Availability

* A measure of system uptime for users and services

HA (High availability)

* Ensures system availability
* Little or no service disruptions

What HA is NOT…

* Backup or disaster recovery
* High performance
* Load balancing

Scale up

* Scale resource up or vertical scaling (adding more CPU/memory)
* Increase or decrease workload of current resources

Scaling out

* Increase amount of resources (cloning of resources or adding of instances)
* Horizontal scaling
* The preferred method of scaling in the cloud

Elasticity

* The automatic or automated scaling of resources
* The ability of the system to scale dynamically (both out to handle demand and back in to save $)

Agility

* Quickly respond to changes (on the cloud)
* Being able to allocate an de-allocate resources quickly

Fault Tolerance

* Ensures services are always up and running during component and service failures
* Cloud service providers have fault tolerance built in (datacenters in multiple regions)

Replication

* Copying data somewhere else
* 2 identical copies of your application with DNS routing so your users are automatically re-directed if any service fails

Disaster recovery

* The ability to recover from a failure
* Disaster recovery options for various services

Backups

* Allow us to access resources from previous points in time

Economics of scale

* Defines the cost of Azure services
* As the company grows in size, they can decrease price per unit for their customers
* Allow us to do more at a lower cost
* Cloud providers offer slices at a lower cost

CapEx vs OpEx models

CapEx

* Upfront costs
* Creates challenges for a new company or division
* Predictable fixed costs
* Value of assets decreases over time
* Resources can be a loss
* High maintenance

OpEx

* Ongoing billing costs
* Pay for the product as it is used
* Test before committing (buying)
* Great for agile environments where demand is unpredictable (seasonal)
* Can delete the resource when the task is done
* Minimal maintenance

Consumption based pricing model

* Used by cloud service providers
* Only pay for what is used
* No upfront costs
* Stop paying for service when no longer req’d (de-allocate resources - elasticity)
* Multiple pricing components per service
* Granular usage measurement

Spot Instance

* access unused Azure compute capacity at deep discounts
* up to 90 per cent compared to pay-as-you-go prices

Azure Calculator

* get pricing when you know exactly what you need in Azure specifically
* or want to look up pricing for the resources you know about.

TCO Calculator

* when you want to estimate how much it would cost to move your resources from on-premises to Azure, by inputting what you are currently using, and letting it convert that into Azure equivalence.

Reservation vs. Pay as you go

* Reserving is pre-paying for machines (subscription property)
* You get a discount for paying in advance on a 1 or 3 year reservation
* Not a locked in contract -- if you need to upgrade, no problem. But there is small fee if you need to decommission services all together (12% monthly)

