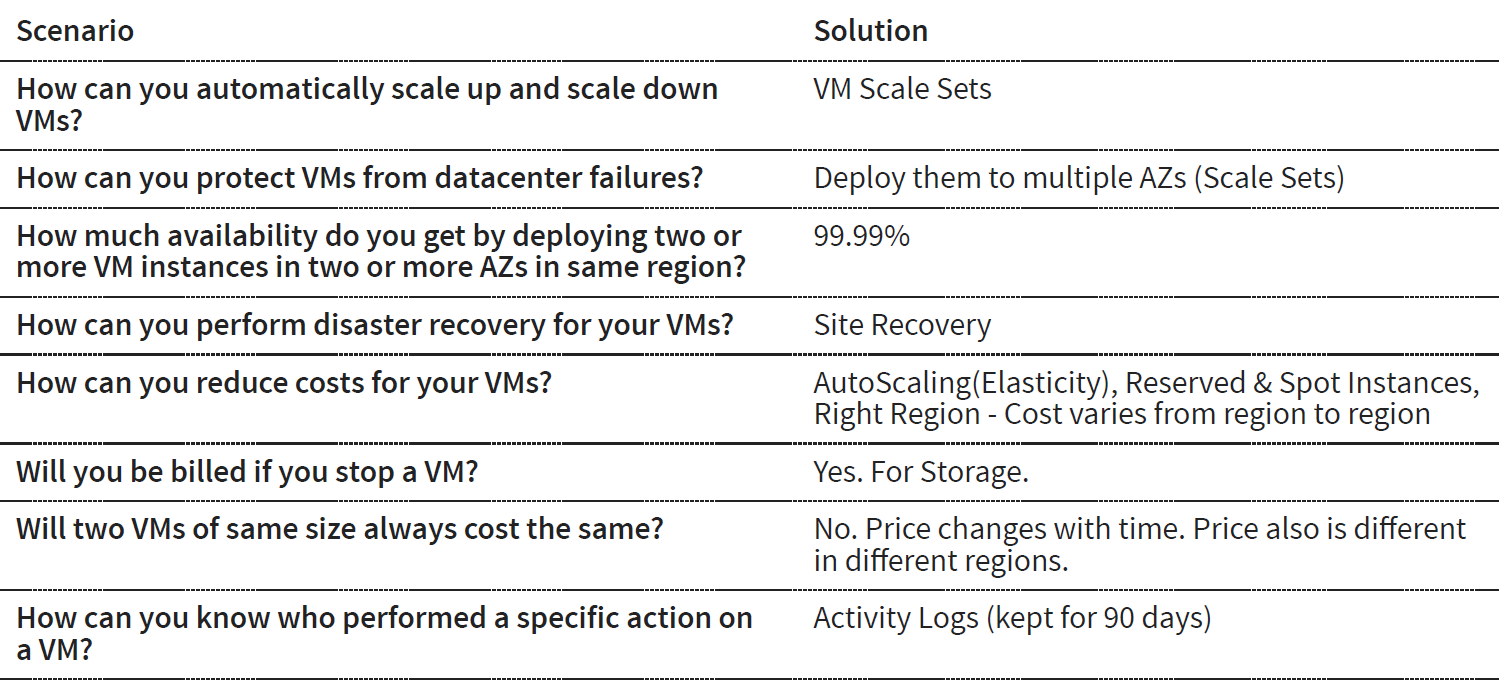
* As it is a dedicated host – no other VM can be placed in the host.
* We can able to control the maintenance events of the VMs

## AZURE SPOT INSTANCES

## WORKLOAD

|  |  |
| --- | --- |
|  | * Workload is unit functionality which can be an application or service. * For example – If we have a web application which we want to host then it can be called as “workload”. Similarly, if we want to host a database server - they it called as a workload |

