AZURE A LEARNING GUIDE

Ashoka Chakravarti Marpu
Sr Technical Specialist
http://www.linkedin.com/in/acmarpu
Source content: docs.microsoft.com
GitHub: https://github.com/acmarpu

Table of Contents

Ashok
[Email address]

What is Azure?

Microsoft Azure is an ever-expanding set of cloud services to help your organization meet your business challenges. It’s the freedom to build, manage, and deploy applications on a massive, global network using your favorite tools and frameworks.

Azure is Microsoft's cloud solution. A cloud is essentially a collection of host data centers that you don't have to directly manage. You can request services from that cloud

Cost, Global scale, performance, security, speed, productivity, Reliability.

Azure is Responsible for

Availability of the platform (datacenter, connectivity, server, power cooling)
Data availability
Maintenance of the platform (datacenter, connectivity, server storage)
Physical security
Availability of the service (VM, storage, Network)

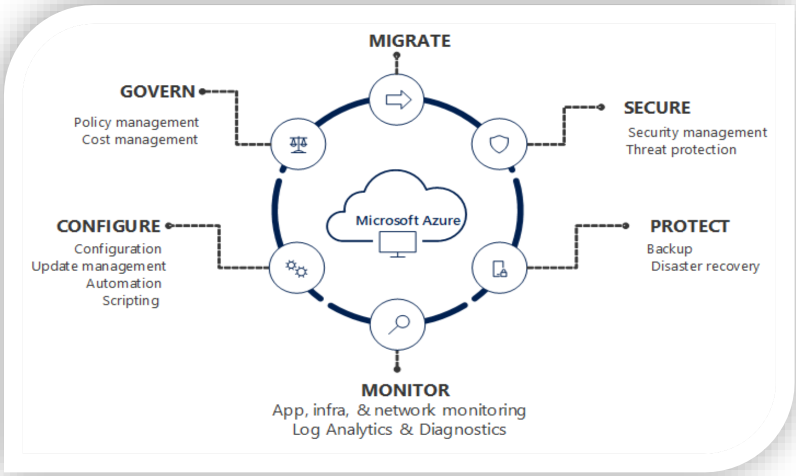
Azure is NOT responsible for

VM OS, Application deployment on the VM, Resource security

Customer are responsible for

VM maintenance & VM OS maintenance
Application availability
Backup and recovery &Configure the monitoring
User’s security, Configure the AD or other services

Responsibility	On-prem	IaaS	PaaS	SaaS
Data Governance &rights Management	Customer	Customer	Customer	Customer
Clients Endpoints	Customer	Customer	Customer	Customer
Account & Access Management	Customer	Customer	Customer	Customer
Identity & directory infrastructure	Customer	Customer	Microsoft/ Customer	Microsoft/ Customer
Application	Customer	Customer	Microsoft/ Customer	Microsoft
Network control	Customer	Customer	Microsoft/ Customer	Microsoft
Operating system	Customer	Microsoft	Microsoft	Microsoft
Physical Host	Customer	Microsoft	Microsoft	Microsoft
Physical network	Customer	Microsoft	Microsoft	Microsoft
Physical datacentre	Customer	Microsoft	Microsoft	Microsoft



Governance: - Governance provides mechanisms and processes to maintain control over your applications and resources in Azure. It involves planning your initiatives and setting strategic priorities. Governance in Azure is primarily implemented with two services. Azure Policy allows you to create, assign, and manage policy definitions to enforce rules for your resources. This feature keeps those resources in compliance with your corporate standards. Azure Cost Management allows you to track cloud usage and expenditures for your Azure resources and other cloud providers.

What is Azure Subscription?

- A subscription is a logical unit of Azure services that is linked to an Azure account. Each associated account has a role in a subscription. Billing for Azure services is done on a per-subscription basis.
- A Microsoft Azure subscription grants you access to Azure services and to the Microsoft Azure Platform Management Portal.
- Azure subscription is billing container for deployed Microsoft Azure Services
- We can deploy our IaaS, PaaS, SaaS application (web apps VM storage account network DR etc.)
- Azure Subscription has trusted relationship with Azure AD
- All the users, service, and devices authentication from Azure AD

Introduction to Azure Enterprise and Subscription Management

Billing account

- Represents a single owner (Account administrator) for one or more Azure subscriptions. An Account Administrator is authorized to perform various billing tasks like create subscriptions, view invoices or change the billing for subscriptions.

Subscription

- Represents a grouping of Azure resources. An invoice is generated at the subscription scope. It has its own payment methods that are used to pay its invoice.

What is an Azure account?

Account Administrator: 1 per Azure account

- Access the Azure Account Center
- Manage all subscriptions in an account
- Create new subscriptions
- Cancel subscriptions
- Change the billing for a subscription
- Change the Service Administrator
- **Note:** Conceptually, the billing owner of the subscription.
  The Account Administrator has no access to the Azure portal.

Service Administrator: 1 per Azure subscription

- Manage services in the Azure portal
- Cancel the subscription
- Assign users to the Co-Administrator role
- By default, for a new subscription, the Account Administrator is also the Service Administrator.
- The Service Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.
- The Service Administrator has full access to the Azure portal.
- **Note:** By default, for a new subscription, the Account Administrator is also the Service Administrator. The Service Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope. The Service Administrator has full access to the Azure portal.

Co-Administrator: 200 per subscription

- Same access privileges as the Service Administrator, but can't change the association of subscriptions to Azure directories
- Assign users to the Co-Administrator role, but cannot change the Service Administrator
  Note: The Co-Administrator has the equivalent access of a user who is assigned the Owner role at the subscription scope.

Azure Enterprise

Any Enterprise Agreement customer can add Azure to their agreement by making an upfront monetary commitment to Azure. That commitment is consumed throughout the year by using any combination of the wide variety of cloud services Azure offers from its global datacenters

Azure Enterprise Agreement Benefits

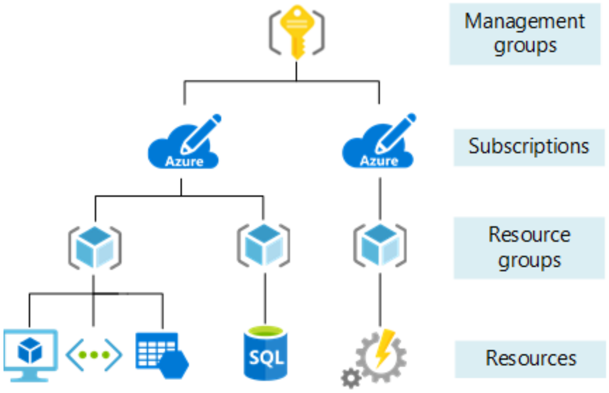
1. An EA is better for managing teams
2. An EA provides discounts
3. An EA helps with cash flow management
4. An EA gives you access to unique Azure features
5. Pay for additional usage beyond the commitment, at the same rates.

Azure EA admin Accounts

Enterprises enrollment

- The enterprises enrollment defines the shape and use of azure services with a company and is the core governance structure
- Within the enterprise's agreement customer can further subdivide the environment into department accounts and finally subscription
- Enterprises admin can add or associate accounts to the enrolment, can view usage data across all accounts

Organize your resources with Azure Management Groups



Manage Subscription with Portal

Use Subscriptions page to:

View and edit subscription details
Usage and billing information
View and edit profile
Change payment method
Cancel subscription
Enable preview features

Azure Resource Group

- Container for resource
- Logical grouping of resource of similar purpose
- Allows to delegate permission
- No costing is monitoring, or bill generate specific to location
- Sub-component under subscription
- Requires at least on resource group to create resource or consume resource

Role Base Access Control

RBAC provides fine-grained access management to your resources in Azure

Using RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. Instead of giving everybody unrestricted permissions in your Azure subscription or resources, you can allow only certain actions at a particular scope

Role-based access control can be used to assign permissions to:

- Users
- Groups
- Application

Scope: -
What level these permissions will apply
The scope of role assignment can be:

- Subscription
- Resource group
- Single resource
- Management group level

Here are some examples of what you can do with RBAC:

- Allow one user to manage virtual machines in a subscription and another user to manage virtual networks
- Allow a DBA group to manage SQL databases in a subscription
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets
- Allow an application to access all resources in a resource group

Owner has full access to all resources including the right to delegate access to other users.
Contributor has full access to all resources but can't delegate control to other users.
Resource Policy Contributor can create and manage policies in the directory on the resources.
Reader can view existing Azure resources

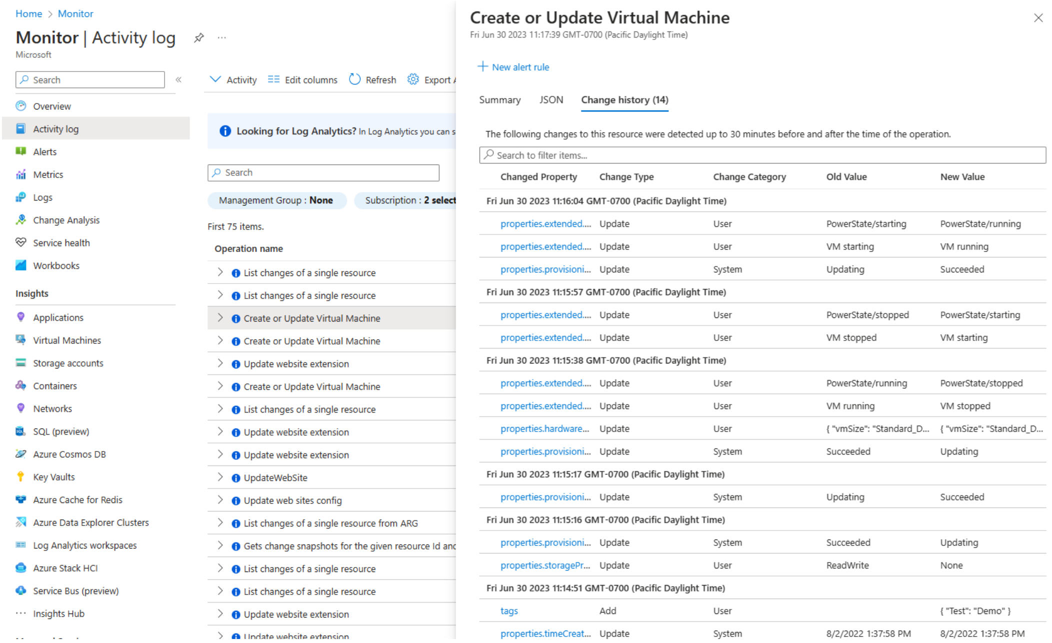
- Provide exact permission to user or group
- Grant access by assigning the appropriate RBAC role
- Can use built-in role or create custom role
- We ca grant to access at subscription level
- We can give the access at resource group
- We can grant the access for specific site

View Activity logs for RBAC changes

The Azure Activity log provides visibility into subscription-level events that have occurred in Azure
You can determine what operations were taken on the resources in your subscription

The Activity log has eight categories

Administrative: this contains all the records for create, update, delete, and action operations performed. Here we will see events related to RBAC
Service Health: This contains any health-related events that affect Azure.
Resource health: This contains that record of any resource health events that have occurred to your deployed resources in Azure
Alert: This contains all the alerts that have been activated
Autoscale: This includes all the record of events related to Autoscale.
Recommendation: this contains recommendation events from azure advisor
Security: This contains the record of any alerts generated by Azure security center
Policy: This contains records of all effect action operations performed by Azure policy



Looking for Log Analytics? In Log Analytics you can s

First 75 items.

Operation name
- List changes of a single resource
- List changes of a single resource
- Create or Update Virtual Machine
- Create or Update Virtual Machine
- Update website extension
- Create or Update Virtual Machine
- List changes of a single resource
- Update website extension
- Update website extension
- UpdateWebSite
- Update web sites config
- List changes of a single resource from ARG
- Gets change snapshots for the given resource Id anc
- List changes of a single resource
- List changes of a single resource
- Update website extension
- Update website extension

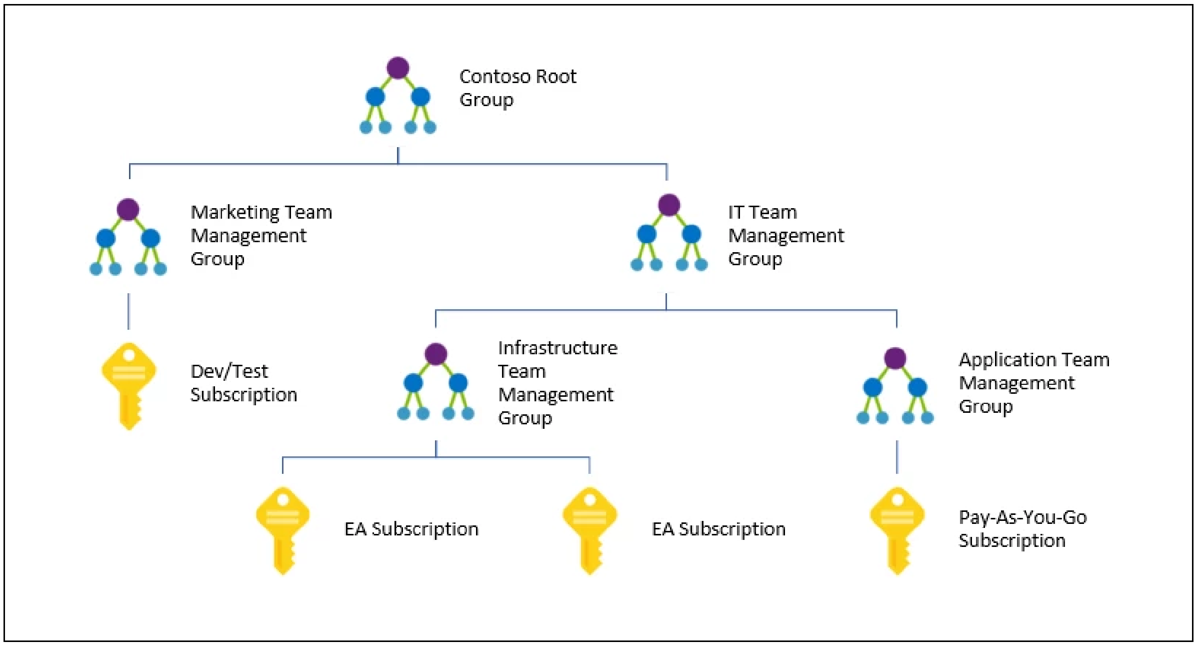
Create or Update Virtual Machine
Fri Jun 30 2023 11:17:39 GMT-0700 (Pacific Daylight Time)

The following changes to this resource were detected up to 30 minutes before and after the time of the operation.