Cloud service models - IaaS vs PaaS vs SaaS

BaaS = Backup as a Service

DaaS = Database as a Service

IDaas = Identity as a Service

OnPrem

* We are responsible for everything

IaaS

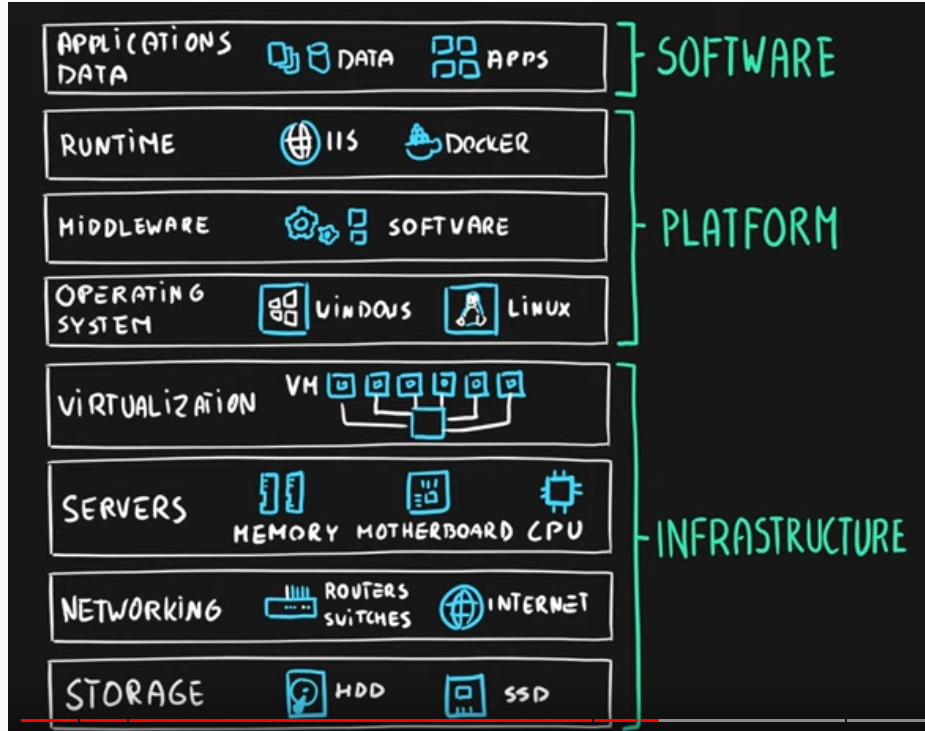
* Hosted by a cloud service provider
* Service provider is responsible for the infrastructure
* Customer is responsible for the OS, configuration and backups on the VMs
* Pay for what is used
* Hardware + virtualization
* the most flexible category of cloud services, gives you the most control
* Example use cases – migration of workloads, test & development, storage backup & recovery

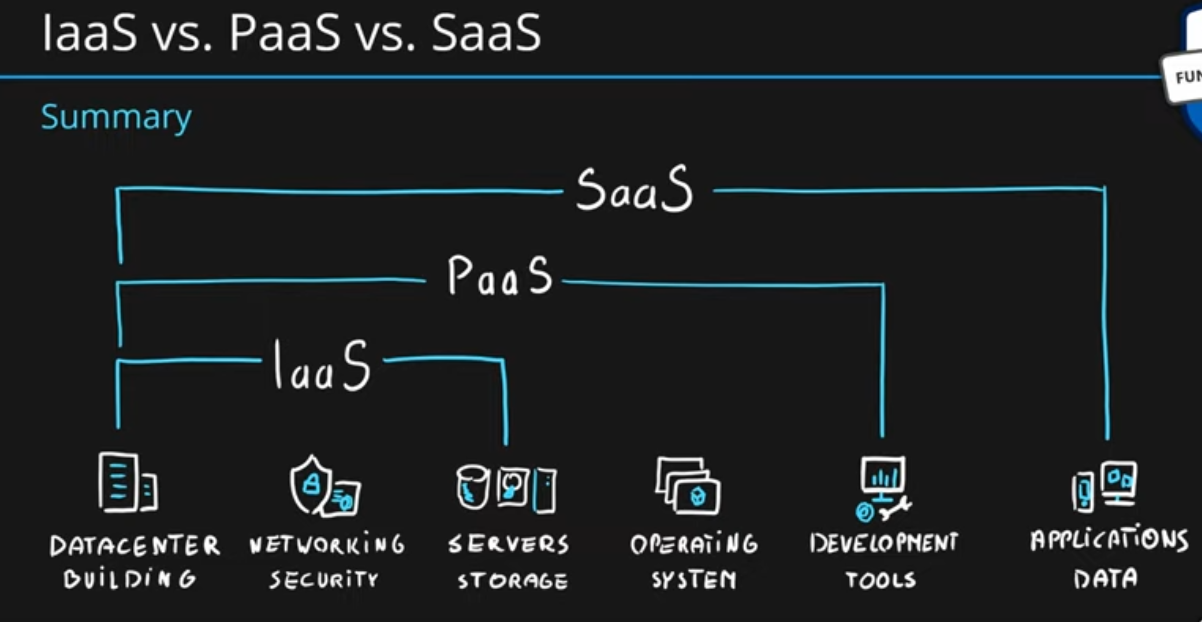
PaaS

* Prebuilt services by the service provider (web apps, db’s and analytics)
* Service provider is responsible for infrastructure, OSs, managements and backups
* Customers are responsible for the applications and data
* Use cases – dev framework, analytics & intelligence
* SQL dbs are a typical usage

