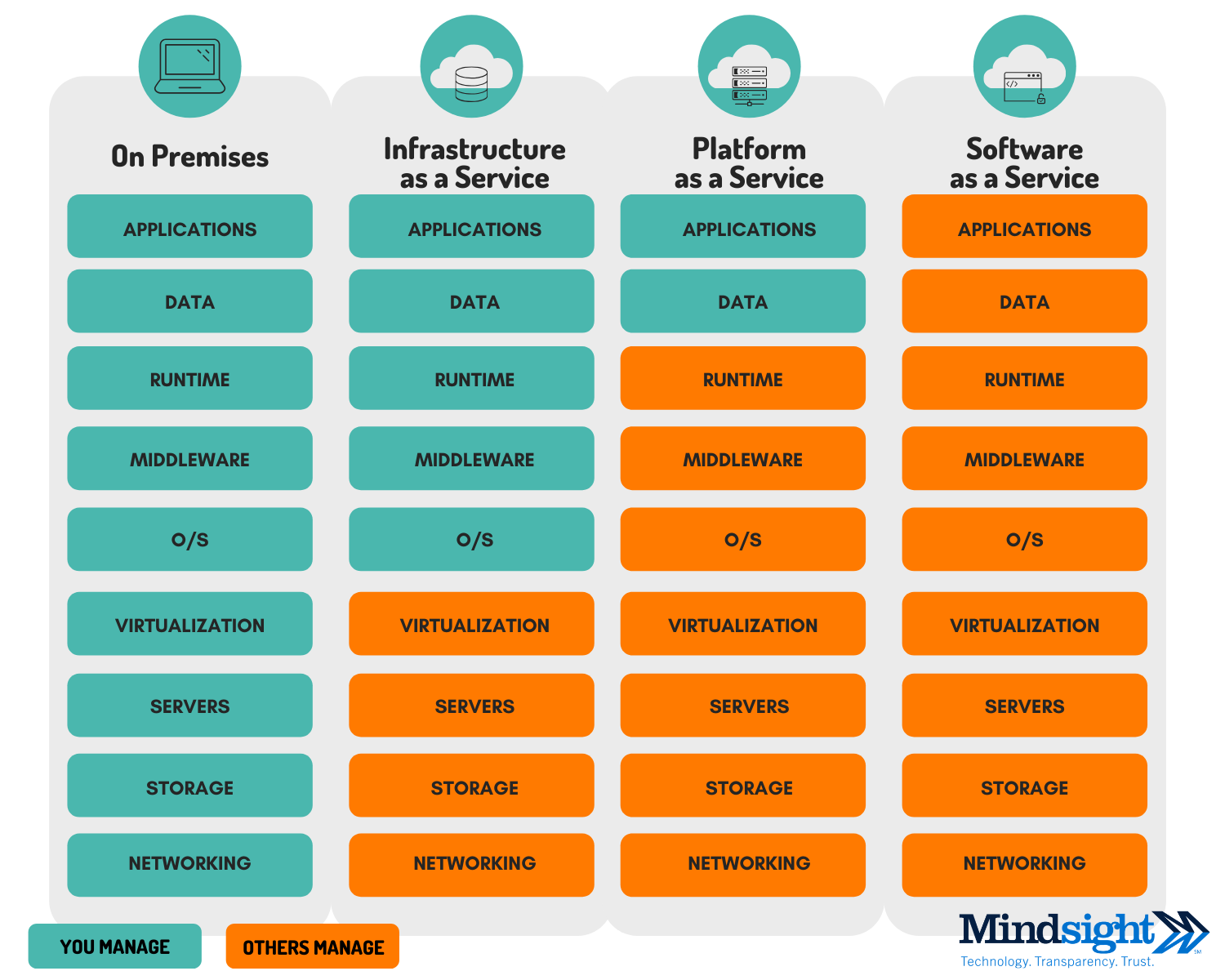
### What are the different types of services offered in the cloud?

* Saas
* Iass
* Pass

|  |  |
| --- | --- |
| SaaS Examples: | Google Apps, Microsoft office365, Google docs, Gmail, |
| PaaS Examples: | Windows Azure, Heroku, Force.com, Google App Engine, |
| IaaS Examples: | Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE) |



Top SAAS Services:

1) **SalesForce:** This is arguably the top-most accredited cloud-based CRM (customer relationship management) aimed to boost the sales of organizations by managing all the leads and prospects at one place

2) **Dropbox:** Dropbox offers amazing file storage solutions synced across all your devices and act as your cloud-based hard drive.

3) **Google Applications (G suite):** With the variety of SaaS applications offered by search engine vanguard. Now it is known as G suit, offering applications which need no introduction like Gmail, Google Docs, Google Sheets, Google Drive etc.

4) **Slack:** Slack is another prominent example of Software as a service application. This includes private messaging as well as group discussions with all types of file sharing options available backed by privacy protection and full end to end encryption security.

5) **SAP Concur:** Another American SaaS company which streamlines the traveling and expense management services into complete automation.

6) **Atlassian Jira:** Developed by Atlassian, Jira is a very useful SaaS application for developers and project managers who want to track and manage the workflow of software development projects.

### What is cloud computing?

It is the use of servers on the internet to “store”, “manage” and “process” data. The difference is, instead of using your own servers, you are using someone else’s servers to do your task, paying them for the amount of time you use it for.

And Companies offering these computing services are called cloud providers

### What are the different cloud deployment models?

**Explanation: Following are the three cloud deployment models:**

**Public Cloud: The infrastructure is owned by your cloud provider and the server that you are using could be a multi-tenant system.**

**Private Cloud: The infrastructure is owned by you or your cloud provider gives you that service exclusively. For eg: Hosting your website on your servers, or hosting your website with the cloud provider on a dedicated server.**

**Hybrid Cloud: When you use both Public Cloud, Private Cloud together, it is called Hybrid Cloud. For Example: Using your in-house servers for confidential data, and the public cloud for hosting your company’s public facing website. This type of setup would be a hybrid cloud.**

### Which service in Azure is used to manage resources in Azure?

1. **Application Insights**
2. **Azure Resource Manager**
3. **Azure Portal**
4. **Log Analytics**

**Answer: B Azure Resource Manager**

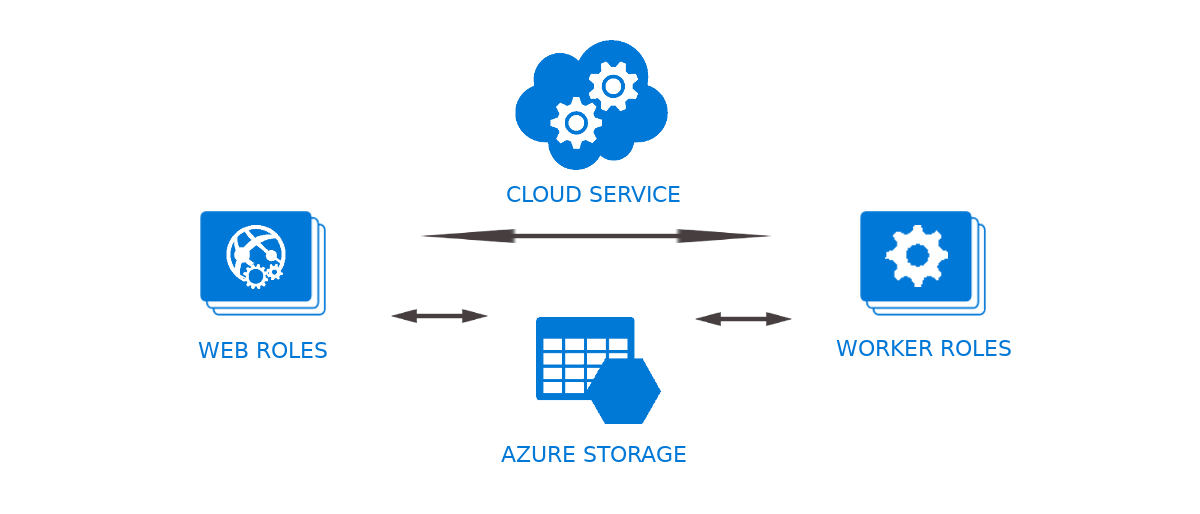
**Explanation: Azure Resource Manager is used to “manage” infrastructures which involve a no. of azure services. It can be used to deploy, manage and delete all the resources together using a simple JSON script.**

### What are Roles and why do we use them?

Roles are servers in layman terms. These servers are managed, load balanced, Platform as a Service virtual machines that work together to achieve a common goal.