## IMPORTANT USE CASES AND SOLUTIONS

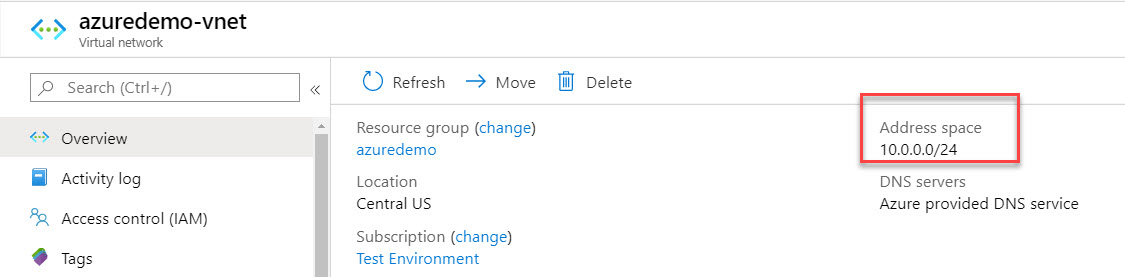


# AZURE VIRTUAL NETWORK

## CREATING A VIRTUAL NETWORK



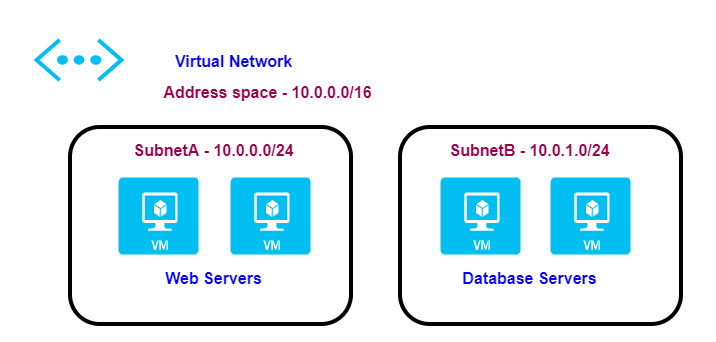
* The Azure Virtual Network service is used to define an isolated network in Azure. The virtual network can then be used to host the resources such as Azure virtual machines.
* The Azure virtual network gets assigned an address space (IP address range) which we can specify when we create an Azure virtual network.
* *Note: When we create a VM needs to be part of virtual network*
* Virtual network has something called IP address range / address space as shown below



## CREATING A SUBNET IN VIRTUAL NETWORK

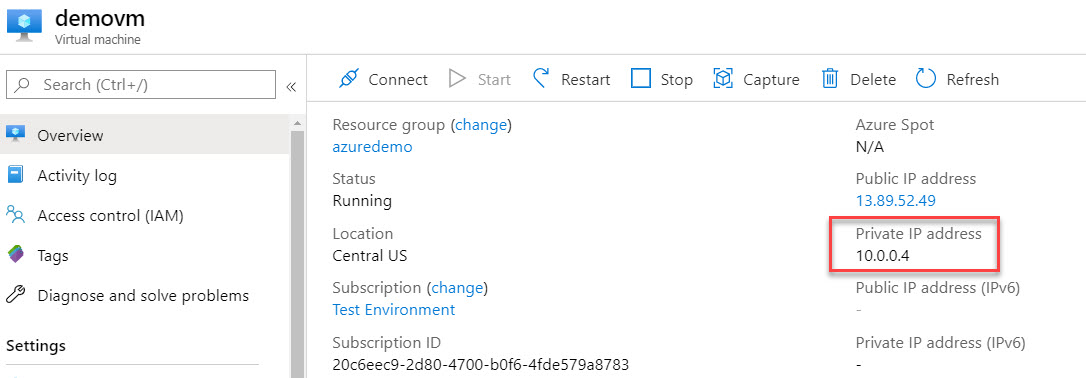
After creating a Virtual Network – We can then add subnets to the Azure virtual network. This helps divide the network into more logical segments.

An example is shown below of having multiple subnets. You could have one subnet named SubnetA in the virtual network to host your Web servers and another subnet to host the Database servers.



## CREATING A VIRTUAL MACHINE IN VIRTUAL NETWORK

* When we create a virtual machine in a virtual network, the virtual machine gets a Private IP address from the address space of the subnet is it launched in. The range of IPs of the Subnet is a subset of the Virtual network IPs.

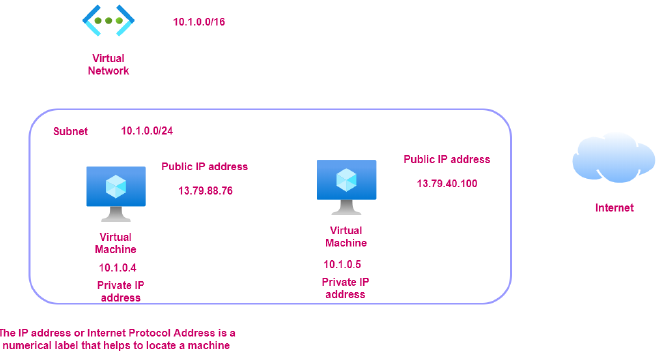


* Any VM created in virtual network gets a private and public IP address. If the private IP of VM lies within the range of Virtual network – then the VM is said to be part of that Virtual Network.
* The IP address is a numeric representation – to identify a machine – Similarly private IP address help in uniquely identifying a VM in a Virtual network.
* The public IP address is used to connect with VM from internet. (We cannot use private IP to access from internet)

*Questions*

1. *If I have pre-created VM (which belong to some another virtual network) can I change the Virtual network of the VM ? - No*
2. *Can a VM can be a part of two different Virtual Network? – No*

## COMMUNICATION ACROSS VIRTUAL MACHINES IN A VIRTUAL NETWORK

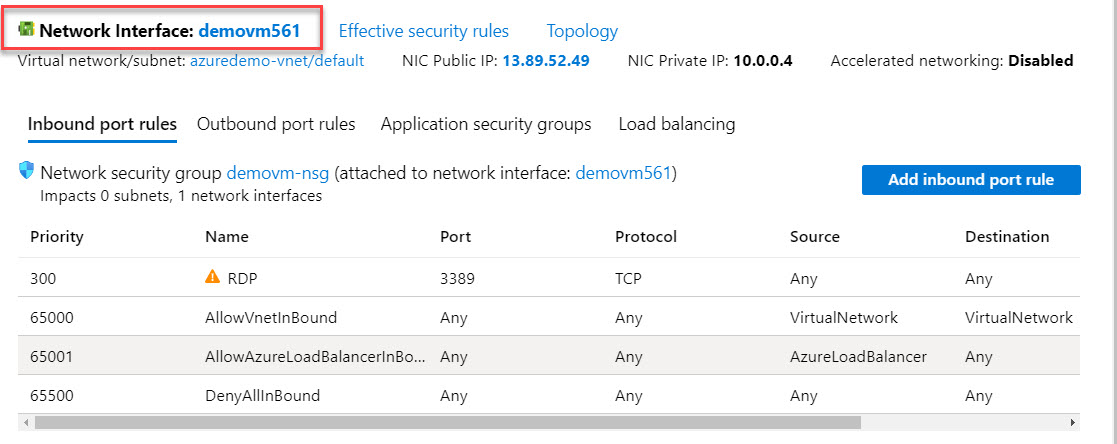


## NETWORK SECURITY GROUP

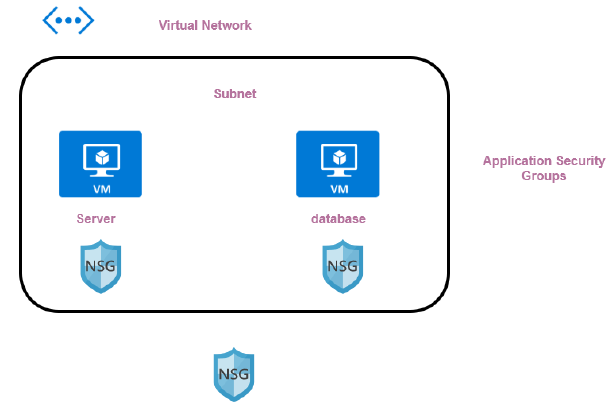
* ***Network security group is used to filter the in-bound and outbound traffic which is flowing to the VM.***



* All the data flows into VM go through the Virtual Network Device. Hence – when we access the VM using the public IP address. The traffic flow via Virtual Network interface.
* ***The Network security group ( which is attached to the Virtual Network Interface) - has set of rules which controls / filters the inbound and outbound traffic. Its like a basic firewall.***
* By default, all traffic into a virtual machine is DENIED.
* We have to explicitly add rules to allow traffic into a virtual machine
* There are also outbound rules to control the traffic flowing out of the virtual machine. By default, all traffic outbound onto the Internet is allowed.
* The inbound / outbound rules include the rules around protocol , port number , Source and Destination and Priority.