Changed Property	Change Type	Change Category	Old Value	New Value
Fri Jun 30 2023 11:16:04 GMT-0700 (Pacific Daylight Time)				
properties.extended....	Update	User	PowerState/starting	PowerState/running
properties.extended....	Update	User	VM starting	VM running
properties.provisioni...	Update	System	Updating	Succeeded
Fri Jun 30 2023 11:15:57 GMT-0700 (Pacific Daylight Time)				
properties.extended....	Update	User	PowerState/stopped	PowerState/starting
properties.extended....	Update	User	VM stopped	VM starting
Fri Jun 30 2023 11:15:38 GMT-0700 (Pacific Daylight Time)				
properties.extended....	Update	User	PowerState/running	PowerState/stopped
properties.extended....	Update	User	VM running	VM stopped
properties.hardware...	Update	User	{ "vmSize": "Standard_D...	{ "vmSize": "Standard_D...
properties.provisioni...	Update	System	Succeeded	Updating
Fri Jun 30 2023 11:15:17 GMT-0700 (Pacific Daylight Time)				
properties.provisioni...	Update	System	Updating	Succeeded
Fri Jun 30 2023 11:15:16 GMT-0700 (Pacific Daylight Time)				
properties.provisioni...	Update	System	Succeeded	Updating
properties.storagePr...	Update	User	ReadWrite	None
Fri Jun 30 2023 11:14:51 GMT-0700 (Pacific Daylight Time)				
tags	Add	User		{ "Test": "Demo" }
properties.timeCreat...	Update	System	8/2/2022 1:37:58 PM	8/2/2022 1:37:58 PM

What is a management group?

An Azure Management group is logical containers that allow Azure Administrators to manage access, policy, and compliance across multiple Azure Subscriptions. Management groups allow you to build an Azure Subscription tree that can be used with several other Azure service, including Azure Policy and Azure Role Based Access Control. Azure Management Groups provide flexibility for organizing policy, access control, and compliance across multiple subscriptions. We can nest Azure Management Groups up to six levels deep for efficient management of resources.


Contoso Root Group
Marketing Team Management Group
IT Team Management Group
Dev/Test Subscription
Infrastructure Team Management Group
Application Team Management Group
EA Subscription
EA Subscription
Pay-As-You-Go Subscription

Azure AD / Microsoft Entra ID

****Azure Active Directory is now Microsoft Entra ID****

Windows Active Directory is a directory service developed by Microsoft for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. Initially, Active Directory was used only for centralized domain management.
Microsoft Entra ID 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.
Identity: Something that can be authenticated before permitting access to the desired resources.
Account: they the data associated with the identities that defines your permission
Azure Tenant: dedicated and trusted instances of azure AD created automatically.
Custom domain: your origination domain name which is added to azure apart from initial domain name.

AD features:
Application management
B2B, B2C Management
Conditional access
Device management
Identity management
Domain services
Privileged identity management
Reporting and monitoring
End-user self-service

MFA (Multi-Factor Authentication) on Azure
Provides additional security by requiring a second from of authentication
Many options can be configured by the admin to better customize the user experience
The organization can determine the preferred authentication methods
Fraud alerts can be configured
The multi-Factor authentication can be configured to accept different forms of authentication methods
Calling your phone
Sending a text massage
Notification in authenticator app
Verification code

Microsoft Intune
Microsoft Intune is a cloud-based enterprise mobility management tool that aims to help organizations manage the mobile devices employees use to access corporate data and applications, such as email.
It is a component of Microsoft's Enterprise Mobility + Security (EMS) offering, a mobile device management and application management platform. Microsoft's Intune app is designed to integrate with other parts of the EMS platform, including Azure Active Directory and Azure Information Protection. The app protection policy component of Microsoft Intune uses Azure Active Directory identity to maintain separation between corporate and personal data.

Azure AD Connect
It is used to integrate the on-premise directories (Active Directories) with Azure Active Directory which provides a common identity for accessing both cloud and on-premise resources.
There are various features of Azure AD Connect:
1) Password Hash Synchronization: Sign-in method that synchronizes a hashed user on-premised AD password with Azure AD.
2) Pass-through authentication: Sign-in method that provides access to users to use the same password on-premise and on the cloud.
3) Synchronization: Responsible for creating users, groups, and other objects and also validate if the identity information of your on-premise users and groups matches with the cloud.
4) Health Monitoring: A central place to view the activity and also provide monitoring.

Managed Identity:

What it is: Managed identities are a feature in Azure that provides an identity for a service or resource within the Azure Active Directory (Azure AD) tenant. They are designed to simplify the management of credentials used by applications and services running in Azure.

Use cases: Managed identities are typically used when you have a resource (such as an Azure Virtual Machine or Azure Function) that needs to authenticate and access other Azure resources securely. Instead of managing credentials (e.g., usernames and passwords) manually, you can use a managed identity.

How it works: When you enable a managed identity for an Azure resource, Azure creates a service principal in the Azure AD tenant that represents that resource. This service principal is used to authenticate the resource with Azure AD, and it has specific permissions associated with it.

Managed identity types

There are two types of managed identities:

System-assigned Some Azure services allow you to enable a managed identity directly on a service instance. When you enable a system-assigned managed identity an identity is created in Azure AD that is tied to the lifecycle of that service instance. So, when the resource is deleted, Azure automatically deletes the identity for you. By design, only that Azure resource can use this identity to request tokens from Azure AD.

User-assigned You may also create a managed identity as a standalone Azure resource. You can create a user-assigned managed identity and assign it to one or more instances of an Azure service. In the case of user-assigned managed identities, the identity is managed separately from the resources that use it.

Service Principal:

What it is: A service principal is essentially an identity created for an application, service, or automation tool to access resources within a specific Azure AD tenant or other Microsoft services. It is not limited to Azure resources and can be used to authenticate and access various Microsoft services.

Use cases: Service principals are versatile and can be used in a wide range of scenarios, including when you need to access Azure resources, call Azure REST APIs, or integrate with other Microsoft services like Microsoft Graph.

How it works: A service principal is explicitly created and configured by an administrator. It can have specific roles and permissions assigned to it within Azure or other Microsoft services. Service principals are often used in applications and scripts to authenticate and access resources programmatically.

What is Azure AD Privileged Identity Management

Privileged Identity Management (PIM) is a service in Azure Active Directory (Azure AD) that enables you to manage, control, and monitor access to important resources in your organization. These resources include resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune. The following video introduces you to important PIM concepts and features

- Provide just-in-time privileged access to Azure AD and Azure resources
- Assign time-bound access to resources using start and end dates
- Require approval to activate privileged roles
- Enforce multi-factor authentication to activate any role
- Use justification to understand why users activate
- Get notifications when privileged roles are activated
- Conduct access reviews to ensure users still need roles
- Download audit history for internal or external audit
- Prevents removal of the last active Global Administrator role assignment

Azure DNS

- Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure
- By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.
- Utilize the Microsoft global service footprint providing highly available services
- Common records such as A, AAAA, CNAME, MX, NS, PTR, SOA, SRV and TXT supported.
- Private zones enable virtual networks to participate either as
- A registration VNet (one per private zone and publishes records)
- A resolutions VNet (10 per private zone and resolves records)

DNS and Virtual Network

- DNS configuration is possible with a virtual network and at the VM Nic level
- The Azure DNS can be used which provided name resolution for all services within the virtual network
- DNS servers can explicitly be configuration such as you Dc's (we can use our on-premises DNS to our Azure Cloud)
- The DNS configuration is applied to the VMs vis DHCP
- VMs in Azure almost ALWAYS get their IP configuration via DHCP and never static configuration
- VM must be restarted to get the updated DNS configuration.

Azure Networking

IP support in Virtual network

- IPV4 and IPV6
- TCP, UDP, and ICMP
- No multicast, broadcast GRE protocols or IP-in-IP packets
- VM always get the IP address via DHCP in azure (unless using multiple IPs on a VM nic)
- Never try and assign a static IP unless mandatory otherwise it will break at some points
- When a VM re-provisioned to the fabric it gets a new vmNIC and possibly a new IP.
- Static IP can be assigned via the Azure fabric using portal, PowerShell and CLI
- Create a separate subnet as the pool for static IP assignment.

Ingress Egress

- Data in bound to Azure
- There is no charge for ingress

Egress

- Data outbound from Azure, there are charge for egress (unless using an unmetered express route connection) from azure datacenter.

Network Interface Card (NIC)

VMs communicate with other VMs and other resources on the network by using virtual network interface card (NIC) virtual NICs configure VMs with Private IP address optional Public IP Address VM can have more than NIC for different network configuration.

Azure DNS

- Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure
- By hosting your domains in Azure, you can manage your DNS records by using the same credentials, APIs, tools, and billing as your other Azure services.
- Utilize the Microsoft global service footprint providing highly available services
- Common records such as A, AAAA, CNAME, MX, NS, PTR, SOA, SRV and TXT supported.
- Private zones enable virtual networks to participate either as
- A registration VNet (one per private zone and publishes records)
- A resolutions VNet (10 per private zone and resolves records)

DNS and Virtual Network

- DNS configuration is possible with a virtual network and at the VM Nic level
- The Azure DNS can be used which provided name resolution for all services within the virtual network
- DNS servers can explicitly be configuration such as you Dc's (we can use our on premises DNS to our Azure Cloud)
- The DNS configuration is applied to the VMs vis DHCP
- VMs in Azure almost ALWAYS get their IP configuration via DHCP and never static configuration
- VM must be restarted to get the updated DNS configuration.

Azure Virtual Network (VNet)

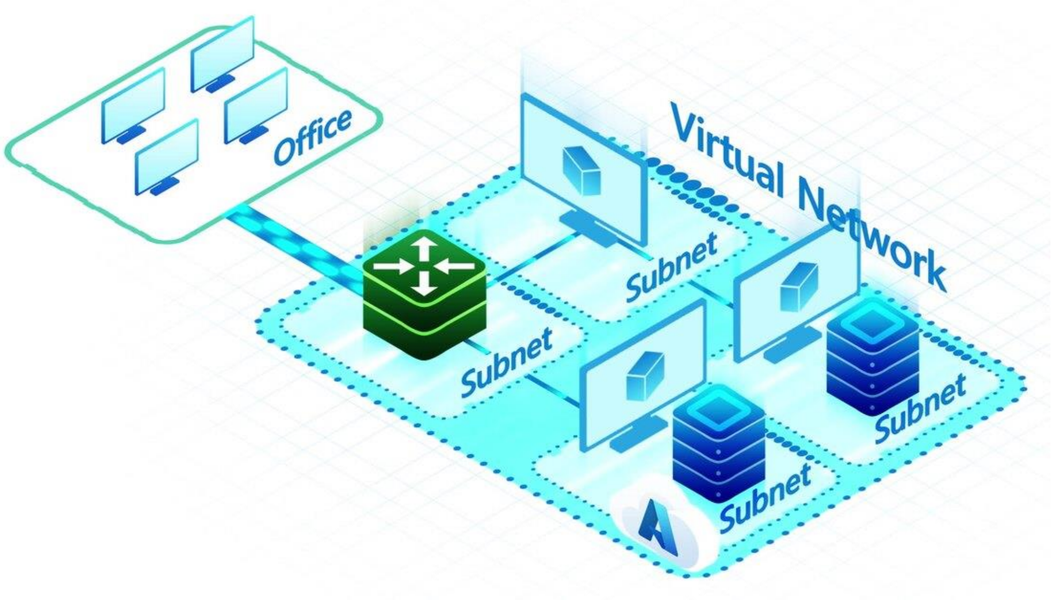
- An Azure Virtual Network (VNet) is a representation of your own network in the cloud. It is a logical isolation of the Azure cloud dedicated to your subscription.
- Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure
- A VNet is a constrict creates in azure lives within a region within subscription has one or more IP address assigned to it.
- You can fully the control IP address blocks DNS settings, security polices and route table within the network.
- you can also further segmentation of the VNet into subnets and launch azure IaaS virtual machines and /or Cloud services (PaaS role instance)
- You can use VNets to provision and manage virtual private networks (VPNs) in Azure and, optionally, link the VNets with other VNets in Azure, or with your on-premises IT infrastructure to create hybrid or cross-premises solutions.
- Each VNet you create has its own CIDR block and can be linked to other VNets and on-premises networks as long as the CIDR blocks do not overlap.
- 4096 private IPS per Virtual network
- Whatever IP range selected should not conflict with on-premises network and another Virtual network

Why use an Azure virtual network?

- Key scenarios that you can accomplish with a virtual network include:
- Communication of Azure resources with the internet.
- Communication between Azure resources.
- Communication with on-premises resources.
- Filtering of network traffic.
- Routing of network traffic.
- Integration with Azure services.

Use VNets to

- Create a dedicated private cloud-only VNet Sometimes you don't require a cross-premises configuration for your solution. When you create a VNet, your services and VMs within your VNet can communicate directly and securely with each other in the cloud. You can still configure endpoint connections for the VMs and services that require Internet communication, as part of your solution.
- Securely extend your datacentre With VNets, you can build traditional site-to-site (S2S) VPNs to securely scale your datacentre capacity. S2S VPNs use IPSEC to provide a secure connection between your corporate VPN gateway and Azure.
- Enable hybrid cloud scenarios VNets give you the flexibility to support a range of hybrid cloud scenarios. You can securely connect cloud-based applications to any type of on-premises system such as mainframes and Unix systems.



Subnet

- A subnet is a range of IP address in the VNet. You can divide a VNet into multiple subnets.
- VM deployed to subnets (same or different) with in a VNet can communicate each other without any extra configuration
- You can also configure route tables and NSG to subnet
- Within each subnet, the first three IP address and last IP address are reserved and can be not used for VMs, the smallest subnets are supported to use a 29-bit subnet mask
- First and last reserved per protocol for host id and broadcast.
- The 1st three IP address are reserved binary 01, 10 and 11 in the host ID portion of the IP address
- We can add more address spaces.
- Azure reserves 5 IP addresses within each subnet. These are x.x.x.0-x.x.x.3 and the last address of the subnet. x.x.x.1-x.x.x.3 is reserved in each subnet for Azure services.
- x.x.x.0: Network address
- x.x.x.1: Reserved by Azure for the default gateway
- x.x.x.2, x.x.x.3: Reserved by Azure to map the Azure DNS IPs to the VNet space
- x.x.x.255: Network broadcast address

CIDR

- Class less Inter – Domain Routing
- CIDR way to represent network IP block. The length of the network prefix in IPv4 CIDR is specified as part of the IP address.
- For example: 192.30.250.0/24 the 192.30.250.0 is the network address it self and the “24” says that the first 24 bit are the network part of the address. Leaving the last 8 bit for specific host address
- CIDR notation is a compact representation of an IP address and its associated routing prefix.
- The notation is constructed from an IP address, a slash (“/”) character and a decimal number. The number is the count of leading 1 bit in the routing mask traditionally called the network mask
- Used in virtual network configuration combing the IP address and it associate network mask
- XXX.XXX.XXX.XXX/N
- XXX.XXX.XX.XXX/ IP address
- N is the number of bits used for subnet mask E.g. 24 would equal to 255.255.255.0 10.2.1.0/24 equates to IP range 10.2.10 to 10.2.1.255

Azure VNet Pricing

- There is no extra cost for using Virtual Networks in Azure
- The compute instances launched within the VNet will be charged the standard rates as described in Azure VM pricing
- The VPN gateway and public IP address used in the VNet will also be charged standard rates

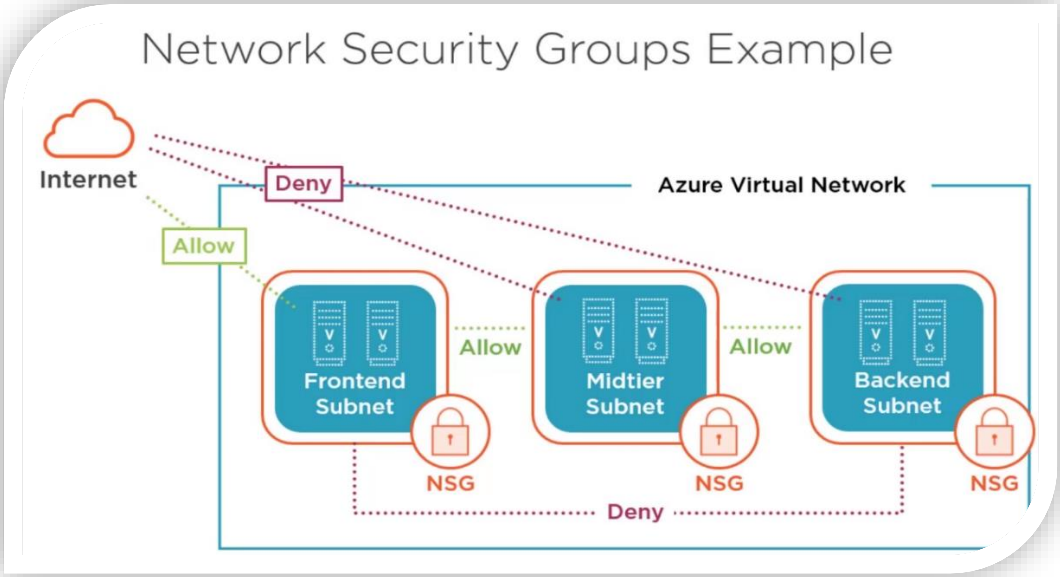
Virtual Network Benefits

- **Isolation.** Vnets are completely isolated from one another. That allow you to create disjoint network from development, testing, production that use the same CIDR address book
- **Access to the Public internet** All IaaS and PaaS role instances in a Vnet can access the public internet by default. You can control access by using by network security group (NSG)
- **Access to VMs with the Vnet.** PaaS role instance and IaaS VMs can be launched in the same virtual network and they can connect each other using private IP address if they are in different subnets without need to configure a getaway or use public IP address
- **Name resolution** Azure provide the internal name resolution for IaaS VMs and PaaS role instance deployed in your Vnet you can also deploy your own DNS servers and configure the Vnet use them.
- **Security** traffic entering and existing the virtual machines and PaaS role instance in a Vnet can be controlling use Network Security Group
- **Connectivity** Vnets can be connected to each other, and even to your on-premises datacentre by using Site-to-Site VPN connection or Express route connection.

Network Security Group:

- **It contains a set of security rules that allow or deny inbound and outbound traffic using the following 5-tuple: protocol, source IP address range, source port range, destination IP address range, and destination port range.**
- A network security group can be associated to multiple network interfaces and subnets, but each network interface or subnet can be associated to only one network security group.
- Network security group is a layer of security that acts as a virtual firewall for controlling traffic in and out of virtual machines (via network interfaces) and subnets.
- Which inspect the incoming and outgoing traffic on the interface
- Which allows / denies based in the incoming and outgoing rules
- Sit at the network level
- The last rule is denied all
- It can consist of allow rule and deny rule
- Based on priority it will allow or deny the traffic
- Can be associated with multiple virtual machines
- **Name** A unique identifier for the rule
- **Direction** traffic is inbound or outbound

- **Priority** Rule with higher priority apply
- **Access** Specifies whether is traffic is allowed or denied
- **Source IP address Prefix** This identifies from where traffic originates
- **Source Port Range** This specifies port range
- **Destination IP address Prefix** This identifies the destination traffic
- **Destination Port Range** This Specifies destination port range
- **Protocol** protocol specifies a protocol that match the rule it can be UDP, TCP, or the asterisk (*****) wildcard character



- Traffic flow in a Virtual Network:
- This may not always be desired
- -in a multi- tiered application may want only neighbour tires to communicate
- -May want to restrict types of traffic
- Enable rule to be created then assigned to a network security group
- Applied to subnet or vmNIC
- When applied to subnet it is still enforced at the vmNIC it is not an “edge” device

Azure Firewall

- **Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.**
- NSGs provide the ability to control traffic but is based around IP ranges and implemented in the VFP
- Azure firewall provides a native NVA that is deployed to a virtual network and is highly available and leverages full cloud scalability
- UDR is utilized to direct internet bound traffic via the azure firewall
- Azure firewall enables for FQDN whitelisting and NAT services
- High availability
- Unrestricted scalability
- Azure Firewall is a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability and unrestricted cloud scalability.

Application Security Group

- Application Security Groups helps to manage the security of the Azure Virtual Machines by grouping them according the applications that runs on them. It is a feature that allows the application-centric use of Network Security Groups.
- NSGs are focused on the IP address range which may be difficult to maintain for growing environment
- Application Security group (ASGs) enable monikers for different application roles to be defined
- E.g. webserver DD server, web app, webapp2
- The vmNIC for a VM is made a member off one or more ASGs
- The ASGs are used in rule that are part of NSGs to control the flow of communication and can still use NSG features like service tags

Public Facing IPs

- The private IPs used by VM cannot be used to offer services to the internet
- An internet-routable address public IP, is required
- Azure provides public IP address which can be static or dynamic along with DNS name
- Public IP address are bound to the region they are created in (same region cannot move)
- Customer public IP addresses cannot be used in Azure
- Public IPs are created as an azure resource

Has a DNS name

<name>. <region>. cloudapp.azure.com

Assigned to

-A VM (not recommended in most scenarios)

- An azure load balance instance as the front-end address
-A VPN gateway
- An application gateways
A virtual application is a VM in the above

Stop: Public IP will be released, and NAT is deleted
Temporary disk will delete permanently
Start: Azure will assign Dynamic IP address
NAT attach a temporary storage disk
Reboot: Restart the guest O/S
VM will continue to run on the same physical host
VM will have the same public IP
VM will have the same temporary disk
Delete: will permanently delete the VM and VM disk public and private IP release temporary Disk

Dynamic Vs. Static Public IP

Dynamic IP

- is assigned when a service is started
- Azure will assign when a Vm is started and release when a VM is stopped or deleted.

Use Static IP when

- Azure will assign a public IP, which can exist even vm is powered off
- Static IP is assigned at time of creation
- Will use a DNS name host (A) record pointing to the services
- There are firewall rule or other security based on the service IP address
- SSL certificates that link to the IP address
- Move the static IP

Assigning a public IP to a VM

- When assigning a public IP directly to a VM the OS inside the VM does not see the IP address
- Rather any traffic sent to that public IP address is sent to the VM
- Each IP configuration (on a vmNIC) can have a public IP
- This is a useful option when the service offered needs to use a wide range of ports that would not be possible via port forwarding rules / NAT
  - Passive FTP
- Limits scale and resiliency

Virtual Applications

Azure network virtual appliance is used in the Azure application to enhance high availability. It is used as an advanced level of control over traffic flows, such as when building a demilitarized zone (DMZ) in the cloud.

A large number of virtual appliances are available in the azure marketplace
License can be based on: -

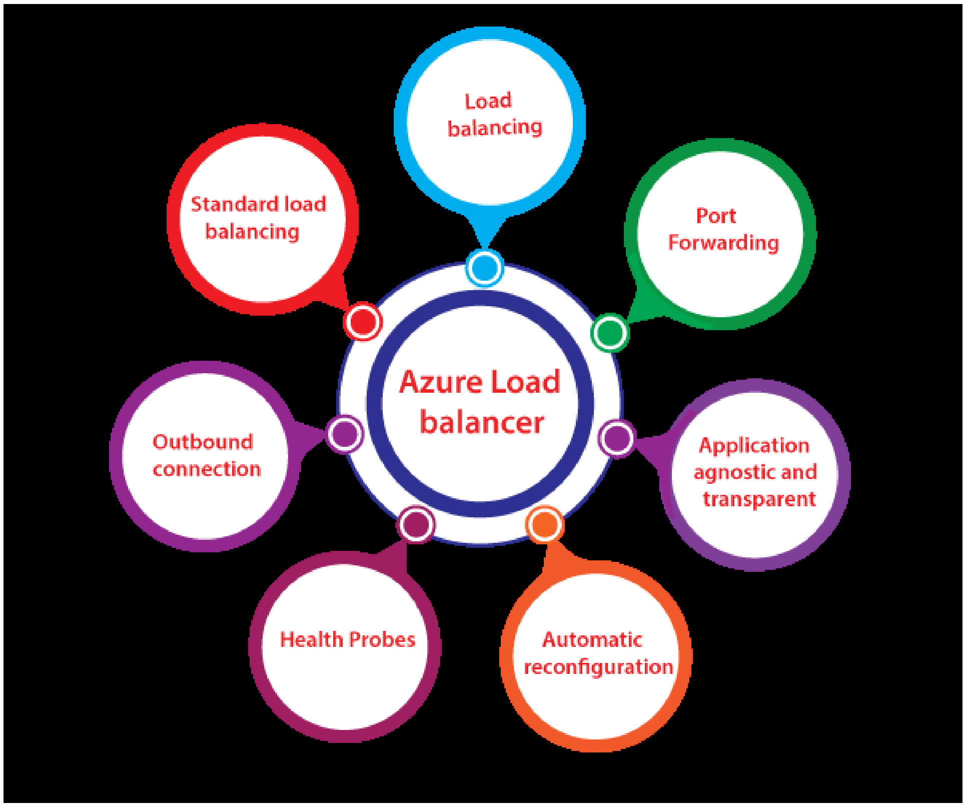
- Bring your own license
- Hourly billing

Essentially a VM pre-configured software and configuration to perform a certain set of functionalities
Common examples include firewall and load balancer

Azure Load Balancer

- **The load balancer is used to distribute the incoming traffic to the pool of virtual machines. It stops routing the traffic to a failed virtual machine in the pool. In this way, we can make our application resilient to any software or hardware failures in that pool of virtual machines.**
- Azure Load Balancer operates at layer 4 of the OSI model. It's the single point of contact for clients
- Azure Load Balancer can be defined as a cloud-based system that allows a set of machines to perform as one single machine to serve the request of a user.
- With Azure Load Balancer, you can scale your applications and create high availability for your services. Load Balancer supports inbound and outbound scenarios, provides low latency and high throughput, and scales up to millions of flows for all TCP and UDP applications.
- Virtual machines and cloud services in a virtual network can be exposed to using Azure Load balancer.
- Is an explicit object
- With Azure Load Balancer, you can create a load-balancing rule to distribute traffic that arrives at frontend to backend pool instances. Load Balancer uses a hash-based algorithm for distribution of inbound flows and rewrites the headers of flows to backend pool instances accordingly. A server is available to receive new flows when a health probe indicates a healthy backend endpoint

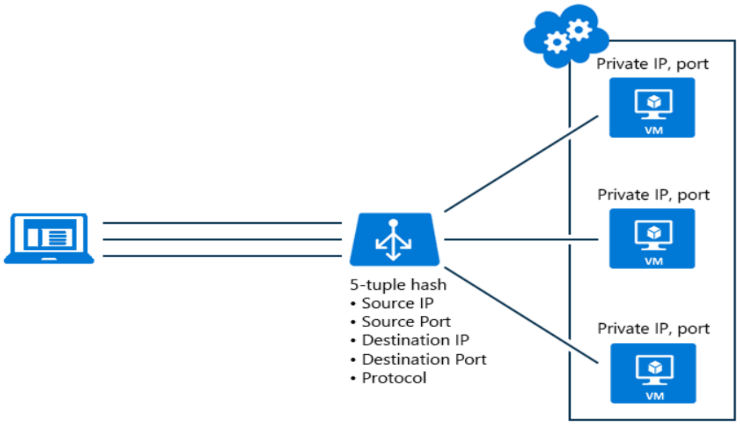
- **Port forwarding**
  With Load Balancer, you can create an inbound NAT rule to port forward traffic from a specific port of a specific frontend IP address to a specific port of a specific backend instance inside the virtual network. This is also accomplished by the same hash-based distribution as load balancing



- **Automatic reconfiguration**
  Load Balancer instantly reconfigures itself when you scale instances up or down. Adding or removing VMs from the backend pool reconfigures the Load Balancer without additional operations on the Load Balancer resource.
- **Health probes**
  To determine the health of instances in the backend pool, Load Balancer uses health probes that you define. When a probe fails to respond, the Load Balancer stops sending new connections to the unhealthy instances. Existing connections are not affected, and they continue until the application terminates the flow, an idle timeout occurs, or the VM is shut down
- **Source IP Affinity mode**
  Load Balancer can also be configured by using the source IP affinity distribution mode. This distribution mode is also known as session affinity or client IP affinity. The mode uses a 2-tuple (source IP and destination IP) or 3-tuple (source IP, destination IP, and protocol type) hash to map traffic to the available servers. By using source IP affinity, connections that are initiated from the same client computer go to the same DIP endpoint.

Two types

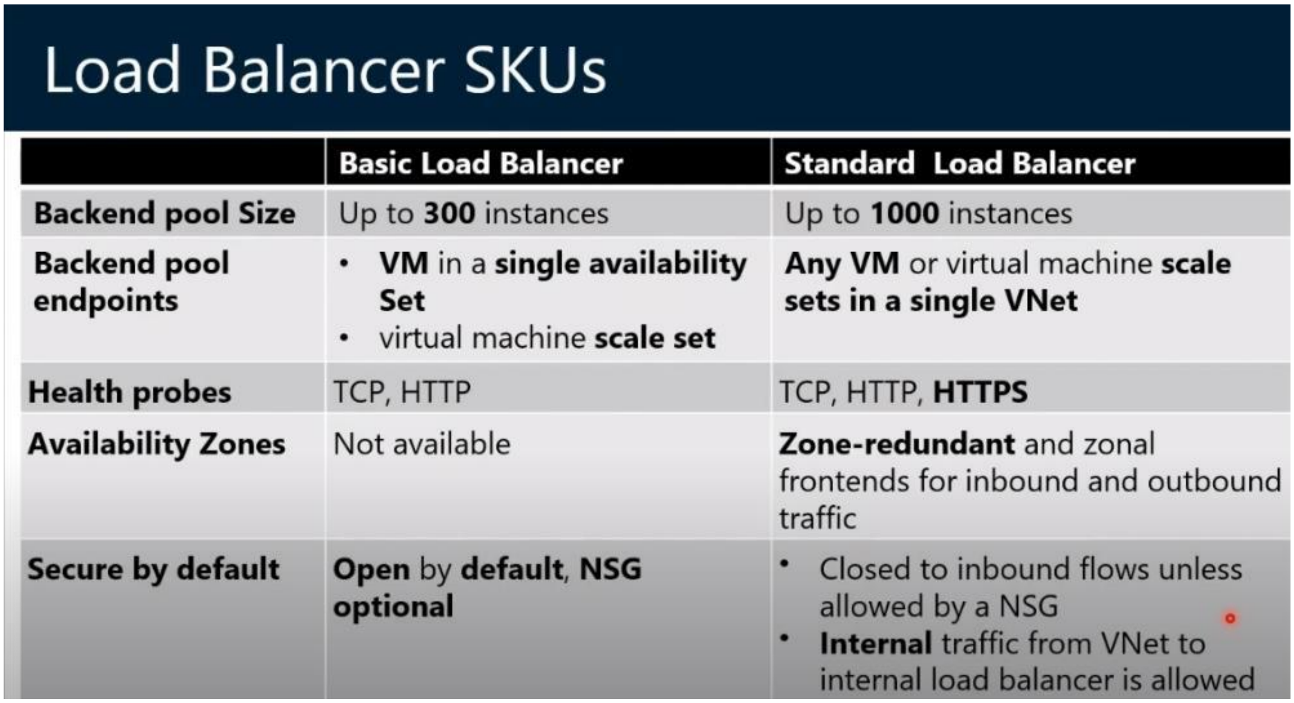
a. **External Load balancer/ internet-facing load balancer** you can use external load balancer to provide high availability for IaaS VMS and PaaS role instance accessed from the Public internet.
   Balances incoming traffic from the internet to VMs in Azure and its front end has a public IP
b. **Internal Load balancer** you can use internal load balancer to provide high availability for IaaS VMs and PaaS role instance accessed from other services in your Vnets.
   Balances traffic between VMs in a Virtual network (or connected network) am dots front end has a private IP



Load balancer can have multiple front-end configuration
Load balancer Services
Hash-based distribution – Actually balancing traffic between multiple targets
Port forwarding – direct incoming traffic to a port on the LB inbound IP and forwarding to a port on specific target (NAT Rules)

Load balancer Stickiness

By defaults uses 5 tuples
-The source IP address
-The destination IP address
-The protocol type (TCP or UDP)
-The source ports
-The destination ports



Load Balancer SKUs

	Basic Load Balancer	Standard Load Balancer
Backend pool Size	Up to **300** instances	Up to **1000** instances
Backend pool endpoints	• **VM** in a **single availability Set** • virtual machine **scale set**	**Any VM** or virtual machine **scale sets in a single VNet**
Health probes	TCP, HTTP	TCP, HTTP, **HTTPS**
Availability Zones	Not available	**Zone-redundant** and zonal frontends for inbound and outbound traffic
Secure by default	**Open** by **default**, **NSG optional**	• Closed to inbound flows unless allowed by a NSG • **Internal** traffic from VNet to internal load balancer is allowed

Traffic Manger

1. Azure Traffic Manager is a DNS-based traffic load balancer that enables you to distribute traffic optimally to services across global Azure regions,
2. Traffic Manager uses DNS to direct client requests to the most appropriate service endpoint based on a traffic-routing method and the health of the endpoints.
3. An endpoint is any Internet-facing service hosted inside or outside of Azure.
4. Traffic Manager provides a range of traffic-routing methods and endpoint monitoring options to suit different application needs and automatic failover models.
5. Traffic Manager is resilient to failure, including the failure of an entire Azure region.

- Increase application availability
- Improve application performance
- Perform service maintenance without downtime
- Combine hybrid application
- Distribute traffic for complex deployment
- Performance routing to send the requestor to the closest endpoint in terms of latency.
- Priority routing to direct all traffic to an endpoint, with other endpoints as backup.
- Weighted round-robin routing, which distributes traffic based on the weighting that is assigned to each endpoint.

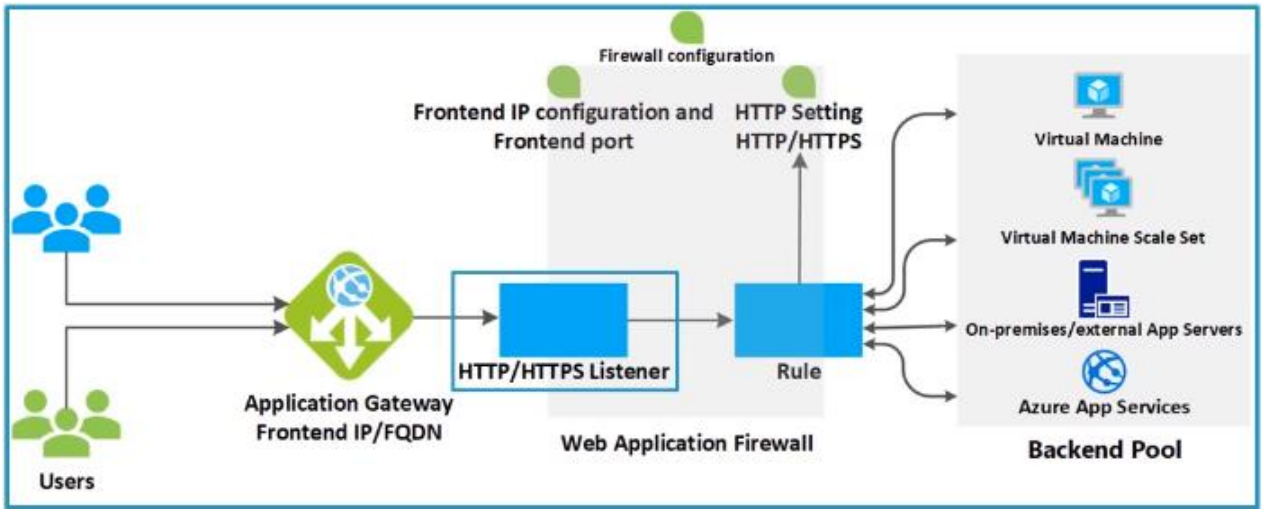
- **Azure endpoints** are used for services hosted in Azure.
- **External endpoints** are used for IPv4/IPv6 addresses, or, for services hosted outside Azure that can either be on-premises or with a different hosting provider.

- **Nested endpoints** are used to combine Traffic Manager profiles to create more flexible traffic-routing schemes to support the needs of larger, more complex deployments.

Azure Application Gateway

- Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.
- Traditional load balancers operate at the transport layer (OSI layer 7 - TCP and UDP) and route traffic based on source IP address and port, to a destination IP address and port.
- Application Gateway you can be even more specific. 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 optimized for videos.
- Can routes the traffic based on the URL
- Features
- Autoscaling
- SSL termination
- Connection draining
- Web application firewall
- URL-based routing
- ETC.

Static VIP - The application gateway VIP now supports the static VIP type exclusively. This ensures that the VIP associated with application gateway does not change even after a restart.



Azure Front Door

Azure Front Door is a global, scalable entry-point that uses the Microsoft global edge network to create fast, secure, and widely scalable web applications. With Front Door, you can transform your global consumer and enterprise applications into robust, high-performing personalized modern applications with contents that reach a global audience through Azure.

Why use Azure Front Door?

With Front Door you can build, operate, and scale out your dynamic web application and static content. Front Door enables you to define, manage, and monitor the global routing for your web traffic by optimizing for top-tier end-user performance and reliability through quick global failover.

Key features included with Front Door:

Accelerated application performance by using split TCP-based anycast protocol.
Intelligent health probe monitoring for backend resources.
URL-path based routing for requests.
Enables hosting of multiple websites for efficient application infrastructure.
Cookie-based session affinity.
SSL offloading and certificate management.
Define your own custom domain.
Application security with integrated Web Application Firewall (WAF).
Redirect HTTP traffic to HTTPS with URL redirect.
Custom forwarding path with URL rewrite.
Native support of end-to-end IPv6 connectivity and HTTP/2 protocol.

Network Security Appliances

Both Microsoft and third-party products

Featuring:

- security and protection
- Infrastructure security
- Web application

Third-party security appliances available through the marketplace

- Barracuda
- Palo alto
- Sophos
- And more

Pricing will vary

- Most have try before you buy
- Scale as needed

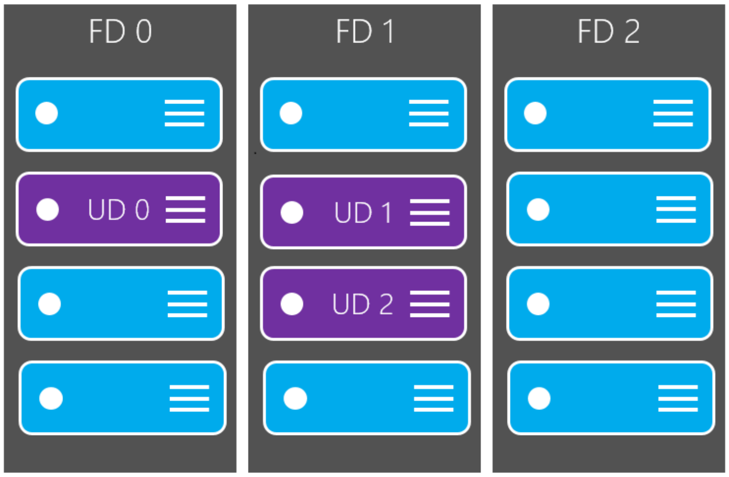
Creates a VM

- Sizing options availability will vary

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.
When a single VM is used with Azure Premium Storage, the Azure SLA applies for unplanned maintenance events.
Consist of Fault domain and update domain
Consist of VM which are running the same application
Distribute the VMs which are in availability set to different fault domains and updates domains

Fault domain: Set of physical servers connected to same power source and network source
Update domain: set of physical servers running win2012 Hyper-V where MS will do patch management or firmware upgradations at once



Availability Zone

Availability Zone is an isolated location inside of an Azure Region, and has its own independent power source, network, and cooling. The physical and logical separation of Availability Zones within an Azure region protects applications and data from zone-level failures. Availability Zone data transfer pricing is based on Availability Zones.

Auto scaling(VMSS)

Auto scaling is the process of dynamically allocating resources to match performance requirements. As the volume of work grows, an application may need additional resources to maintain the desired performance levels and satisfy service-level agreements (SLAs). As demand slackens and the additional resources are no longer needed, they can be de-allocated to minimize costs.

Limitations

SKUs are not mutable. You may not change the SKU of an existing resource.
A Load Balancer rule cannot span two virtual networks. Frontends and their related backend instances must be located in the same virtual network.

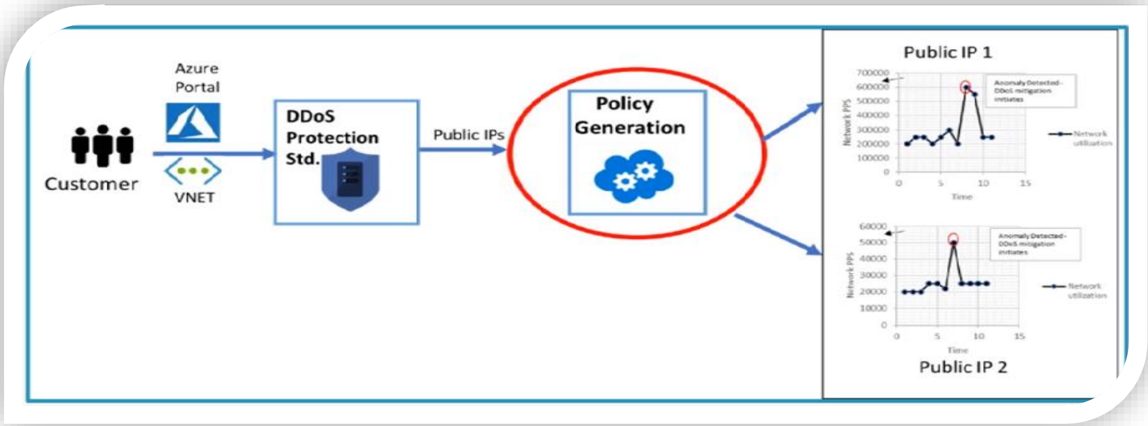
Load Balancer frontends are not accessible across global virtual network peering

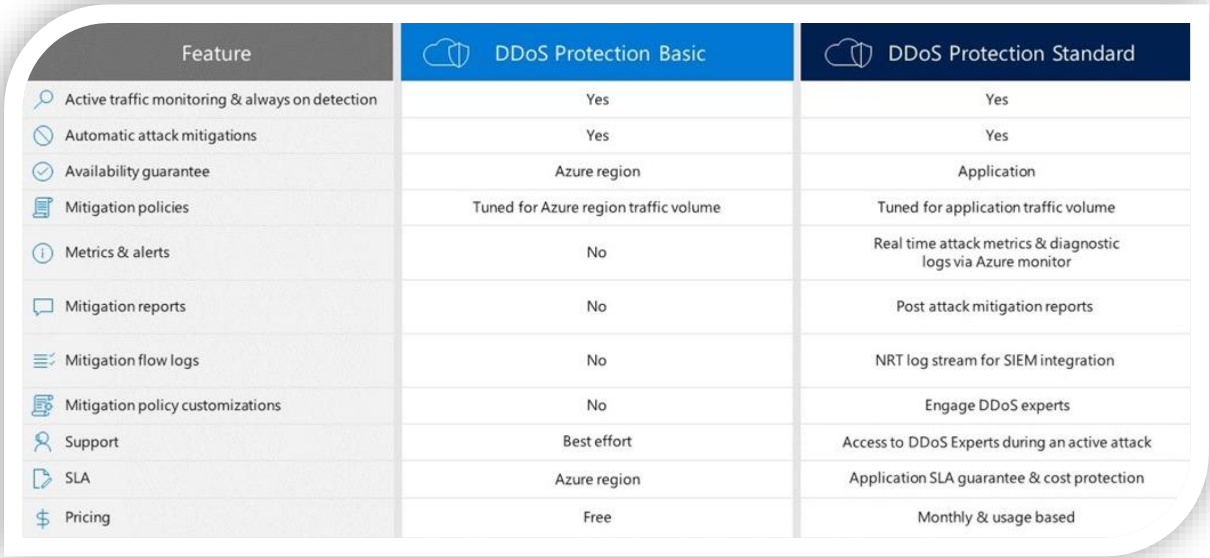
a) Vertical scaling, also called scaling up and down, means changing the capacity of a resource. For example, you could move an application to a larger VM size. Vertical scaling often requires making the system temporarily unavailable while it is being redeployed. Therefore, it's less common to automate vertical scaling.

b) Horizontal scaling, also called scaling out and in, means adding or removing instances of a resource. The application continues running without interruption as new resources are provisioned. When the provisioning process is complete, the solution is deployed on these additional resources. If demand drops, the additional resources can be shut down cleanly and deallocated.

Azure DDOs standard protection

- A malicious attempt to disrupt normal traffic by flooding a website with large amount of fake traffic.
- Distributed denial of service (DDos) is a major threat to internet facing services
- Azure provides a basic large-scale DDos protection for all services but its tolerance is not configurable nor can it be monitored.
- Azure DDos standard protection is enabled at a virtual network level based on user-defined policies that is applied to all public IPs associated with resource in the virtual network.
- Real-time monitoring and telemetry available
- Services basic and standard
- Instant on protection
- Traffic monitoring
- Adaptive tuning
- Attack analytics, metrics, and alerting

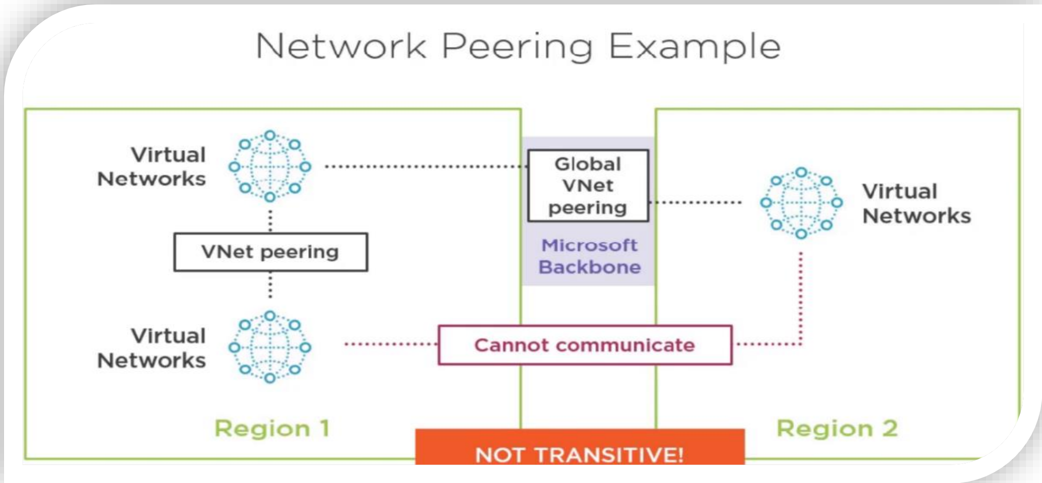




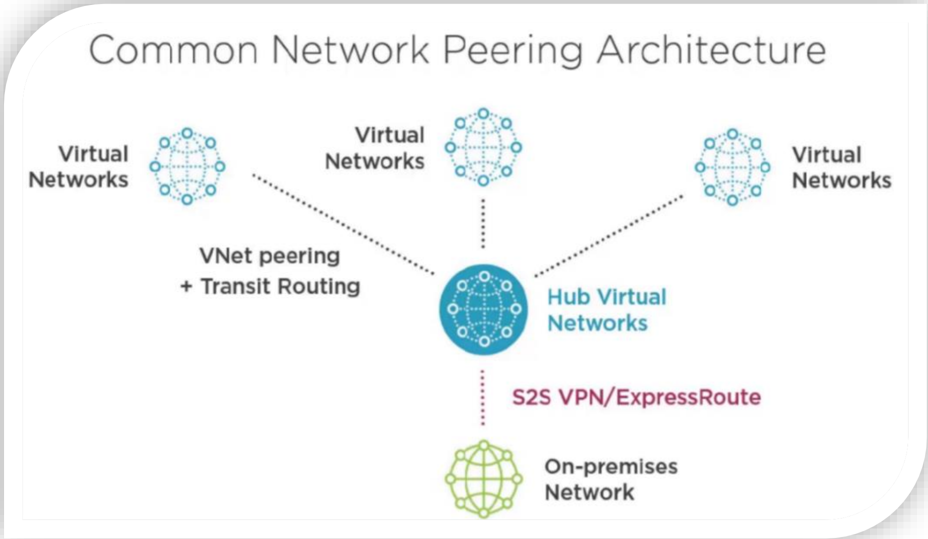
Feature	DDoS Protection Basic	DDoS Protection Standard
Active traffic monitoring & always on detection	Yes	Yes
Automatic attack mitigations	Yes	Yes
Availability guarantee	Azure region	Application
Mitigation policies	Tuned for Azure region traffic volume	Tuned for application traffic volume
Metrics & alerts	No	Real time attack metrics & diagnostic logs via Azure monitor
Mitigation reports	No	Post attack mitigation reports
Mitigation flow logs	No	NRT log stream for SIEM integration
Mitigation policy customizations	No	Engage DDoS experts
Support	Best effort	Access to DDoS Experts during an active attack
SLA	Azure region	Application SLA guarantee & cost protection
Pricing	Free	Monthly & usage based

Peering

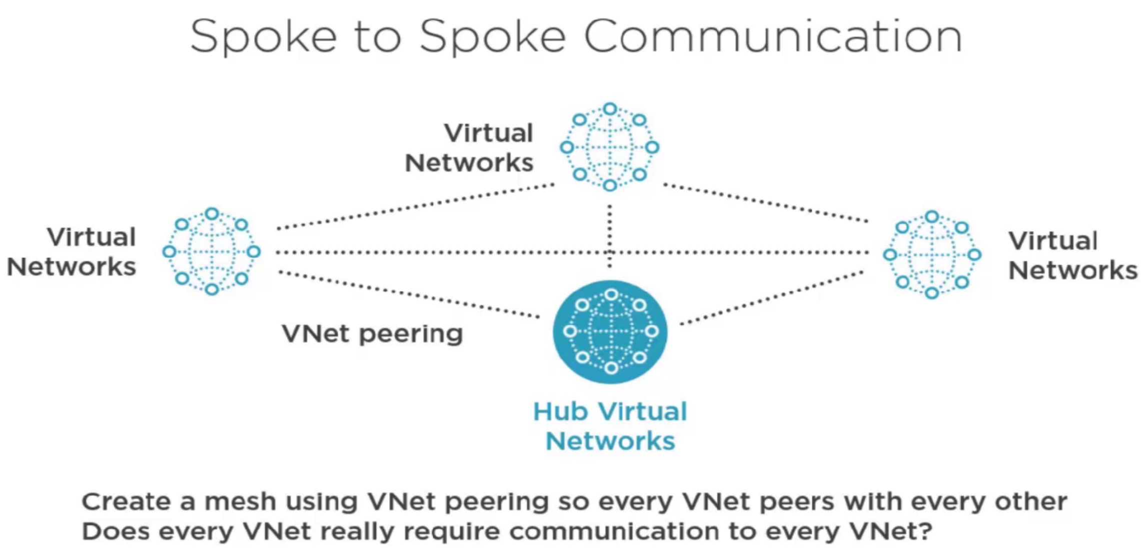
- Enable connectivity between virtual networks using the Azure backbone without gateway
- Nominal ingress and egress cost
- Can be different regions (global Vnet Peering) and different subscriptions
- Utilize S2S VPN between virtual networks
- Connect virtual networks to the same ExpressRoute circuit (or circuits that have routing between them)
- Utilize NVA
- VNet peering - connecting VNets within the same Azure region
- Global VNet peering - connecting VNets across Azure regions



Network Peering Example

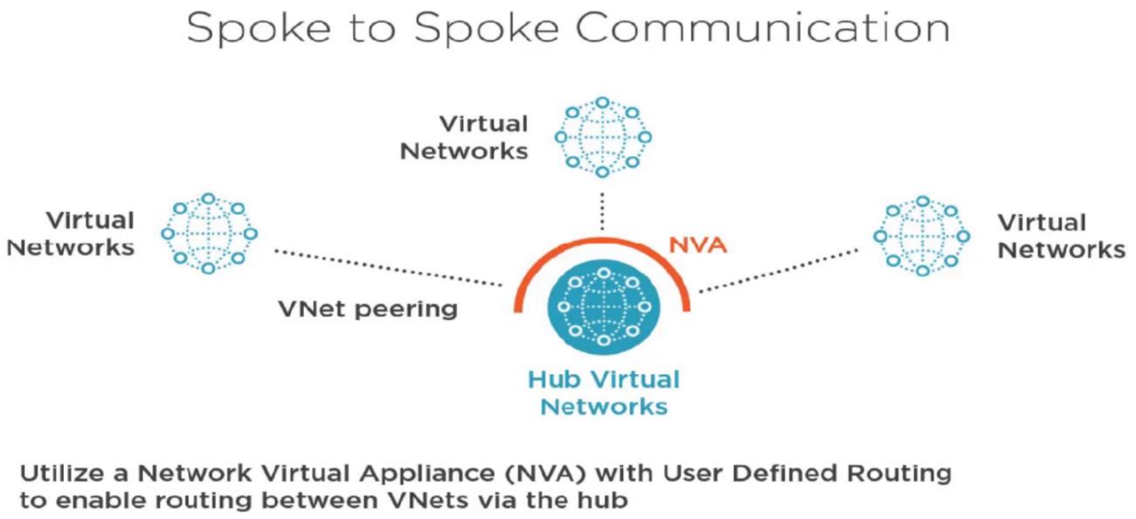


Common Network Peering Architecture



Spoke to Spoke Communication

Create a mesh using VNet peering so every VNet peers with every other
Does every VNet really require communication to every VNet?



Spoke to Spoke Communication

Utilize a Network Virtual Appliance (NVA) with User Defined Routing to enable routing between VNets via the hub

Routing between Azure and on-premises

- Must use unique IP address ranges
- It is not possible to route between networks that use the same IP scheme
- Includes on-premises to Azure
- Azure Vnet to Azure Vnet
- VMs cannot be moved between virtual networks without deleting and recreating
- Get the virtual networks right first time

Types of peering

- Site to site VPN is private peering connecting to a virtual network which is available with ExpressRoute
- ExpressRoute also supports Microsoft peering
- Microsoft peering provides access to nearly all Azure, office and Dynamics services via ExpressRoute instead internet. Premium required for office/Dynamics

Azure VPN Gateway

Used to send encrypted traffic between an azure virtual network and on-prem location over the internet

Can also be used between azure virtual networks

- Encrypted traffic across the azure platform

Connects with azure validated devices

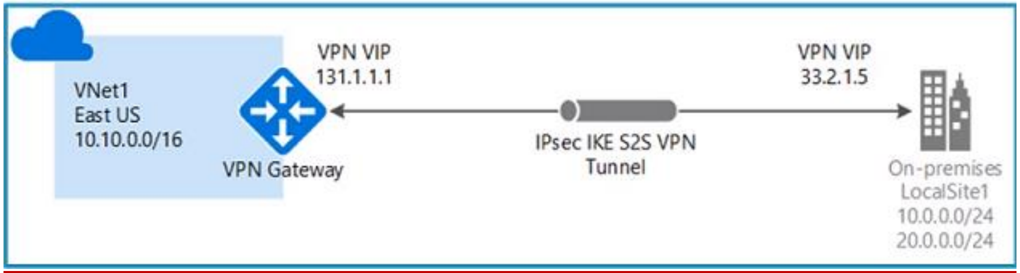
Types of VPN Gateway

- IPSEC is computationally expensive which limits bandwidth
  Four SKUs of gateway
  - Basic -100 Mbps - VpnGw1 – 500 Mbps
  - VpnGw2 -1 Gbps - VpnGw3 – 1.25 Gbps

- Latency will depend on many factors but expect inconsistency
- Basic support 10 tunnels while others support 30
- There are also old SKUs of standard and high performance
- Traffic outside the region/ datacenter would result in egress traffic charges
- Use network peering if possible instead

Point-to -Site VPN

- Allows connection from individual computer to VMs on Azure
- Computers can be on any network that connects to the internet
- SSTP VPN (secure socket tunneling protocol)
- Uses certificate authentication
- Upload root certificate to Azure
- Install client certificate on computers that will use point -to -site VPN client



Site -to -Site VPN

- Used for connecting on-premises network to Azure networks
- Provides connectivity between a virtual network and an on-premises network or another virtual network
- To on-premises connects over the internet
- Virtual networks can be in different regions and different subscription
- Uses IPsec/IKE to encrypt the traffic.
- Allow bi-directional communication between Azure and connected site
- Allows extension of on-premises network into Azure without making resources accessible to host on the internet
- Requires compatible of on-premises routing device
- Templets available for commonly used routers / internet gateways
- Ensure that Azure address space does not overlap on-premises address space
- IPsec VPN
- Azure side VPN gateway requires its own subnet
- Common when creating subnet in new virtual network is to leave an address space at the start to use for the gateway
- Don not use NSG with the gateway subnet

Azure Virtual WAN

- For origination with large number of branches locations providing connectivity between them can be complex
- Azure virtual WAN provides an Azure-based hub services that eases the setup and connectivity
- Remote offices connect via active-active tunnels over an IPsec encrypted VPN connection
- Connectivity is provided between locations and Azure connected virtual networks

Site – to- Site VPN challenges

- It uses the internet
- Bandwidth
- Unpredictable latency
- Security may not meet requirements
- Potentially greater networking cost

ExpressRoute

ExpressRoute is an Azure service that lets you create private connections between Microsoft datacenters and infrastructure that's on your premises or in a colocation facility. ExpressRoute connections do not go over the public Internet, and offer higher security, reliability, and speeds with lower latencies than typical connections over the Internet.Up to 10GB/sec

  - Redundant connection
  - Predictable performance
  - Hight throughput
  - SLA
- Traffic does not flow across public internet
- Requires that ExpressRoute available locally
  - Exchange provider facility
  - Direct connection using network services provider (point -to-point ethernet)
  - Any-to-Any (IPVPN) connection (Network service provider)
- Provides layer 3 connectivity from your location to Azure over the private connection
- Does NOT use the internet so does not need to encrypt

- Uses BGP for routing enabling forced tunneling
- Care should be structured as if all traffic is forced through customer location; that would include access to other Azure services like storage
- Rules should be structured so that Azure services (Microsoft peering) still route via Azure backbone and not via on-premises location unless this is specifically desired
- No encryption required with ExpressRoute
- For SKU of gateway
  Basic -500 Mbps (deprecated)
  Standard -1000 Mbps
  High Performance 2000 Mbps
  Ultra-performance – 9000 Mbps

- **Unlimited data.** Billing is based on a monthly fee; all inbound and outbound data transfer is included free of charge.
- **Metered data.** Billing is based on a monthly fee; all inbound data transfer is free of charge. Outbound data transfer is charged per GB of data transfer. Data transfer rates vary by region.
- **ExpressRoute premium add-on**. ExpressRoute premium is an add-on to the ExpressRoute circuit. The ExpressRoute premium add-on provides the following capabilities:

  - Increased route limits for Azure public and Azure private peering from 4,000 routes to 10,000 routes.
  - Global connectivity for services. An ExpressRoute circuit created in any region (excluding national clouds) will have access to resources across any other region in the world. For

example, a virtual network created in West Europe can be accessed through an ExpressRoute circuit provisioned in Silicon Valley.