There are 3 types of roles in Microsoft Azure:

* Web Role
* Worker Role
* VM Role



**Web Role** – A web role is basically used to deploy a website, using languages supported by the IIS platform like, PHP, .NET etc. It is configured and customized to run web applications.

**Worker Role** – A worker role is more like an help to the Web role, it used to execute background processes unlike the Web Role which is used to deploy the website.

**VM Role** – The VM role is used by a user to schedule tasks and other windows services. This role can be used to customize the machines on which the web and worker role is running.

### Is it possible to create a Virtual Machine using Azure Resource Manager in a Virtual Network that was created using classic deployment?

**Explanation**: This is not supported. You cannot use Azure Resource Manager to deploy a virtual machine into a virtual network that was created using classic deployment.

### What are virtual machine scale sets in Azure?

**Explanation**: This service allows you to create, deploy and manage a group of identical VMs.

The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. Scale sets provide high availability to your applications, and allow you to centrally manage, configure, and update a large number of VMs

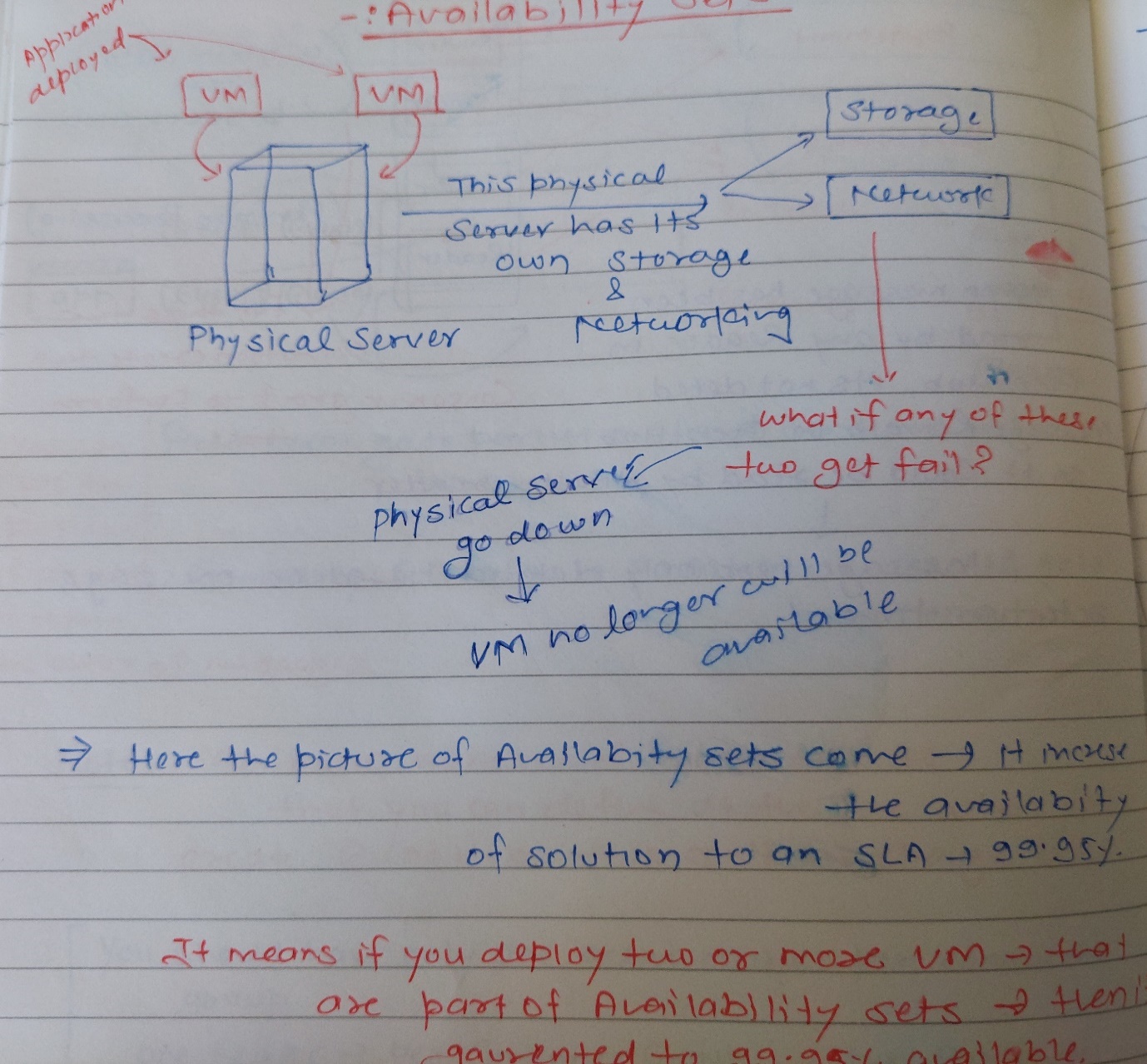
* You can also place the scale sets behind a load balancer to distribute the traffic across the VM
* Easy to create and manage multiple VMs
* Provides high availability and application resiliency
* Allows your application to automatically scale as resource demand changes
* Works at large-scale

### Are data disks supported within scale sets?

**Explanation**: Yes. A scale set can define an attached data disk configuration that applies to all VMs in the set. Other options for storing data include:

* Azure files (SMB shared drives)
* OS drive
* Temp drive (local, not backed by Azure Storage)
* Azure data service (for example, Azure tables, Azure blobs)
* External data service (for example, remote database)

### What is an Availability Set?



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

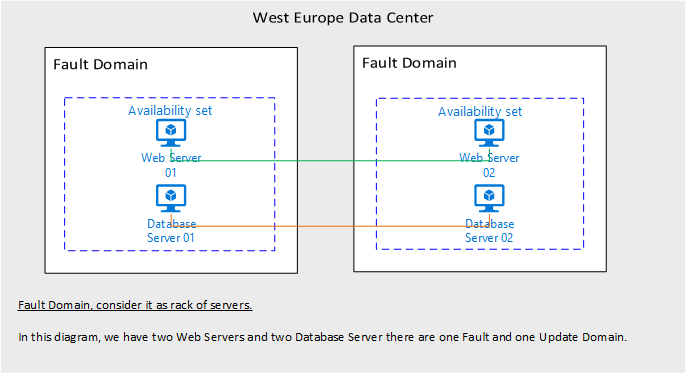
Availability sets contains Fault Domain & Update domain. So In Availability Sets -> VM’s spread across fault domain and update domain itself and managed properly.

Note: At a time of VM creation -> you can only set this VM to be part of Availability Sets.