SaaS

* Centrally hosted software by the cloud service provider
* Office 365 or gmail
* Typically requires a subscription
* The application and the data itself
* Use cases – buying of the shell apps
* SaaS apps are often run in the browser
* VMs virtualize the hardware
* Containers virtualize the OS





Cloud deployment models - Public, Private and Hybrid cloud models

* Public – Apartment
* Private – Home
* Hybrid – Condo

Private

* The organization owns and maintains the data center
* Responsible for everything
* Single client
* Advantage – control
* Disadvantage - CapEx

Public

* Service provider owns and maintains the data center
* They are responsible for everything
* Public access is allowed via internet
* Multiple clients share data centers
* Security and compliance can be a major disadvantage

Hybrid

* Combination of private and public cloud
* We can leverage the benefit of a public offering, including reduced costs.
* Separate the workloads between public and private
* Flexible

Azure Stack

* The onprem variant of Azure
* integrated hardware system
* Approved 3rd party vendors manage the hardware Dell, Lenovo, Cosco) and Microsoft manages the software
* Data transfer from on prem to Azure over VPN = $$$
* Data transfer from Azure to on prem over VPN = free
* Cloud bursting – when the private cloud exceeds capacity, resources are moved to the cloud

Data Center

* Physical infrastructure that holds servers
* Has its own power, cooling & networking infrastructure

Regions

* A group of one or more data centers that connected with low-latency network (<2ms)
* They are globally distributed
* Geographical area on the planet
* This is the location for your services
* Some services are available only in certain regions
* Some services are global services, and are not assigned in specific regions
* Over 50+ regions available

Geographies

* Ensures data residency and compliance boundaries are met
* Contains 2 or more regions
* Customer can select where data is stored
* 5 geographies total

Region pairs

* Every region has a region pair inside a geography (at least 300miles away)
* Regional pairs ensures only one region is updated at a time
* Ensures data resides in the same geography for data compliance reasons
* Region pairs are predetermined and cannot be chosen
* Some services have platform-provided replication

Special Regions

* US Gov’t (and contractors)
  + Azure Government or DoD
  + .us domain instead of .com
* China (21Vianet)
  + available to any Legal entity in China
  + 4 regions in China
* Germany T-Systems (Sovereign)
  + Available to organizations that have already purchased Microsoft Cloud Germany

Availability Zones

* A feature of regions
* Physically separate facilities with independent cooling, power and networking infrastructure
* Not available in all regions
* At least 3 zones per region (if Availability zones are available of course)
* Protect against failures within a datacenter and across datacenters
* A zone is one or more data centers
* Does not protect against regional failure (because Zones are datacenters within the same Region) – need Region pairs for that
* SLA – 99.99% when "2 or more VMs running in 2 or more zones in the same region”
* No noticeable latency between datacenters within different availability zones within a region

Availability zones 2 service categories

1. Zonal services (VMs, disks, etc)
2. Zone-redundant services (SQL, storage, etc)

Availability sets

* Insures VM is online during maintenance or failure
* A VM is assigned to an update domain and fault domain (so 1 machine is updated at a time)
* For each region, Azure provides a maximum of 3 fault domains and a maximum of 20 update domains
* Fault domains provide physical isolation inside the data center
* SLA – 99.95%
* We recommend 2 or more VMs are created within an availability set to meet the 99.95% Azure SLA (those VMs have to be in the same region).
* We can add VM to an Availability Set ONLY when creating the VM, and can't add already created VMs to an Availability Set.
* 50 VMs inside one availability set is the maximum

Azure Service health

* notifies you about Azure service incidents and planned maintenance so you can take action to mitigate downtime
* evaluate the impact of azure service issues with personalized guidance and support
* