**121**

**subscription** is an agreement between an organization and Microsoft to use resources, for which charges are either paid on a per-license basis or a cloud-based

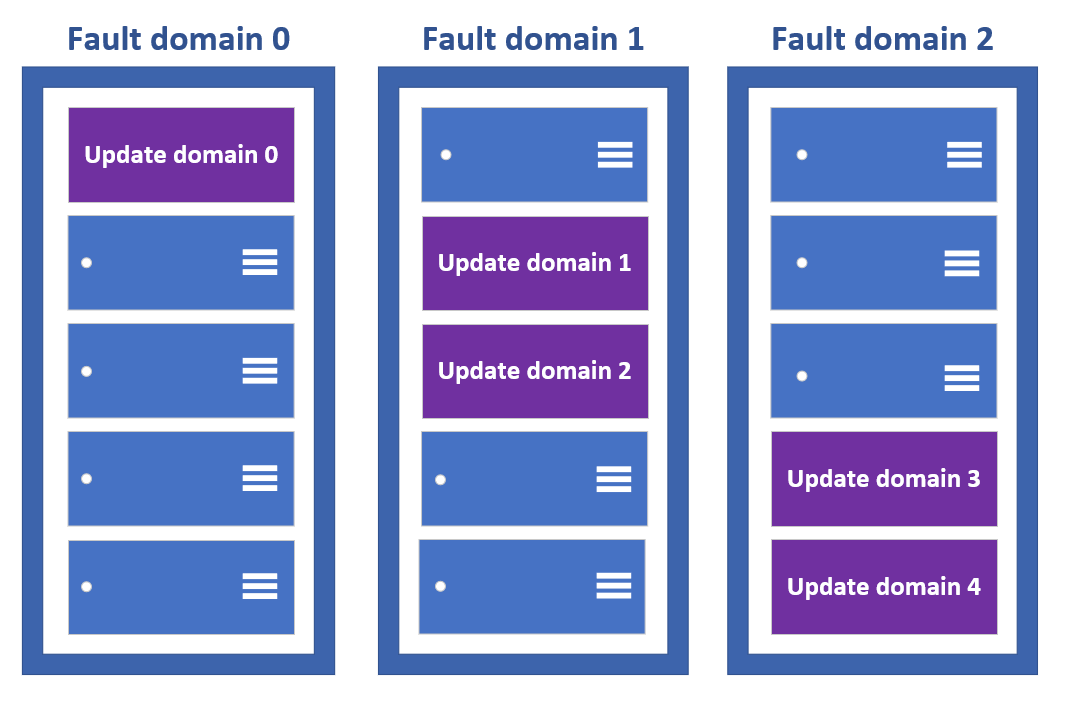
**Availability set**

An availability set is a logical grouping of VMs that allows Azure to understand how your application is built to provide for redundancy and availability. We recommended that two or more VMs are created within an availability set to provide for a highly available application and to meet the [99.95% Azure SLA](https://azure.microsoft.com/support/legal/sla/virtual-machines/).

Each availability set can be configured with up to three fault domains and twenty update domains

**Update domains** indicate groups of virtual machines and underlying physical hardware that can be rebooted at the same time.

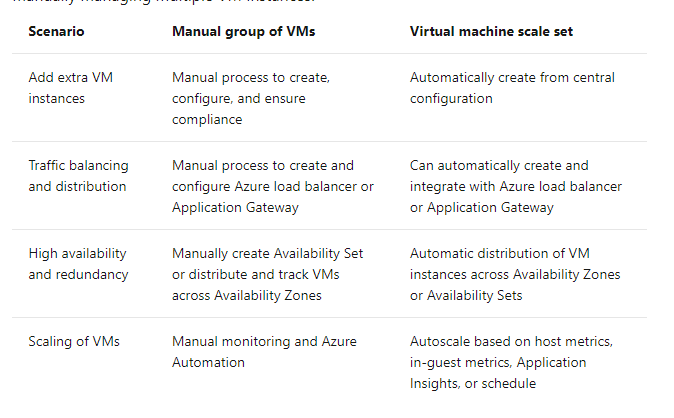
**Fault domains** define the group of virtual machines that share a common power source and network switch. By default, the virtual machines configured within your availability set are separated across up to three fault domains



* So to delete the availability set, you can first delete the virtual machines linked to the availability set and then go ahead and delete the availability set

**Virtual machine scale sets**

Azure virtual machine scale sets provide the management capabilities for applications that run across many VMs, [automatic scaling of resources](https://docs.microsoft.com/en-us/azure/virtual-machine-scale-sets/virtual-machine-scale-sets-autoscale-overview), and load balancing of traffic.



**Availability Zones**

* This features help provides better availability for your application by protecting them from datacentre failures.
* Each Availability zone is a unique physical location in an Azure region.
* Each zone comprises of one or more data centres that has independent power, cooling, and networking
* Hence the physical separation of the Availability Zones helps protect applications against data centre failures
* 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.

**Azure Key Vault**

Azure Key Vault is a cloud service for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, certificates, or cryptographic keys.

**Container** is a standard unit of software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another.

**Docker** container image is a lightweight, standalone, executable package of software that includes everything needed to run an application: code, runtime, system tools, system libraries and settings.

**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. VNet is similar to a traditional network that you'd operate in your own data centre, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

**Public IP addresses** allow Internet resources to communicate inbound to Azure resources.

In Azure Resource Manager, a [public IP](https://docs.microsoft.com/en-us/azure/virtual-network/ip-services/virtual-network-public-ip-address) address is a resource that has its own properties. Some of the resources you can associate a public IP address resource with:

* Virtual machine network interfaces
* Virtual machine scale sets
* Public Load Balancers
* Virtual Network Gateways (VPN/ER)
* NAT gateways
* Application Gateways
* Azure Firewall
* Bastion Host
* Route Serve

**Private IPs** allow communication between resources in Azure.

Resources can be:

* Azure Services such as:
  + Virtual machine network interfaces
  + Internal load balancers (ILBs)
  + Application gateways
* In a [virtual network](https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview).
* On-premises network through a VPN gateway or ExpressRoute circuit.

**ExpressRoute** lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider.

Private IPs allow communication to these resources without the use of a public IP address.

**Network ID and a Host ID**

An IP address consists of two components: a network ID and a host ID. The network ID identifies the network segment to which the host belongs. The host ID identifies an individual host on some specific network segment. A host can communicate directly only with other hosts on the same network segment. A network segment is a logical division of a network into unique numeric network IDs called subnets. A host must use a router to communicate with hosts on other subnets.

**Subnet mask** used to distinguish between network ID and host ID.

We get only 256 Total no.of hosts

Usable IP addresses is 254

EX: 192.0.2.0 is the network id and 192.0.2.255 is the broadcast ID .

CIDR Notation

192.0.2.0 Subnet Mask- 255.255.255.0 192.0.2.0/24

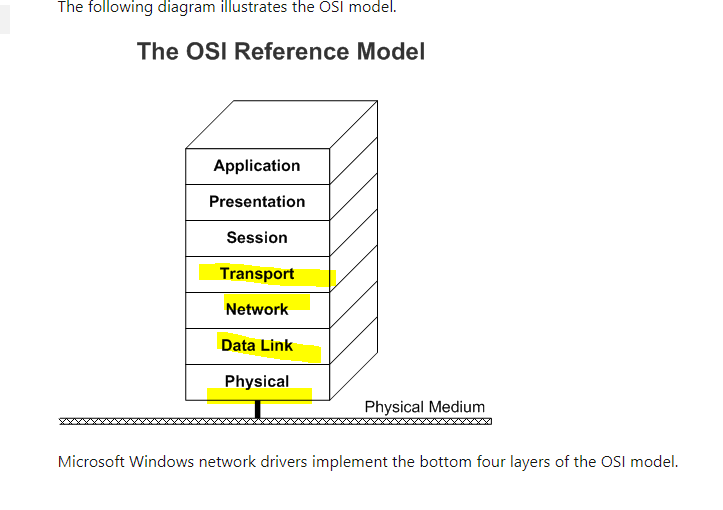
192.0.2.0 Subnet Mask- 255.255.0.0 192.0.2.0/16

**Network interface** enables an Azure Virtual Machine to communicate with internet, Azure, and on-premises resources. When creating a virtual machine using the Azure portal, the portal creates one network interface with default settings for you.

**Azure network security group** is used to filter network traffic to and from Azure resources in an Azure virtual network. A network security group contains [security rules](https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview#security-rules) that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.

* It is a type of firewall which controls in and out traffic of a vm.

**Azure Load Balancer** operates at layer 4 of the Open Systems Interconnection (OSI) model. It's the single point of contact for clients. Load balancer distributes inbound flows that arrive at the load balancer's front end to backend pool instances. These flows are according to configured load-balancing rules and health probes. The backend pool instances can be Azure Virtual Machines or instances in a virtual machine scale set.



Azure load balancer its just looks at ip address and port numbers and distributes the traffic.

A [**public load balancer**](https://docs.microsoft.com/en-us/azure/load-balancer/components#frontend-ip-configurations) can provide outbound connections for virtual machines (VMs) inside your virtual network. These connections are accomplished by translating their private IP addresses to public IP addresses. Public Load Balancers are used to load balance internet traffic to your VMs.

An [**internal (or private) load balancer**](https://docs.microsoft.com/en-us/azure/load-balancer/components#frontend-ip-configurations) is used where private IPs are needed at the frontend only. Internal load balancers are used to load balance traffic inside a virtual network. A load balancer frontend can be accessed from an on-premises network in a hybrid scenario.