### What are Fault Domains?

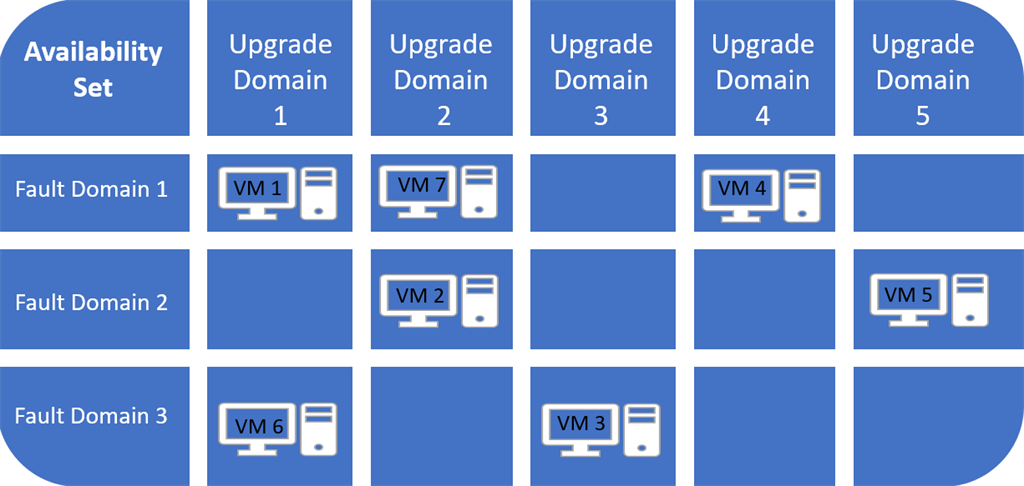
Fault domain is kind of separate physical server, which contains its own power and networking. If fault domain 1 go down -> then fault domain 2 exist.

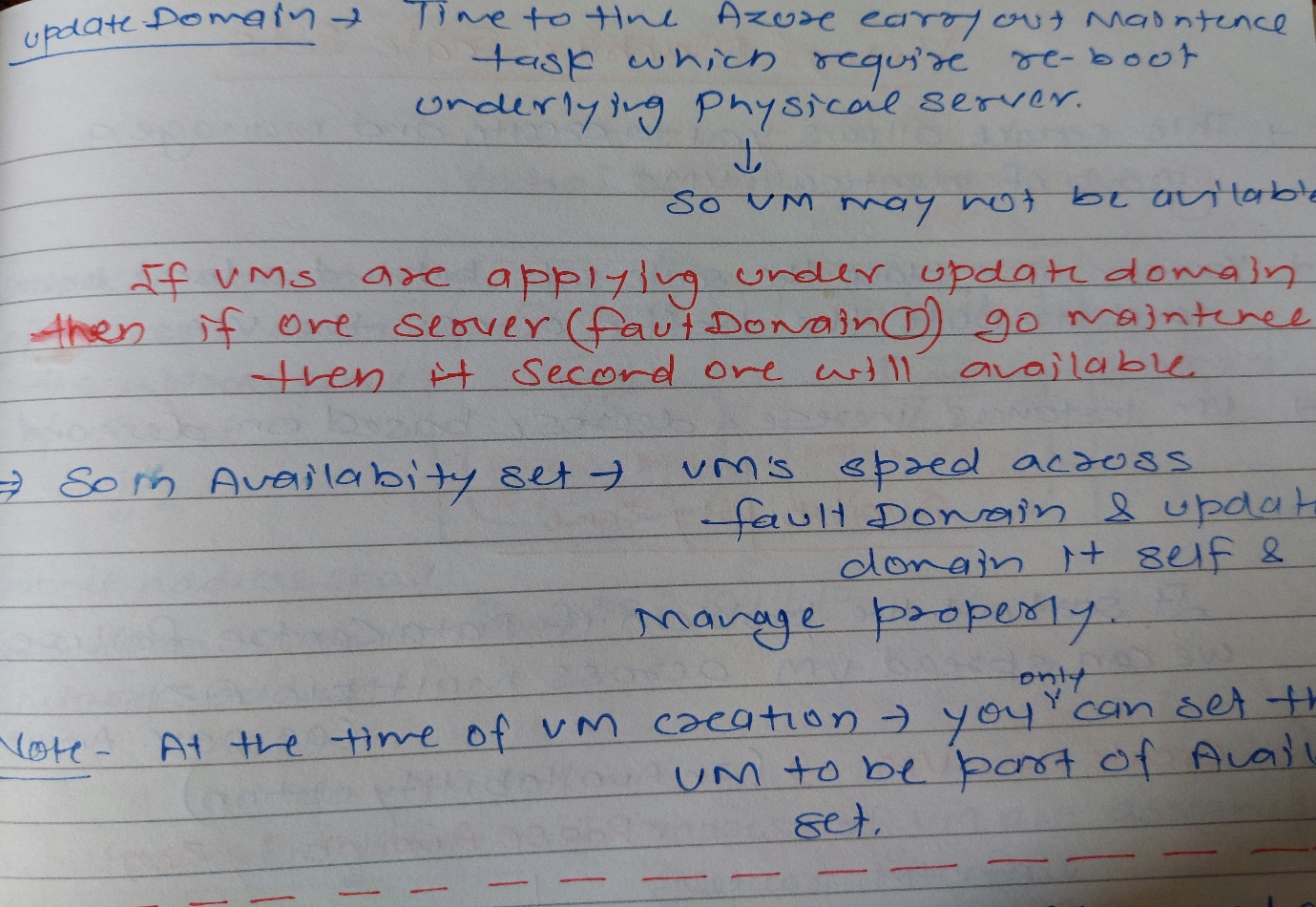
A fault domain is a logical group of underlying hardware that share a common power source and network switch, similar to a rack within an on-premise data-centers. As you create VMs within an availability set, the Azure platform automatically distributes your VMs across these fault domains. This approach limits the impact of potential physical hardware failures, network outages, or power interruptions.



### What are Update Domains?

An update domain is a logical group of underlying hardware that can undergo maintenance or can be rebooted at the same time. As you create VMs within an availability set, the Azure platform automatically distributes your VMs across these update domains. This approach ensures that at least one instance of your application always remains running as the Azure platform undergoes periodic maintenance. The order of update domains being rebooted may not proceed sequentially during planned maintenance, but only one update domain is rebooted at a time.





### Do scale sets work with Azure availability sets?

Yes. A scale set is an implicit availability set with 5 fault domains and 5 update domains.

We can use scale sets when the workload on your solution changes a lot or is unpredictable. For example, if you have a solution that normally works using only one VM, but may need up to 5 VMs to work under heavy demand, you would use a scale set to ensure that your solution quickly scales to demand. Scale sets pre-provision your VM instances so that when they need to scale out, it’s just a matter of starting them, rather than having to wait for Azure to actually create the VMs.

### What are best practices for Azure Autoscale?

* Ensure the maximum and minimum values are different and have an adequate margin between them 🡪 If you have a setting that has minimum=2, maximum=2 and the current instance count is 2, no scale action can occur.

### Manual scaling is reset by autoscale min and max -> If you set the range between 3 and 6. If you have one running instance, the autoscale engine scales to three instances on its next run. Likewise, if you manually set the scale to eight instances, on the next run autoscale will scale it back to six instances on its next run. Manual scaling is temporary unless you reset the autoscale rules as well.

### Always use a scale-out and scale-in rule combination that performs an increase and decrease

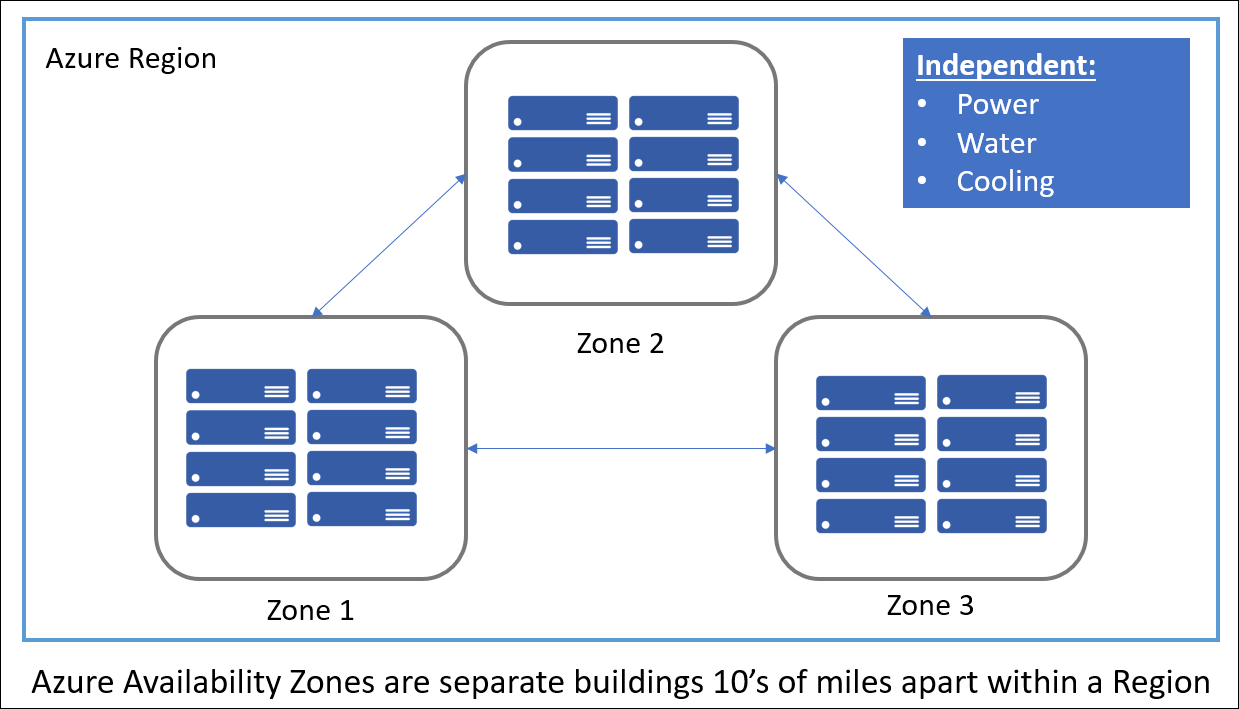
### Choose the thresholds carefully for all metric types. We recommend choosing an adequate margin between the scale-out and in thresholds. As an example, consider the following better rule combination.

Increase instances by 1 count when CPU% >= 80

Decrease instances by 1 count when CPU% <= 60

### Availability Zone?

In sort out the problem if data centre failure -> we can spread VM cross multiple availability zone (99.99% availability)



Unique physical locations within a region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking.

So if you have an application deployed to multiple VMs 🡪 it is good to deploy the VMs to multiple availability zone.

Create new VM -> (In Availability options) Choose Availability Zone 🡪 Select Zone ( From 1, 2, 3) -> Select Zone 1 (It means VM will be launch to data centre belong to Zone 1

Create a Scale Set 🡪 (In Availability options) Choose multiple zone 1,2,3 🡪 Instance count set =3 🡪 Create (These Instance will be on Zone 1,2,3)

### Can we add existing VM to scale set?

You can attach data disks to scale sets.

### How do I connect to a VM scale set?

You can connect to a virtual machine scale set instance directly from the Azure portal using Azure Bastion. Make sure that you have set up an Azure Bastion host for the virtual network in which the virtual machine scale set resides.

* Open the Azure portal. Navigate to the virtual machine scale set that you want to connect to.
* Navigate to the virtual machine scale set instance that you want to connect to, then select Connect.
* After you select Connect, a side bar appears that has three tabs – RDP, SSH, and Bastion. Select the Bastion tab from the side bar.
* On the Bastion tab, enter the username and password for your virtual machine scale set, then select Connect.



### How do I connect to a VM?

**Inbound Security Rules:**

Resource Group --> Go to your Network Security Group --> Inbound Security rules --> Add rules

* When you create a VM, it allocated a port. In order to do RDP -> you have to add port into inbound security rule.
* When you install IIS on VM, and want to excess port 80 outside the VM using IP --> for this you have to add inbound rules for port 80 --> Add HTTP Access

**The big thing about developers and virtual machines is how do you work with a virtual machine?**

So let's say, you have got a Azure environment and you're coding and you want to get your code from your workstation onto an Azure environment.

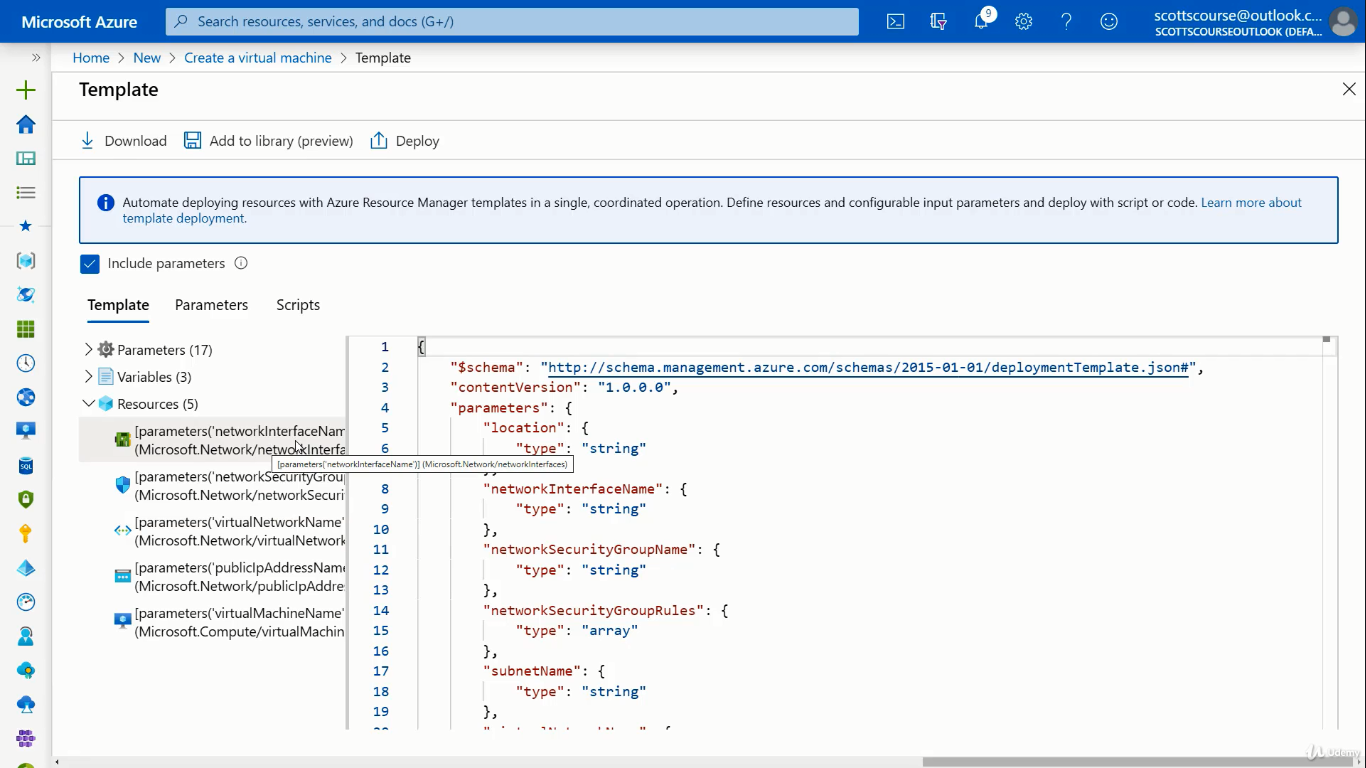
* The recommended approach is something called Azure DevOps.
* There's another technology called web apps that is a lot more developer-friendly in terms of having integrations between your visual studio and the Cloud.

A virtual machine doesn't have that kind of integrations but DevOps is the glue for that.

### How to Deploy ARM Templates

So if you need to deploy ARM templates from your local machine (or cloud shell), I've uploaded the scripts here for you to download and use. <https://github.com/gottagetgit/ARMDeploy>

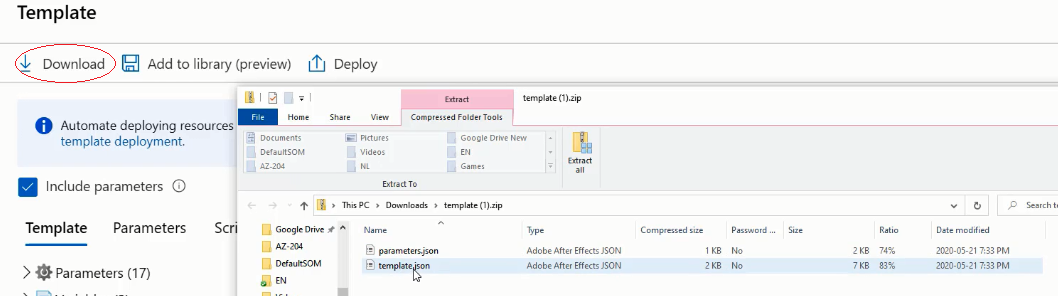
ARM or the Azure Resource Manager model is the underlying model of how resources are managed within Azure.



The template contains all five resources

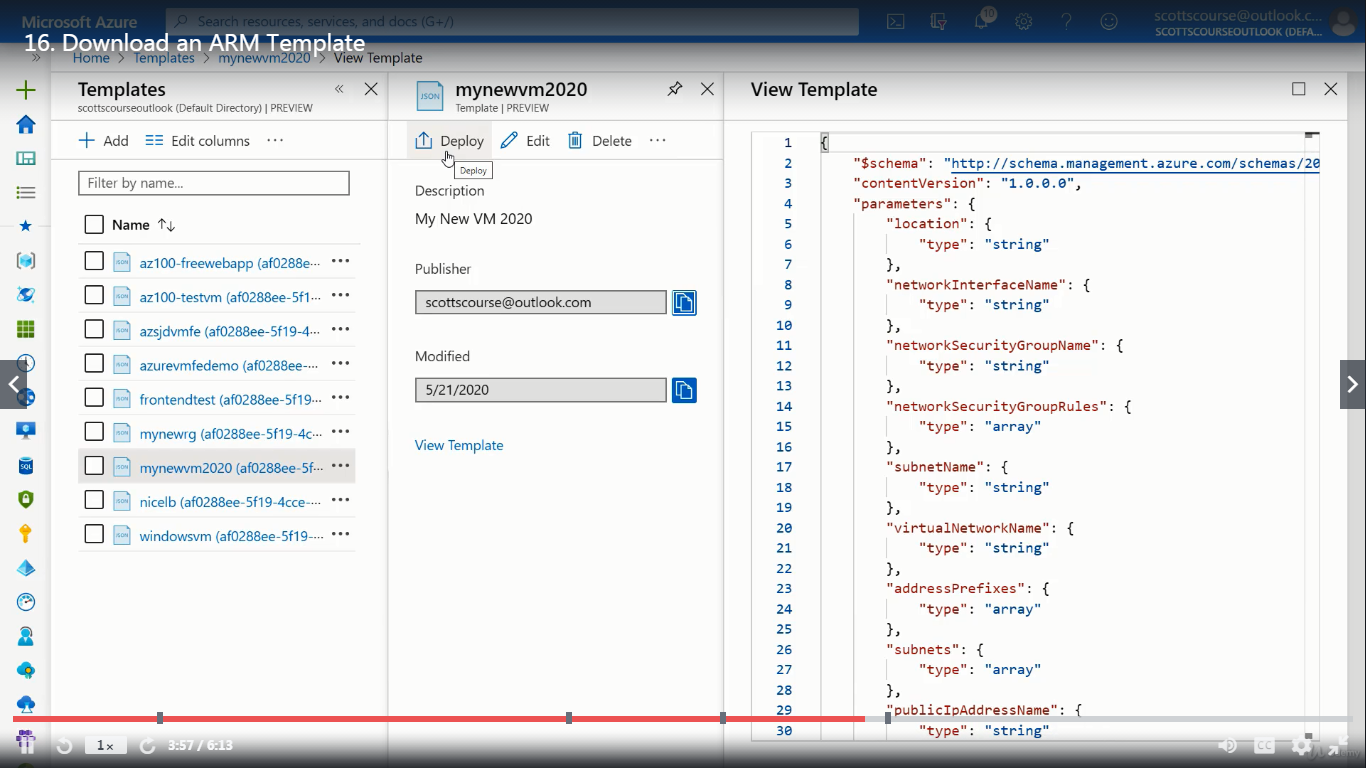
* virtual machine
* public IP address
* virtual network
* security group,
* Network interface card.

Download the template --> will download two files --> template and the parameters file.



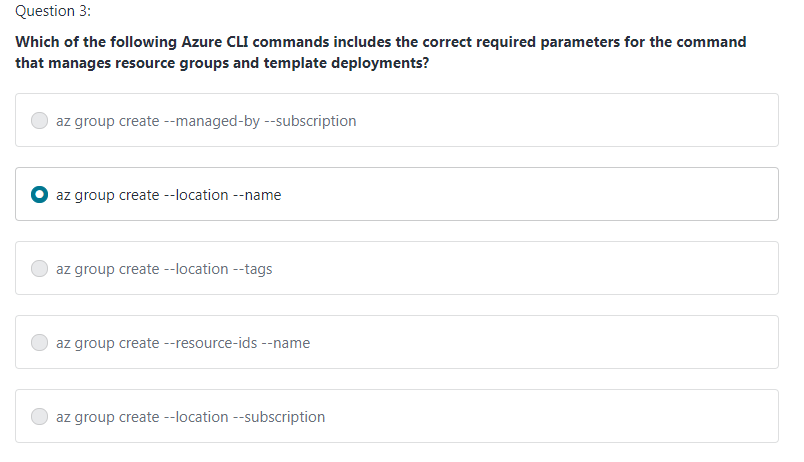
Or you can add to the library, from where you can deploy the template --> remember you need to change the parameters in parameter file.

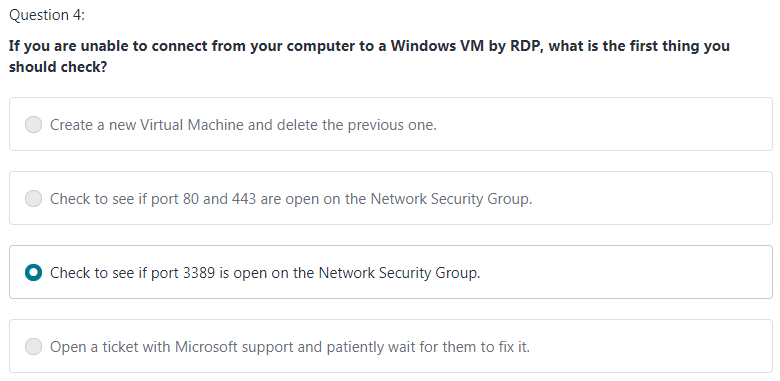
Now search templates and deploy template and create new VM as much you want



When you deploy --> it will not load the parameters --> you need to load parameter you have downloaded --> and then edit the values

When you load the parameter file, it not loaded Resource group and Admin Password of VM.

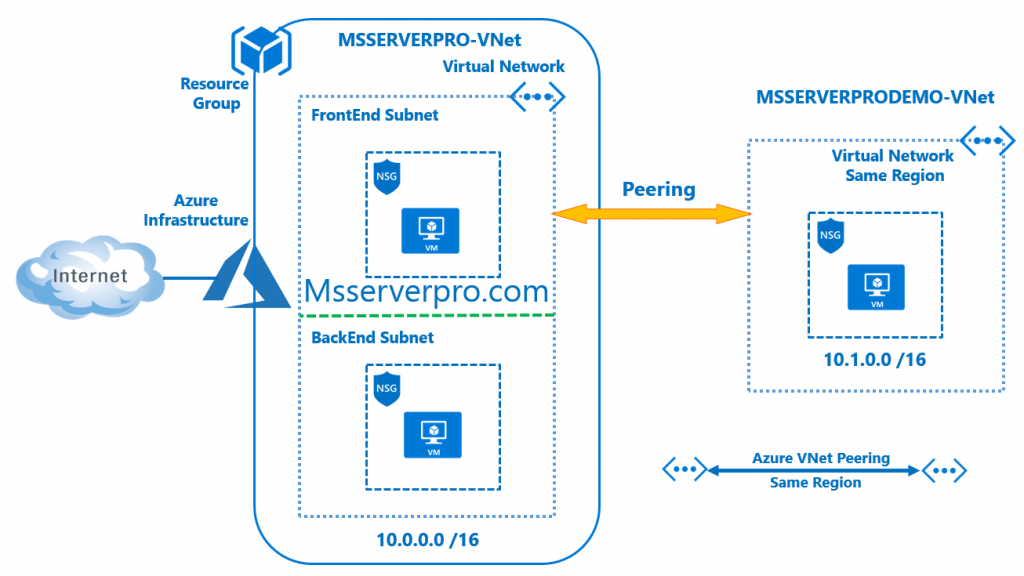
****

****

### What is Azure Virtual Network?

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks.

* Private IP address of VM depends on the address space of Subnet.
* Subnet address space depends on Virtual Network Space



Network Interface: IP address of VM are assigned to Network Interface. Two type of Network Interface.

* Private

1. Private IP used to internal communication between VMs in a virtual network Or across Virtual Network if you did the peering.
2. In private IP address traffic is flowing within in Azure Network not on Internet

* Public

1. If you want resources on the internet reach to your VM -> then you need to assign a public IP address to your network interface on your VM.
2. Public IP has nothing to do with your Subnet address space or Virtual Network address space. It comes from Pool of Azure
3. You can create multiple IP range in Virtual Network, for all IP range you can set subnet address

10.0.0.0/16

20.0.0.0/16

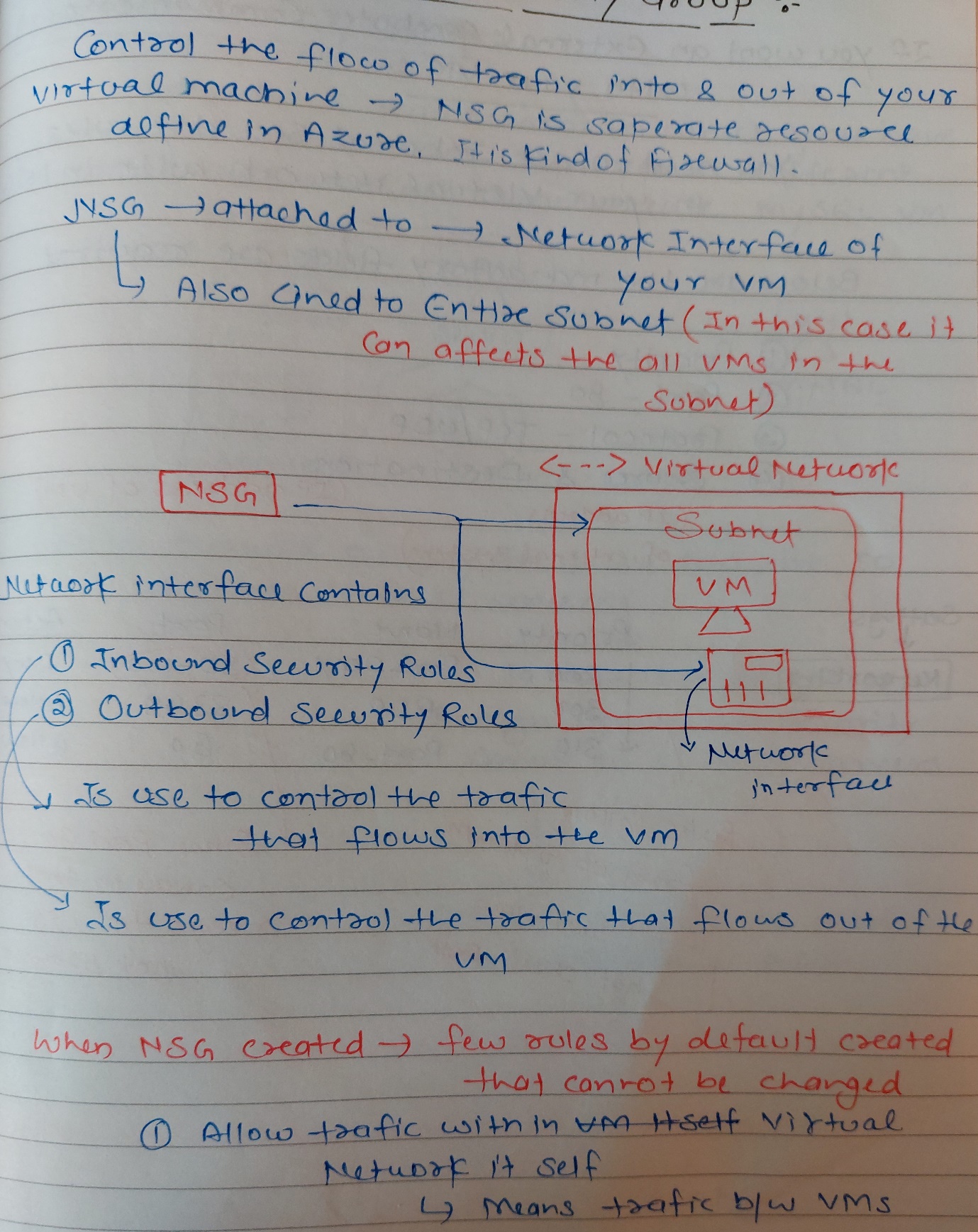
Create a Virtual Network 🡪 Define Subnet 🡪 Now go & create VM 🡪 In Networking Tab select Virtual Network & Subnet

### What are Network Security Groups?

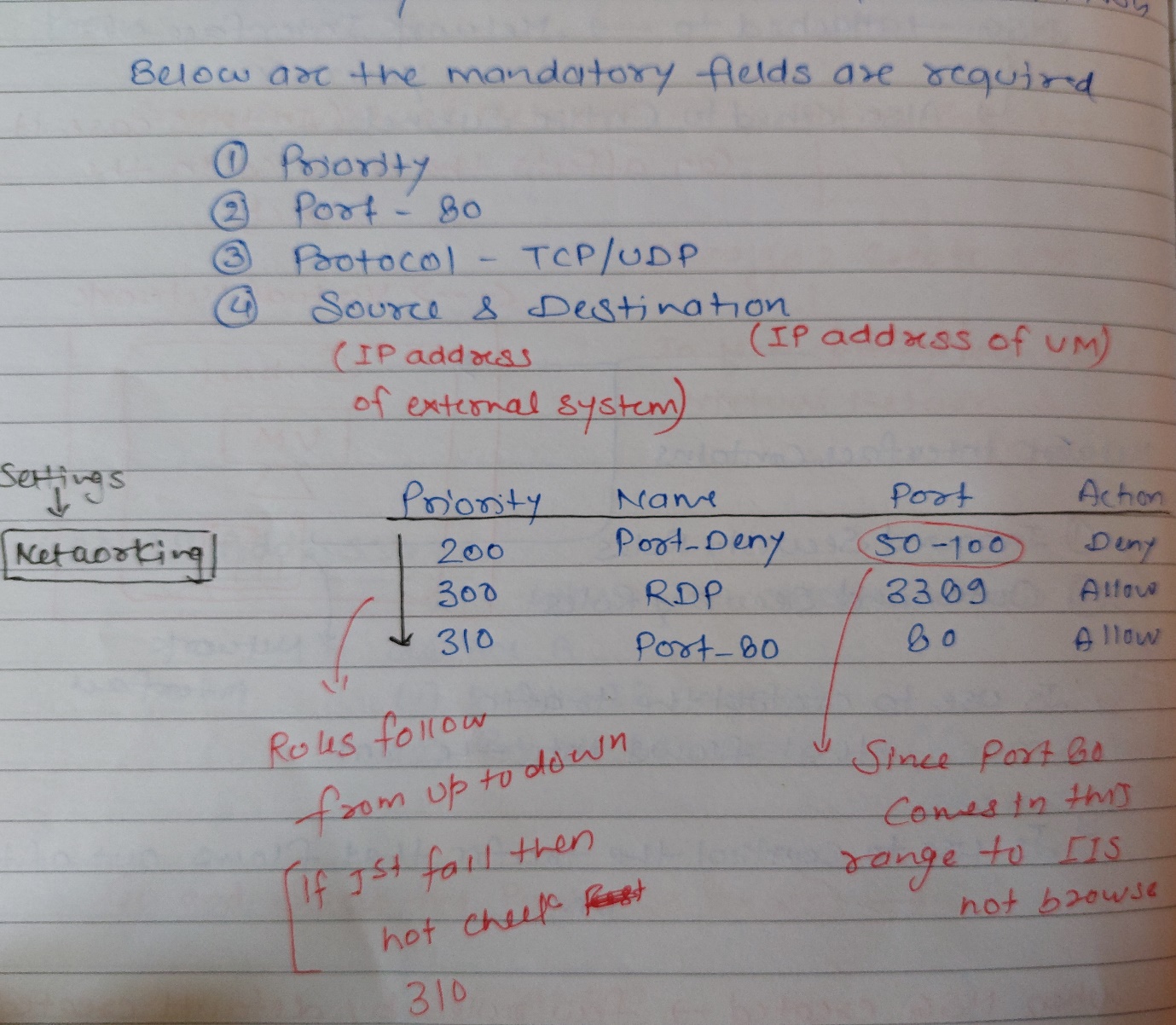
A network security group (NSG) control the flow of traffic into & out of your Virtual Machine. NSG is a separate resource defined in Azure. It’s kind of firewall.