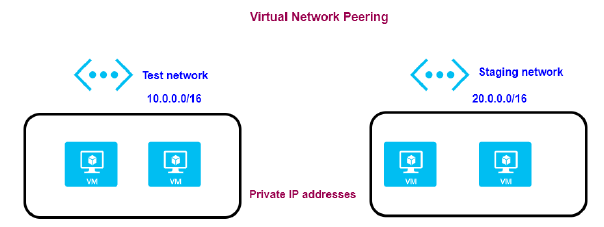
## APPLICATION SECURITY GROUP



## NETWORK CONNECTIVITY OPTIONS

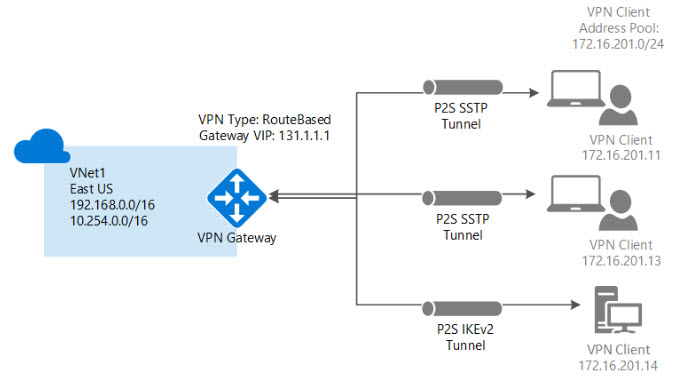
### **VIRTUAL NETWORK PEERING**

* Virtual Network Peering is used to connect two Azure virtual networks together via the backbone network.
* Azure supports connecting two virtual networks located in the same region or networks located across regions.
* Once we enable virtual network peering between two virtual networks, the virtual machines can then communicate via their private IP addresses across the peering connection.
* We can also peer virtual networks that are located across different subscriptions.
* The virtual networks can't have overlapping CIDR blocks.



### **POINT-TO-SITE VPN CONNECTION**

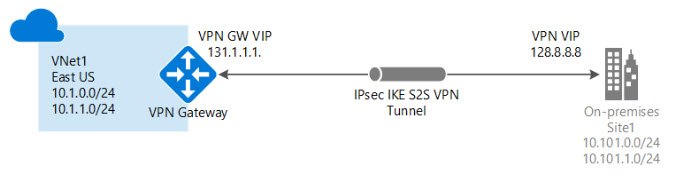
* A Point-to-Site VPN connection is used to establish a secure connection between multiple client machines and an Azure virtual network via the Internet.
* Below is a diagram from the Microsoft documentation on a sample scenario



* To implement a Point to Site VPN connection, you need to create a VPN Gateway in Azure.

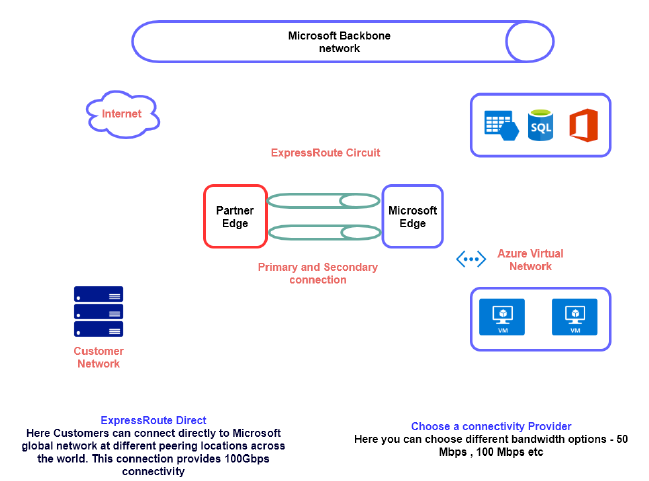
### **SITE-TO-SITE VPN CONNECTION**

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



* On the on-premise side, you need to have a VPN device that can route traffic via the Internet onto the VPN gateway in Azure. The VPN device can be a hardware device like a Cisco router or a software device ( e.g Windows Server 2016 running Routing and Remote services). The VPN device needs to have a publically routable IP address.
* The subnets in your on-premise network must not overlap with the subnets in your Azure virtual network
* The Site-to-Site VPN connection uses an IPSec tunnel to encrypt the traffic.
* The VPN gateway resource you create in Azure is used to route encrypted traffic between your on-premise data center and your Azure virtual network.

## AZURE EXPRESS ROUTE



# AZURE CORE SERVICES

## AZURE STORAGE