**Health probe** that your load balancer can use to determine if your instance is healthy. If your instance fails its health probe enough times, it will stop receiving traffic until it starts passing health probes again.

**Load balancing rules**

A load balancer rule is used to define how incoming traffic is distributed to the all the instances within the backend pool

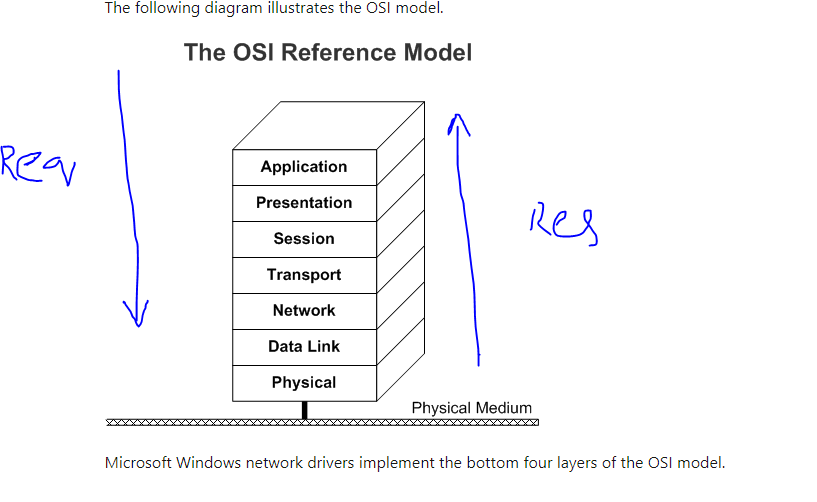
* **Web role**: Automatically deploys and hosts your app through IIS.
* **Worker role**: Does not use IIS, and runs your app standalone

**Application Gateway** can make routing decisions based on additional attributes of an HTTP request, for example URI path or host headers. For example, you can route traffic based on the incoming URL. So if /images is in the incoming URL, you can route traffic to a specific set of servers (known as a pool) configured for images. If /video is in the URL, that traffic is routed to another pool that's optimized for videos.

Our computer sends an request to an website, the request and response follows **OSI model**

At layer 7 (Application layer) we have properties OF HTTP requests and HTTP response

The requests first flow from physical layer up to application layer then Azure application gate way looks at application layer and route accordingly



**Physical layer**: In order to reach the destination the requests need to reach lot of wires.

**Network /transport layer:** This tells that when source system need s to talk with destination there would be a connection made between client IP address and destination IP address

**Application Layer:** web browser makes requestat application layer and all of the web request happened at via HTTP or HTTPS, these are application layer protocols

**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 you enable virtual network peering between two virtual networks, the virtual machines can then communicate via their private IP addresses across the peering connection.
* You 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 notes

**Notes on Point-to-Site VPN Connection**

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

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

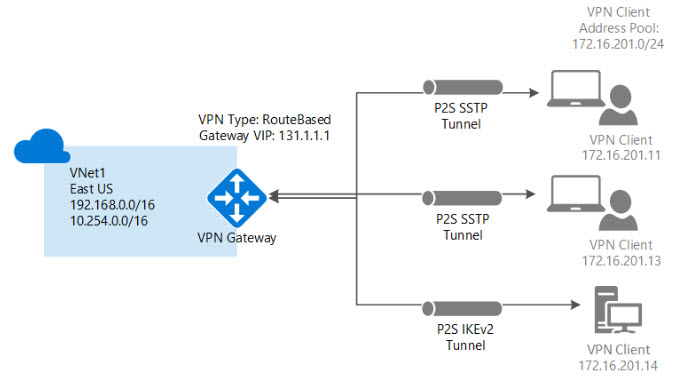


Image reference -<https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

* This sort of connection is based off certificates for authentication.
* You need to have a root certificate in place that needs to be uploaded to Azure for the point-to-site connection.
* A client certificate needs to be generated from the root certificate. This client certificate needs to be on each client computer that needs to connect to the Azure virtual network via the Point-to-Site connection.
* To generate the certificates, you can use a Certificate authority or generate a self-signed certificate using PowerShell. Some commands are given below

**// To generate the root certificate**

$cert = New-SelfSignedCertificate -Type Custom -KeySpec Signature `

-Subject "CN=RootCertificate" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" -KeyUsageProperty Sign -KeyUsage CertSign

**// To generate the client certificate**

New-SelfSignedCertificate -Type Custom -DnsName P2SChildCert -KeySpec Signature `

-Subject "CN=ClientCertificate" -KeyExportPolicy Exportable `

-HashAlgorithm sha256 -KeyLength 2048 `

-CertStoreLocation "Cert:\CurrentUser\My" `

-Signer $cert -TextExtension @("2.5.29.37={text}1.3.6.1.5.5.7.3.2")