A network security group (NSG) contains a list of Access Control List (ACL) rules that allow or deny network traffic to subnets, Network Interface, or both. NSGs can be associated with either subnets or individual NICs connected to a subnet.

When an NSG is associated with a subnet, the ACL rules apply to all the VMs in that subnet. In addition, traffic to an individual NIC can be restricted by associating an NSG directly to a NIC.



If you want an External Computer Communicate with your VM 🡪 You need to set Inbound security rules in your virtual network with in NSG. Below are the mandatory fields are required when setting up inbound rules.





### Application Security Group?



### What is a break-fix issue?

Explanation: Technical problems are called break-fix issue, it is an industry term which refers to “work involved in supporting a technology when it fails in the normal course of its function, which requires intervention by a support organization to be restored to working order”

### Why is Azure Active Directory used?

Explanation: Azure Active Directory is an Identity and Access Management system. It is used to grant access to your employees to specific products and services in your network. For example: Salesforce.com, twitter etc. Azure AD has some in-built support for applications in its gallery which can be added directly.

### Virtual Network Peering?

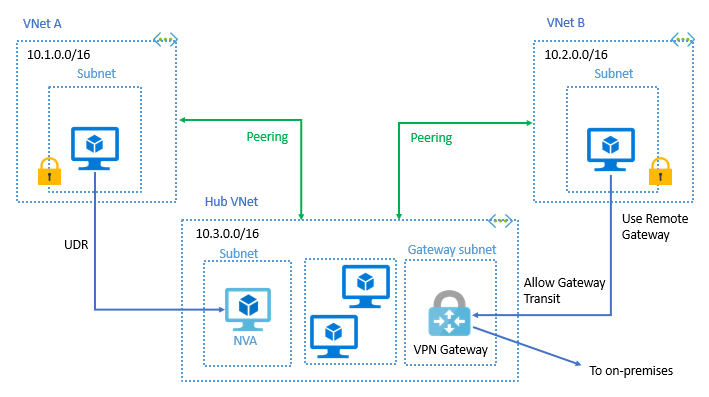
Virtual network peering enables you to seamlessly connect two or more Virtual Networks in Azure.

Peering needs to be setup between two virtual networks -> Important is that by this peering traffic between VMs doesn’t go on internet. Its via Azure backbone network.

* You can connect virtual networks in the same region or across the region.
* You can also connect VNs across different Subscription.
* Ensure that IP address do not conflict.

Azure supports the following types of peering:

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



Go to Virtual Network 🡪 Select any one Virtual Network (Select Staging Network)

Scroll down and select Peering

Add Peering

( Select & choose Network -> Test Network -> Define peering name for both -> Add peering connection from both side) by doing this peering from second virtual Network also get created.

Now you can browse IIS apps using private IP from both VM

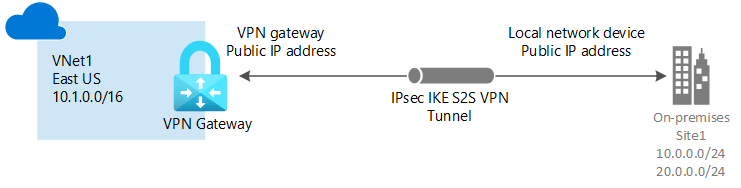
### Difference between azure site-to-site (s2s) and point-to-site (p2s) connections and Express Route?

Point to Site:

* A Point-to-Site (P2S) VPN gateway connection lets you create a secure connection to your virtual network from an individual client computer.
* This solution is useful for who want to connect to Azure VNets from a remote location, such as from home or a conference. P2S VPN is also a useful solution to use when you have only a few clients that need to connect to a VNet.
* In P2S workstation can connect VN via private IP address.
* P2S connections do not require an on-premises public-facing IP address or a VPN device.
* Usually, if you log-off or restart the workstation it loses connection, and you have to reconnect every time. Your computer will be authenticated to the VPN using certificates.

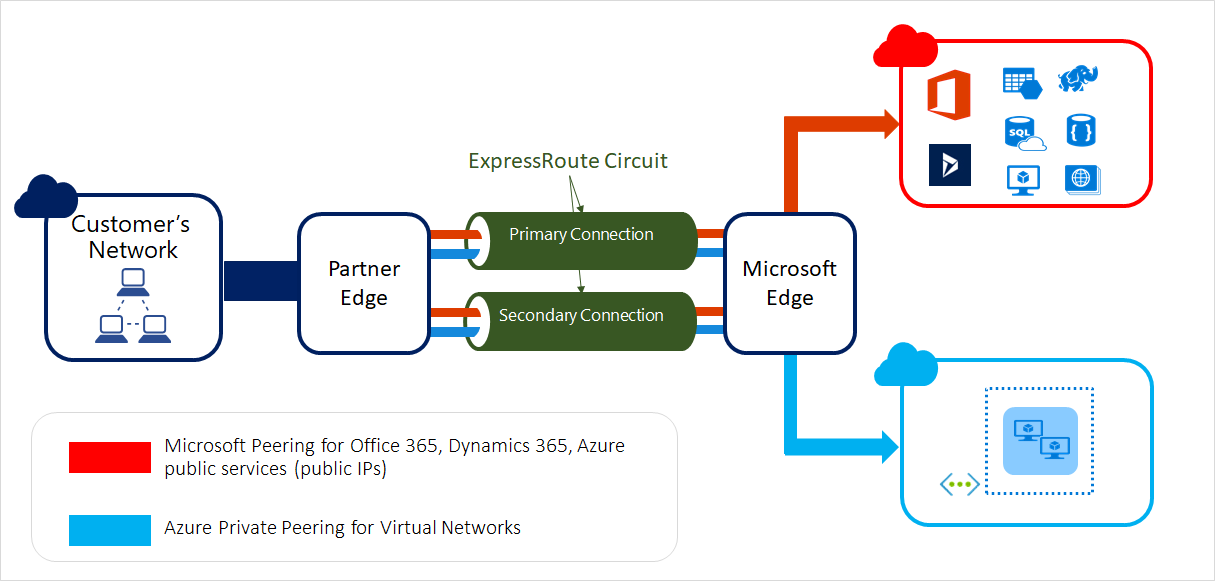
Site to Site

* A Site-to-Site VPN tunnel is great for when you need a persistent connection from many on-prem devices and computers to your Azure network. This is an ideal option for creating hybrid cloud solutions where you need to be able to connect to your Azure resources seamlessly. (Example, your application needs to get data from the customer database automatically with or without someone logged in the VM, then site-to-site is a better approach.)
* Site-to-Site VPN communication is done vis private IP and traffic travels encrypted over the public 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.