  - Increased number of VNet links per ExpressRoute circuit from 10 to a larger limit, depending on the bandwidth of the circuit.

Route Filters

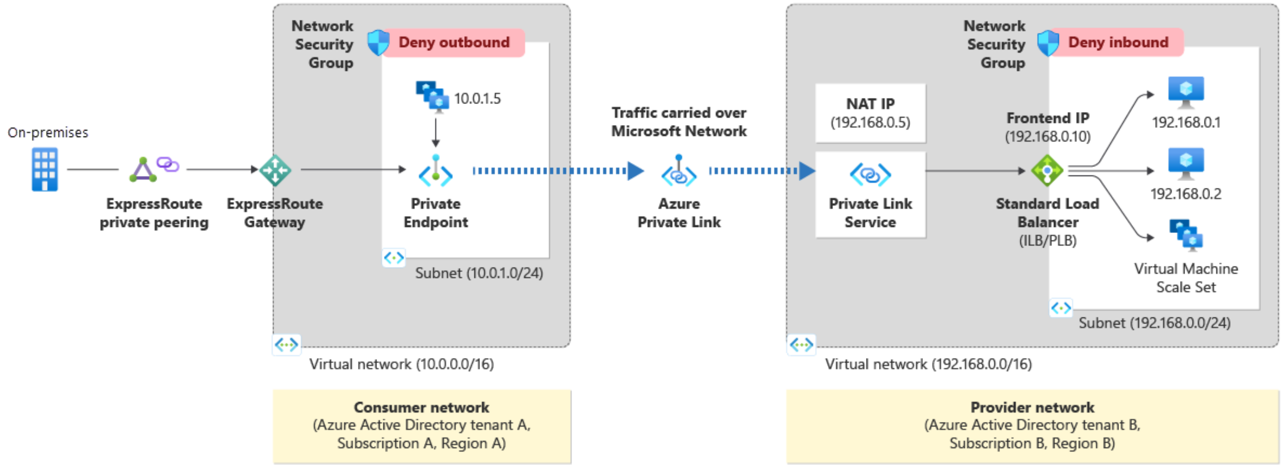
- Origination may not want all services advertised via ExpressRoute
- Route filters enable control of certain services based on BGP community value, e.g. Exchange
- Azure services by region can also be controlled via route filters

Connecting Azure Vnets with ExpressRoute

- Multiple virtual networks are automatically connected by connecting them to the same ExpressRoute
- Standard ExpressRoute supports connecting any in the same geo-political boundary e.g any US region
- ExpressRoute premium support connecting any globally
- Communications are via the peering point so that should be considered carefully as it may increase latency compared to other options, i.e. network peering

Azure Private Link

Azure Private Link service is the reference to your own service that is powered by Azure Private Link. Your service that is running behind Azure Standard Load Balancer can be enabled for Private Link access so that consumers to your service can access it privately from their own VNets. Your customers can create a private endpoint inside their virtual network and map it to this service. This article explains concepts related to the service provider side.



Private Endpoint

- A private endpoint is a network interface that uses a private IP address from your virtual network. This network interface connects you privately and securely to a service that is powered by Azure Private Link. By enabling a private endpoint, you are bringing the service into your virtual network.

The service could be an Azure service such as:

- Azure Storage
- Azure Cosmos DB
- Azure SQL Database

Service Endpoints

- Service Endpoints enables private IP addresses in the VNet to reach the endpoint of an Azure service without needing a public IP address on the VNet. Microsoft recommends use of Azure Private Link and private endpoints for secure and private access to services hosted on the Azure platform.

Network Monitoring Requirements

- In Azure the network fabric is the responsible of Microsoft, so no monitoring of physical infrastructure is required.
- Even with Azure IaaS VMs there is no access to the underlying network fabric
- This means no fabric level monitoring tools can be used
- Any agent can run with in the VM to examine local traffic and pass details to a target
- No network monitoring in promiscuous mode will work

Azure Monitor

- A single source for the monitoring of Azure resource
- Provide insight into log metric alerts
- Can create action groups which can be utilized as part of alerts to perform multiple actions centrally defined

Azure Network Watcher

- An instance is deployed to a region for services in that region
- Large number of capabilities
- Topology viewer
- Packet capture (Via an agent installed into VM)
- IP flow verify and next hop determination
- Connection monitor and troubleshoot
- Security group viewer
- NSG flow logging

- Virtual network gateway and virtual network connection troubleshooting
- Network use against subscription limits
- Enable or disable log for resource for virtual network

Hub-spoke network topology

This reference architecture shows how to implement a hub-spoke topology in Azure. The hub is a virtual network in Azure that acts as a central point of connectivity to your on-premises network. The spokes are virtual networks that peer with the hub, and can be used to isolate workloads. Traffic flows between the on-premises datacenter and the hub through an ExpressRoute or VPN gateway connection

The benefits of this topology include:

Cost savings by centralizing services that can be shared by multiple workloads, such as network virtual appliances (NVAs) and DNS servers, in a single location.

Overcome subscriptions limits by peering virtual networks from different subscriptions to the central hub.

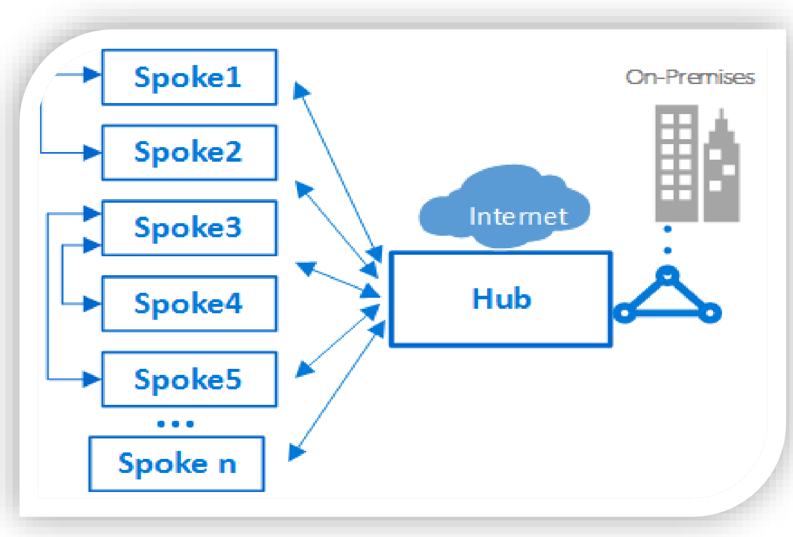
Separation of concerns between central IT (SecOps, InfraOps) and workloads (DevOps).

Typical uses for this architecture include:

Workloads deployed in different environments, such as development, testing, and production, that require shared services such as DNS, IDS, NTP, or AD DS. Shared services are placed in the hub virtual network, while each environment is deployed to a spoke to maintain isolation.

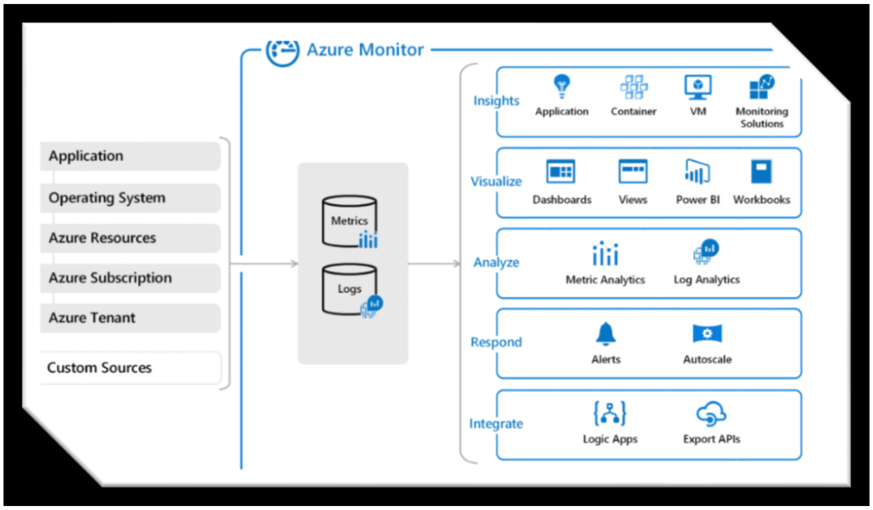
Workloads that do not require connectivity to each other, but require access to shared services.

Enterprises that require central control over security aspects, such as a firewall in the hub as a DMZ, and segregated management for the workloads in each spoke.



Azure Monitoring

Azure Monitor is the service offered by Microsoft that helps in analyzing, collecting and telemetry data on on-premise and cloud environment. The major advantage of Azure Monitoring is that it helps in identifying the issues in a split of a second. It also helps in improving the performance. Azure Monitor is the local monitoring solution for Azure, and when we are using Azure or doing anything, it is present in the background collecting data for you. Metrics and logs are collected by Azure monitor from all your Azure resources and used to create alerts, monitor, troubleshoot issues, performance and create dashboards so that you have full visibility of your Azure estate and a means to act when problems arise



Metrics
Logs
Health
Service events

Log Analytics

Log analytics part of Azure Monitor, is a log collection and search service hosted in Microsoft azure.

Azure Diagnostics

Windows Azure Diagnostics enables you to collect diagnostic data from an application running in Windows Azure. You can use diagnostic data for debugging and troubleshooting, measuring performance, monitoring resource usage, traffic analysis and capacity planning, and auditing.

Azure Application Insights

Application Insights, a feature of Azure Monitor, is an extensible Application Performance Management (APM) service for developers and DevOps professionals. Use it to monitor your live applications. It will automatically detect performance anomalies and includes powerful analytics tools to help you diagnose issues and to understand what users actually do with your app.

CDN (Content Delivery Network):

It is used for the delivery of the contents stored in the storage account.

We can use a content delivery network to reduce the latency of the delivery.

We'll create a CDN endpoint near to the users to reduce the latency.

Azure Storage

Azure storage provides storage that is highly available, secure, durable, scalable and redundant.

Azure Storage options:

- **General purpose V2 (GPv2)**
  - Accounts provide all the latest features, and supports blobs, files, Queues, and tables
  - This include blob- level tiering, archive storage, higher scale account limits, and storage events.
  - For block blobs, you can choose between hot and cool storage tires at the account level, or hot, cool, and archive tires at the blob level based on access patterns.
  - Storage frequently, infrequently and rarely accessed data in the hot, cool, and archive storage tiers respectively to optimize cost.
  - Importantly, and GPv1 account can be upgrade to GPv2 account in the portal, CLI or PowerShell.
- **General purpose V1 (GPv1)**
  Account provide use of all azure storage services but may not have the latest features or the lowest GB pricing.
  For example, cool and archive storage are not supported in GPv1
- **Blob Storage**
  Account provide all the latest features for block blobs, but only support block blobs

Azure Storage: pricing
All storage accounts use a pricing model for blob storage based on the tire or each blob

- When using a storage account, that following billing consideration apply:
- **Storage Costs**
  - The cost of storing data varies depending on the storage tier
  - The per-gigabyte cost decreases as the tire gets cooler
- **Data access costs**
  - Data access charges increase as the tire gets cooler
  - For data in the cool and archive storage tier, you are charged a per-gigabyte data access charged for reads.
- **Transaction cost**
  - There is a per-transaction charge for all tires
- **Geo-replication data transfer costs**
  - This only applies to accounts with geo-replication configured, including GRS and RA-GRS.
  - GEO-replication data transfer incurs a per gigabyte charge

Azure Storage: Security

- Azure storage provides a comprehensive set of security capabilities.
- The storage account itself can be secured using role-based access control and azure active directory
- Data can be secured in transit between an application and azure by using client-side encryption, HTTPS, or SMB 3.0
- Data can be set to be automatically encrypted when written to azure storage using storage service encryption. SSE is at storage level
- OS and data disk used by virtual machine can be set to be encrypted using Azure disk encryption. ADE is more like OS level encryption
- Delegate access to the data objects in azure storage can be granted using shared access signature

Azure Disks

A data disk is a VHD that's attached to a virtual machine to store application data, or other data you need to keep. Data disks are registered as SCSI drives and are labeled with a letter that you choose. Each data disk has a maximum capacity of 4,095 GB, managed disks have a maximum capacity of 32,767 GiB. The size of the virtual machine determines how many data disks you can attach to it and the type of storage you can use to host the disks.

Azure creates an operating system disk when you create a virtual machine from an image. If you use an image that includes data disks, Azure also creates the data disks when it creates the virtual machine. Otherwise, you add data disks after you create the virtual machine.

You can add data disks to a virtual machine at any time, by **attaching** the disk to the virtual machine. You can use a VHD that you've uploaded or copied to your storage account or use an empty VHD that Azure creates for you. Attaching a data disk associates the VHD file with the VM by placing a 'lease' on the VHD so it can't be deleted from storage while it's still attached.

Unmanaged Disks

Unmanaged disks are the traditional type of disks that have been used by VMs. With these disks, you create your own storage account and specify that storage account when you create the disk. Make sure you don't put too many disks in the same storage account, because you could exceed the scalability targets of the storage account (20,000 IOPS, for example), resulting in the VMs being throttled. With unmanaged disks, you must figure out how to maximize the use of one or more storage accounts to get the best performance out of your VMs.

Managed Disks

Managed Disks handles the storage account creation/management in the background for you and ensures that you do not have to worry about the scalability limits of the storage account. You simply specify the disk size and the performance tier (Standard/Premium), and Azure creates and manages the disk for you. As you add disks or scale the VM up and down, you don't have to worry about the storage being used.

Managed Disks	Unmanaged Disks
• Up to 1000 storage accounts per region	• Up to 200 storage accounts per region
• Storage accounts performance limits not relevant.	• Up to 40 disks per standard storage accounts.
• Disks of VMs in the same availability set in the different stamps	• Storage accounts per VMs in the same availability set might be in the same storage stamp
• A custom image must be in the same region as VM disks	• A custom image must be in the same storage account as VM disk
• Simple and scalable VM deployment	
• Better reliability for Availability Sets	
• Highly durable and available • Granular access control • Azure Backup service support	

Standard HDD disks

Standard HDD disks are backed by HDDs and deliver cost-effective storage. Standard HDD storage can be replicated locally in one datacenter or be geo-redundant with primary and secondary data centers. For more information about storage replication, see Azure Storage replication.

Standard SSD disks

Standard SSD disks are designed to address the same kind of workloads as Standard HDD disks, but offer more consistent performance and reliability than HDD. Standard SSD disks combine elements of Premium SSD disks and Standard HDD disks to form a cost-effective solution best suited for applications like web servers that do not need high IOPS on disks. Where available, Standard SSD disks are the recommended deployment option for most workloads. Standard SSD disks are available as Managed Disks in all regions but are currently only available with the locally redundant storage (LRS) resiliency type

Premium SSD disks

Azure Premium Storage delivers high-performance, low-latency disk support for virtual machines (VMs) with input/output (I/O)-intensive workloads. VM disks that use Premium Storage store data on solid-state drives (SSDs). To take advantage of the speed and performance of premium storage disks, you can migrate existing VM disks to Premium Storage.

Azure Storage: Tiers

- **Premium storage (preview)** provides high performance hardware for data that is accessed frequently.
- **Hot storage**: is optimized for storing data that is accessed frequently.
- **Cool storage** is optimized for storing data that is infrequently accessed and stored for at least 30 days.
- **Archive storage** is optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

Disk Type	**Premium SSD**	**new Standard SSD**	**Standard HDD**
Summary	Designed for IO intensive enterprise workloads. Delivers consistent performance with low latency and high availability.	Designed to provide consistent performance for low IOPS workloads. Delivers better availability	Optimized for low-cost mass storage with infrequent access. Can exhibit some variability in performance.

		and latency compared to HDD Disks.	
Workload	Demanding enterprise workloads such as SQL Server, Oracle, Dynamics, Exchange Server, MySQL, Cassandra, MongoDB, SAP Business Suite, and other production workloads	Web servers, low IOPS application servers, lightly used enterprise applications, and Dev/Test	Backup storage
Max IOPS	7,500 IOPS provisioned	Up to 500 IOPS	Up to 500 IOPS
Max Throughput	250 MBPS provisioned	Up to 60 MBPS	Up to 60 MBPS

Azure Storage: Tiers

Premium storage (preview) provides high performance hardware for data that is accessed frequently.

Hot storage: is optimized for storing data that is accessed frequently.

Cool storage is optimized for storing data that is infrequently accessed and stored for at least 30 days.

Archive storage is optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours).

Storage Account

Azure storage or azure account is a service from Azure, which provides storage service for various use case. Azure storage is the cloud solution for modern application that rely on durability, availability and scalability to meet the needs of their customers.

- An azure storage account provides a unique namespace to store and access your Azure storage data object
- In order to use Azure Storage, you begin by creating a storage account.
- You can create many storage accounts within a single Azure subscription.
- Each storage account can contain up to 500 TB of data.
- For each storage account, you must specify:
  URL
  Location or Affinity Group
  Replication

http(s)://account_name.file.core.windows.net

Storage Replication

Locally – Redundant storage (LRS)- Synchronously replicates data to three disks within a data center in the primary region. Offers a moderate level of availability at a lower cost

Zone – Redundant storage (ZRS) - Synchronously replicates data among three Azure availability zones in the primary region. Provides a higher level of resilience at higher cost.

Geo – Redundant storage (GRS) - GRS provides additional redundancy for data storage compared to LRS or ZRS. In addition to the three copies of data stored in one region, there are three copies stored in a paired Azure region

Read Access Geo – Redundant storage (RA-GRS)- Same as GRS, but allows data to be read from both azure regions

Object Replication for Block Blob Storage — a special type of replication used only for block blobs, replicating them between a source and target storage account.

Blob: (Binary Large Objects)

<File Name>.blob.core.windows.net

- Azure Blob Storage is a service for storing large amount of unstructured object data, such as text or binary data.
- Blob storage can any type of text or binary data, such as a document, media files or application installer.
- You can use blob storage to expose data publicly to the world, or to store application data privately.
- Blob storage is also referred to as object storage.

- You can create any number of containers within a single storage account.
- Within each container, you can store any number of blobs up to the 500 TB limit. File, document, image, video, VM disk, database, etc.

Container

- A container provides a grouping of a set of blobs
- All blobs must be in a container
- An account can contain an unlimited number of containers
- A container can store an unlimited number of blobs

Tiers

- **Hot storage**: is optimized for storing data that is accessed frequently. Higher Storage cost, Lower Transition cost
- **Cool storage** is optimized for storing data that is infrequently accessed and stored for at least 30 days. Lower transition cost, higher transition cost
- **Archive storage** is optimized for storing data that is rarely accessed and stored for at least 180 days with flexible latency requirements (on the order of hours). Lower transition cost, higher transition cost

Blob

- A file of any type and size.
- Azure storage offers three types of blobs

Block Blob

- Used for storing text or binary files, such as documents and media files.
- Each block can be a different size, up to a maximum of 100 MB.
- A single block blob can contain up to 50,000 blocks. Individual blocks bobs can be up to 4.75 TB in size (100MBx 50,000)
- With a block blob, you can upload multiple blocks in parallel to decrease upload time.

Append Blob

- Each block in an append blob can be a different size, up to a maximum of 4 MB
- are made up of blocks like block blobs, but are optimized for append operations. Append blobs are ideal for scenarios such as logging data from virtual machines.
- A single append blob can contain up to 50,000 blocks for a total size of slightly more than 195GB (4MB x 50,000)

Page Blob

- store random access files up to 8 TB in size. Page blobs store virtual hard drive (VHD) files and serve as disks for Azure virtual machines.
- Page blob are a collection of 512-byte pages optimized for random read and write operations
- Can be up to 8 TB in size, and are more efficient for frequent read/write operations

You can interact with Blob Storage through any of the below

AzCopy – a command-line interface to be downloaded locally
Azure Data Factory
Azure SDKs (.NET, Java, Python etc.) – allowing you to interact with Azure Storage directly within Python or R
Azure Data Box Disk
Azure Import/Export service

Queue

- Azure Queue Storage is service for storing large number of **Messages** that can be accessed from anywhere in the world via authenticated call using HTTP or HTTPS.
- The azure queues storage service provides temporary messaging store.
- A single queue message can be up to 64KB in size, and queue can contain millions of messages, up to total capacity limits of a storage account.
- Queue Storage enables messages queueing for large workloads in simple, cost-effective and durable manner

What are the advantages of Azure Queue storage?

- Enables users to build flexible apps and separate functions for greater durability
- It provides rich client libraries for java, Android, C++, PHP, Ruby, Etc.
- Ensures users' applications are scalable and less prone to individual component failure.
- Enables queue monitoring to ensure servers aren't overwhelmed by sudden traffic

https://<storage.account>.queue.core.windows.net/queue

File System

- Azure files offer fully managed file shares in the cloud that are accessible via common internet file system (CIFS)
- Azure file shares can be mounted concurrently by cloud or on-premises deployment of windows, linux, and macOS
- up to the 5TB total capacity of the file share.
- A file storage share is an SMB file share in Azure.
- All directories and files must be created in a parent share.
- Azure storage account can store multiple shares with a total of 500 TiB stored across all shares.
  - **Azure files support two data redundancy options:**
    LRS
    GRS
  - **Replace or supplement on-premises file servers**
  - Azure file can be used to completely replace or supplement traditional on-premises file servers or NAS

- **“Lift” and “Shift” applications**

– Azure files make it easy to “lift and shift” application to the cloud that expect a file share to store files applications or user data.

Azure files data access method

Azure files offer two data access methods that you can use separately, or in combination with each other to access your data:

Direct cloud Access:

Azure file share can be mounted by windows, macOS and/or linux.

Azure file Sync:

With azure file sync, shares can be replicated to windows server on-premises or in azure.
Users would access the file share through the windows server
Data may be replicated between multiple windows server endpoints.
Data tired to azure files, but the server does not have a full copy of the data
Rather, data is seamlessly recalled when opened by your user.

<File Name>.file.core.windows.net

Tables

- The Azure table storage service to store large amount of structure data stores partially.
- With each storage account, you can create multiple tables, and each table can contain multiple entities.
- The Service is a No SQL data store which accepts authenticated calls from inside and outside the Azure cloud,
- Azure tables are ideal for storing structured, non-relations data.
- Developers can use table storage as the back-end data store for websites, mobile apps, PaaS cloud services, and other types of solution

<File Name>.table.core.windows.net

Data transfer

Azure Data Box family for offline transfers

Azure Data Box family for offline transfers – Use devices from Microsoft-supplied Data Box devices to move large amounts of data to Azure when you're limited by time, network availability, or costs. Copy on-premises data using tools such as Robocopy. Depending on the data size intended for transfer, you can choose from Data Box Disk, Data Box, or Data Box Heavy.

Azure Import/Export –

Use Azure Import/Export service by shipping your own disk drives to securely import large amounts of data to Azure Blob storage and Azure Files.

This service can also be used to transfer data from Azure Blob storage to disk drives and ship to your on-premises sites.

High network bandwidth (1 Gbps - 100 Gbps)

If the available network bandwidth is high, use one of the following tools.

AzCopy - Use this command-line tool to easily copy data to and from Azure Blobs, Files, and Table storage with optimal performance. AzCopy supports concurrency and parallelism, and the ability to resume copy operations when interrupted.

Azure Storage REST APIs/SDKs – When building an application, you can develop the application against Azure Storage REST APIs and use the Azure SDKs offered in multiple languages.

Azure Data Box family for online transfers – Data Box Edge and Data Box Gateway are online network devices that can move data into and out of Azure. Use Data Box Edge physical device when there is a simultaneous need for continuous ingestion and pre-processing of the data prior to upload. Data Box Gateway is a virtual version of the device with the same data transfer capabilities. In each case, the data transfer is managed by the device.

Azure Data Factory – Data Factory should be used to scale out a transfer operation, and if there is a need for orchestration and enterprise grade monitoring capabilities. Use Data Factory to regularly transfer files between several Azure services, on-premises, or a combination of the two. with Data Factory, you can create and schedule data-driven workflows (called pipelines) that ingest data from disparate data stores and automate data movement and data transformation.

Azure Data Box family for online transfers - Data Box Edge and Data Box Gateway are online network devices that can move data into and out of Azure. Data Box Edge uses artificial intelligence (AI)-enabled Edge compute to pre-process data before upload. Data Box Gateway is a virtual version of the device with the same data transfer capabilities.

Scripting/programmatic tools such as AzCopy/PowerShell/Azure CLI and Azure Storage REST APIs.

AzCopy - Use this command-line tool to easily copy data to and from Azure Blobs, Files, and Table storage with optimal performance. AzCopy supports concurrency and parallelism, and the ability to resume copy operations when interrupted.

Azure PowerShell - For users comfortable with system administration, use the Azure Storage module in Azure PowerShell to transfer data.

Azure CLI - Use this cross-platform tool to manage Azure services and upload data to Azure Storage.

Azure Storage REST APIs/SDKs – When building an application, you can develop the application against Azure Storage REST APIs/SDKs and use the Azure client libraries offered in multiple languages.

Azure File Sync

Use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms Windows Server into a quick cache of your Azure file share. You can use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS. You can have as many caches as you need across the world.

Direct mount of an Azure file share: Since Azure Files provides SMB access, you can mount Azure file shares on-premises or in the cloud using the standard SMB client available in Windows, macOS, and Linux. Because Azure file shares are serverless, deploying for production scenarios does not require managing a file server or NAS device. This means you don't have to apply software patches or swap out physical disks.

Cache Azure file share on-premises with Azure File Sync: Azure File Sync enables you to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure File Sync transforms an on-premises (or cloud) Windows Server into a quick cache of your Azure file share.

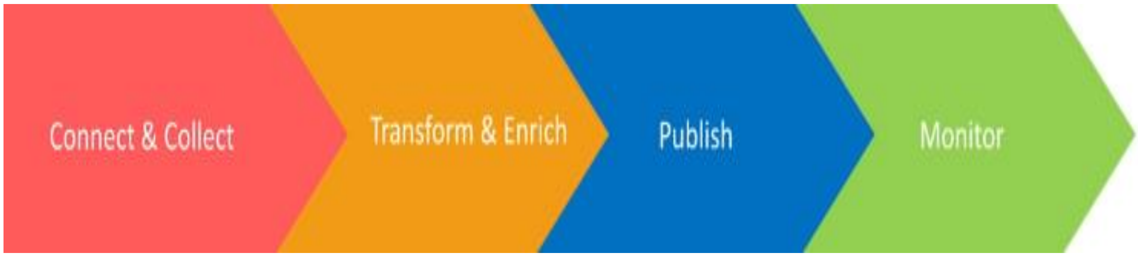
Azure Data Factory

- Modern data handling requires you to move from on premise DB to cloud DW
- This Data needs processing and goes through a series of steps, making the process tedious
- Data Factory: helps you automate this process and thus serve the cause

It is a **cloud-based data integration service** that allows to create data-driven workflows in the cloud for orchestrating and automating data movement and transformation.

Using azure data factory, you can create and schedule data-driven workflow (called pipeline) that can ingest data from disparate data stores.

It can process and transform the data by using compute service such as azure HDinsight Hadoop, spark, Azure data lake Analytics, and Azure machine learning.



Data factory concepts

Pipeline: A pipeline is a logical grouping of activities that performs a unity of work
Activity: Activities represent processing step in a pipeline
Is step or task such as copying data in pipeline. Three types

- Data Movement activities
- Data Transformation activities
- Control activities

Dataset: datasets represent data structure within the data stores
Linked Services: information needed to connect to external sources
Gateway: connects your on-premises data to cloud
Data Lake: it is an enterprise wide hyperscale repository for big data analytics workload. Azure data lake holds data of any size, type and allows you to do operational and exploratory analytics.
Key:
Analytics on data of any size
All users productive on day one
Ready for your enterprise
Types of Data Stored:
Structured data
Semi structured data
Unstructured data

Microsoft Azure Site Recovery tool changed to Azure Migrate

Microsoft Azure Site Recovery

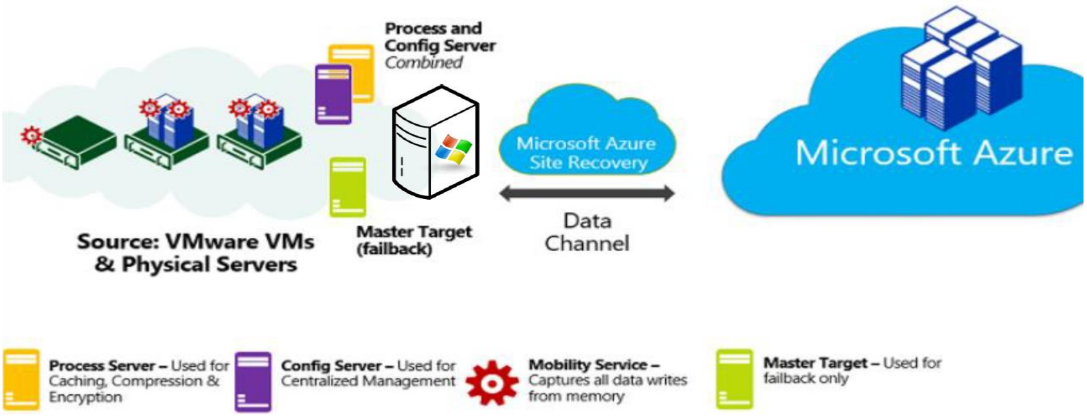
Microsoft link

As an organization you need to adopt a business continuity and disaster recovery (BCDR) strategy that keeps your data safe, and your apps and workloads up and running, when planned and unplanned outages occur.