Express Route



ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection. ExpressRoute connections don’t go over the public Internet, and they offer more reliability, faster speeds and lower latencies than typical Internet connections.

With ExpressRoute, establish connections to Azure at an ExpressRoute location, such as an Exchange provider facility, or directly connect to Azure from your existing WAN network, such as a multiprotocol label switching (MPLS) VPN, provided by a network service provider.

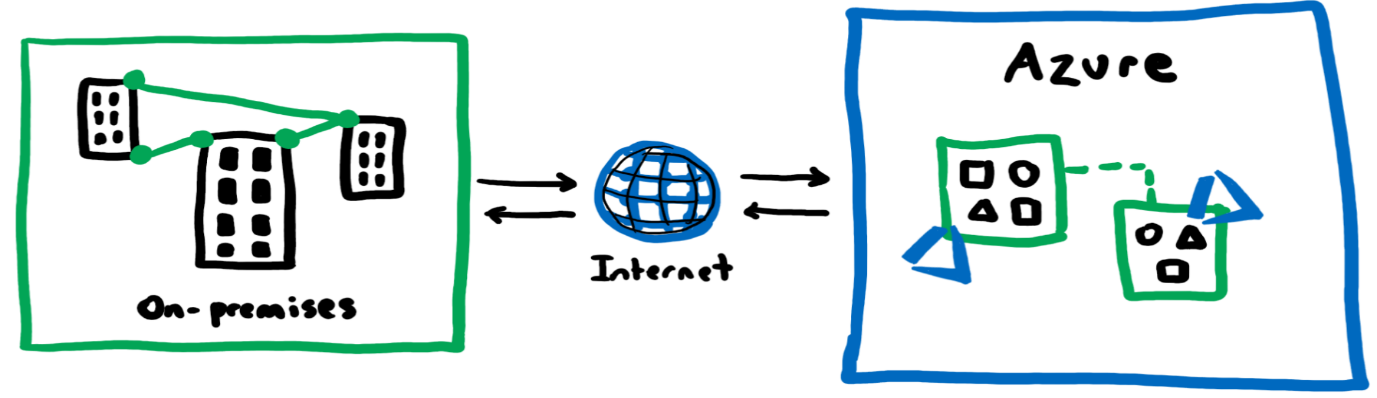
**Key benefits:**

* Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.
* Connectivity to Microsoft cloud services across all regions in the geopolitical region.
* Global connectivity to Microsoft services across all regions with the ExpressRoute premium add-on.
* Dynamic routing between your network and Microsoft via BGP.
* Built-in redundancy in every peering location for higher reliability.
* Connection uptime SLA.
* QoS support for Skype for Business.

### Question: whether one should pick **VPN Gateway** or **ExpressRoute** to connect to Azure.

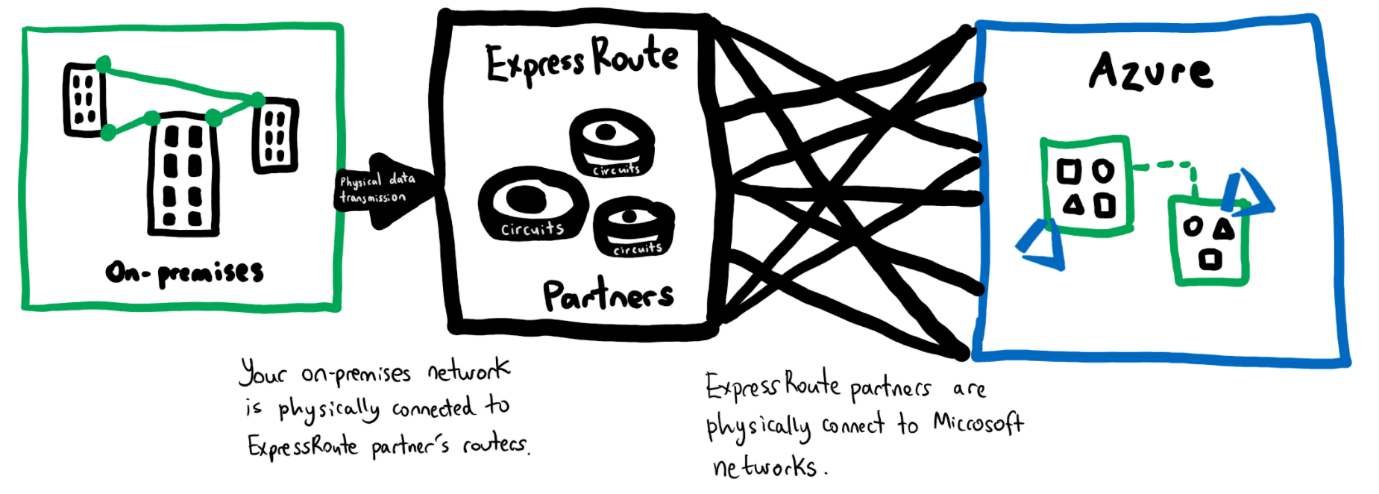
**Azure VPN Gateway:** Azure VPN Gateway allows you to connect your on-premises network to Azure networks to send encrypted traffic over an insecure channel. Let's say you have bunch of servers on-premises (which are just machines in some organization or some datacentre) and you want some of those machines to be able to connect and communicate with a bunch of Azure services (cloud services). This is an example of site-to-site connection. We have one site (on-premises) connecting to another site (Azure).

To enable site-to-site connection (S2S), we need to install a VPN device into one of the on-premises network. This VPN device allows you to connect to a VPN Gateway which you have to put into your Azure virtual network (VNET).



**Azure Bastion** : which allows you to privately access your Azure VMs through the Azure portal so as long as you can securely access the Azure portal and identify yourself, you can access Bastion which you can think of as an agent that lives inside your Azure virtual networks that can then access your Azure virtual machines on your behalf.

**Azure ExpressRoute :** Express route says allows us to physically connect our on-premises networks into Azure.



**But why would we want to do that** - Well, we don't want our traffic going over the internet anymore. And besides, we have been experiencing latency with more members joining the team and we keep getting internet outages, it's just a nightmare.

All traffic is now traversed over your own organization's networks and the Microsoft Azure networks which means even if the public internet crashes, it will not affect your traffic flow.

**What happens when my ExpressRoute circuit goes down? -** you would have two ExpressRoute circuits set up, one as a primary link and one as a secondary or backup link. For disaster recovery, you can set up one circuit in one region and another circuit in another region so even if the entire region (or city) goes down, your connection to Azure is not broken.

ExpressRoute Global Reach connects ExpressRoute circuits together which means if we connected our main office to an ExpressRoute circuit and our new office to another ExpressRoute circuit then link those two ExpressRoute circuits together, we will be able to do all our office communication privately over the Microsoft network.

the traffic that traverses over ExpressRoute is not encrypted but you can encrypt the traffic over ExpressRoute if you really want to with IPSec and Azure Virtual WAN.

**So, should we pick Azure VPN Gateway or Azure ExpressRoute to connect to Azure?**

And the answer is, that depends on your business requirements. VPN gateway is typically cheaper than ExpressRoute and whilst you get the anonymity and security of encryption with VPN gateway, you are still traversing over a publicly exposed and insecure channel and are dependent on internet providers for network consistency. With ExpressRoute, your traffic is not encrypted but it is private and you would experience lower latency than with VPN Gateway (think of ExpressRoute like plugging your device straight into the Ethernet port for faster internet speed vs. VPN Gateway relying on the wireless connection or WiFi) however this comes at a cost as you need to pay for hardware that is specifically dedicated to you.