- Site Recovery service: Site Recovery helps ensure business continuity by keeping business apps and workloads running during outages. Site Recovery replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location. When an outage occurs at your primary site, you fail over to secondary location, and access apps from there. After the primary location is running again, you can fail back to it.
- Backup service: The Azure Backup service keeps your data safe and recoverable by backing it up to Azure

How site recovery work

Replicating Azure, VMware, Hyper-V, VM's and physical servers
Leveraging existing HA/DR options
Working with the ASR deployment planner
BC/DR
Continue replication
APP-consistent snapshot
Flexible failovers
Recovery plans
Azure Automation integration
Creating recovery vault


Process and Config Server Combined
Microsoft Azure Site Recovery
Data Channel
Microsoft Azure
Source: VMware VMs & Physical Servers
Master Target (failback)
Process Server – Used for Caching, Compression & Encryption
Config Server – Used for Centralized Management
Mobility Service – Captures all data writes from memory
Master Target – Used for failback only

Extension Mobility Service

- It is going to read the data from RAM, when there is a write to ram it will send the data from physical machine/ VMWare server to process server
- Coordinates replication between on-premises VMware servers/physical servers and Azure/secondary site
  Installed on VMware VM or physical servers you want to replicate

Process server component

- Used for caching, compressing, and encryption.
- Used for caching, compression & encryption followed by pushing the data into storage
- Installed by default on the configuration server. It receives replication data; optimizes it with caching, compression, and encryption; and sends it to Azure Storage. As your deployment grows, you can add additional, separate process servers to handle larger volumes of replication traffic

Configuration server component

- Used for centralized management, Master target server component
- This will have the configuration of all the physical server. Used for centralized management. Install the mobility service on target systems
- Coordinates communications between on-premises VMware servers and Azure

Master Target Server – Used for fail back to on premise infra

https://docs.microsoft.com/en-us/azure/site-recovery/site-recovery-plan-capacity-vmware

QUESTIONS AND ANSWERS

https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-common-questions

https://docs.microsoft.com/en-us/azure/site-recovery/vmware-azure-deploy-configuration-server#prerequisites

Azure API

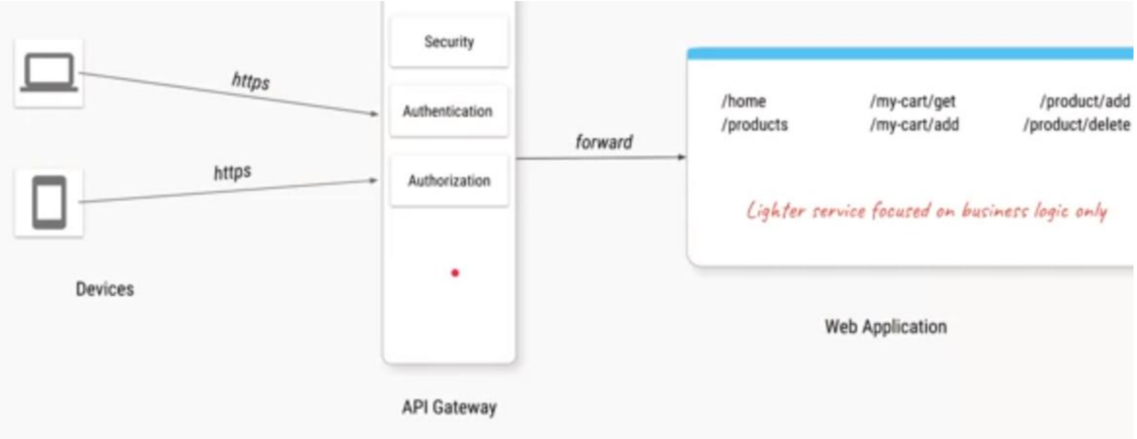
Azure API Apps, a key component of the **Azure** App Services suite, are more than just a way to organize your **APIs**. **API** Apps make it easy to develop, host, and consume **APIs** in the cloud or on-premises while leveraging the magic of **Azure** App Services to include features such as discovery and authentication.

Manage all your APIs in one place

API Gateway

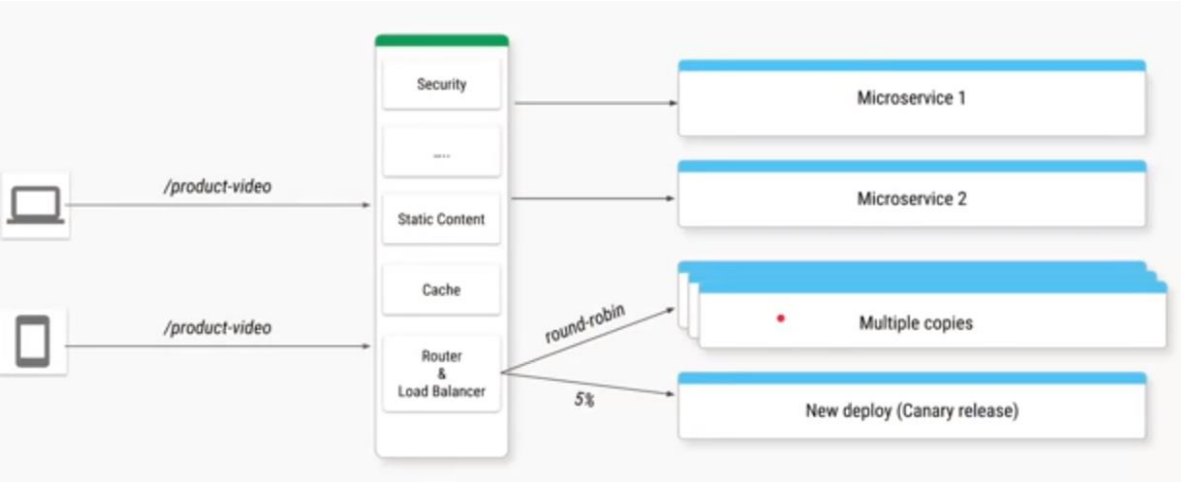
Feature#1 Separate out cross cutting concerns

- Authentication
- Authorization
- SSL termination
- DDoS protection / Throttling



Feature#2 Separate and consolidate cross cutting concerns across microservices

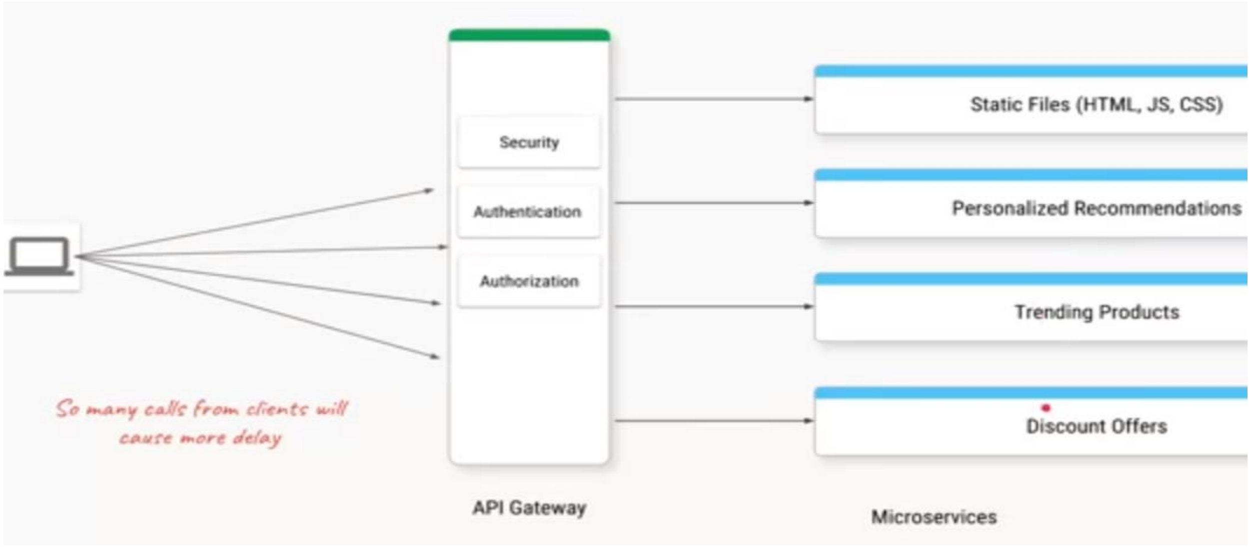
- Authentication
- Authorization
- SSL termination
- DDoS protection / Throttling
- Routing

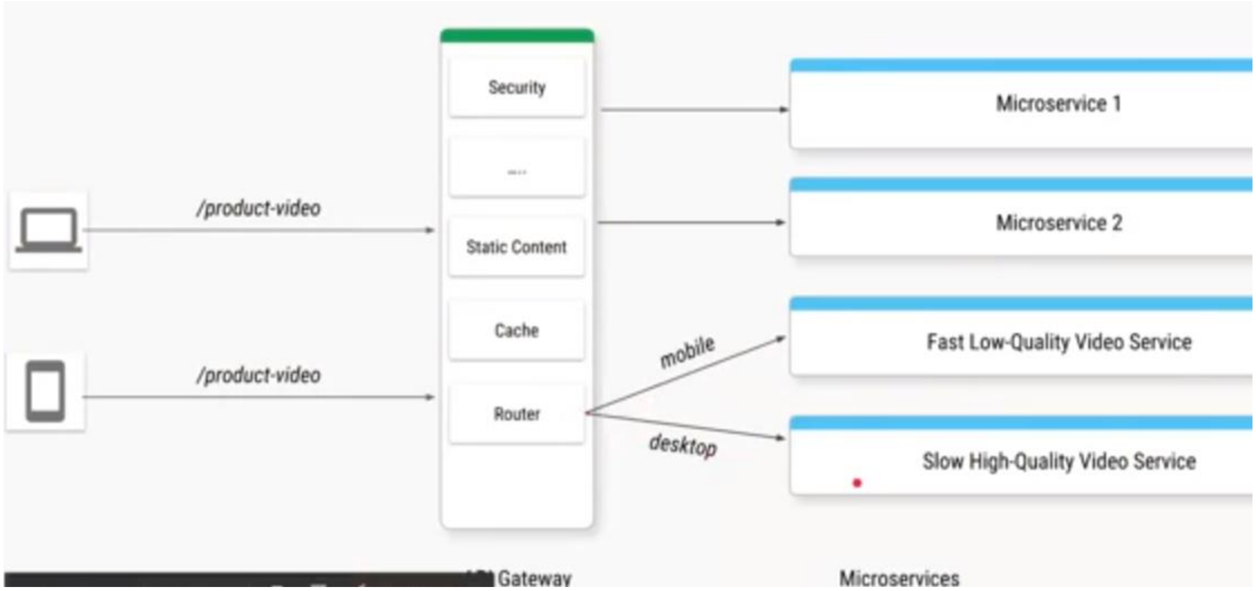


Feature#3 Replacing multiple clients calls with single API call

Also, some features of revers proxy

- Serving static content
- Caching responses

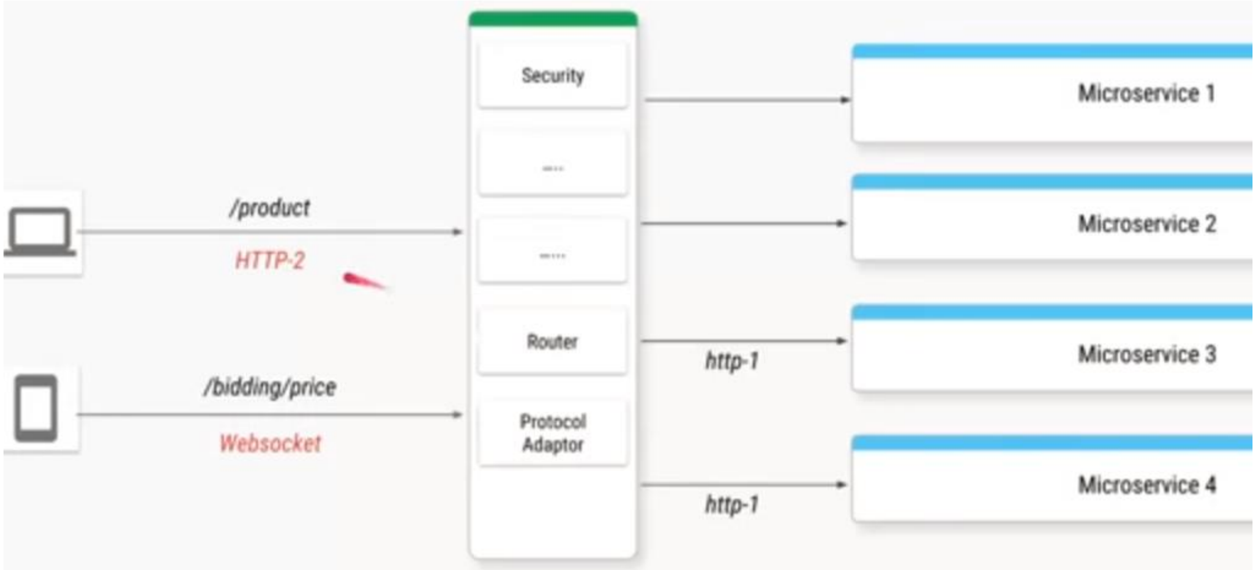

Security
Authentication
Authorization
Static Files (HTML, JS, CSS)
Personalized Recommendations
Trending Products
Discount Offers
So many calls from clients will cause more delay
API Gateway
Microservices



Feature4# Routing based on headers, paths and params etc.

Also, Some features of load balancer component

- Load balancing
- A/B testing
- Canary releases



What is Azure Service Fabric?

Service fabric provides a platform that makes the process of developing microservices and managing application lifecycle easier

- Produce application with faster time to market
- Support windows/ linux, on-premises or other cloud
- Provides the ability to scale up to a thousand machines

Azure App Service?

Azure App Service is a fully managed "Platform as a Service" (PaaS) that integrates Microsoft Azure Websites, Mobile Services, and BizTalk Services into a single service, adding new capabilities that enable integration with on-premises or cloud systems. Azure App Service gives users several capabilities (see Figure 1):

- Provision and deploy Web and Mobile Apps in seconds
- Build engaging iOS, Android, and Windows apps
- Automate business processes with a visual design experience

- Integrate with "Software as a Service" (SaaS) applications (Office 365, Salesforce, Dynamics, OneDrive, Box, Dropbox, Twilio, Twitter, Facebook, Marketo, and so on) and on-premises applications

Azure Key Vault

Azure Key Vault is a tool for securely storing and accessing secrets. A secret is anything that you want to tightly control access to, such as API keys, passwords, or certificates. A vault is a logical group of secrets

Azure Key Vault is a cloud service that provides a secure store for secrets. You can securely store keys, passwords, certificates, and other secrets. Azure key vaults may be created and managed through the Azure portal. In this QuickStart, you create a key vault, then use it to store a secret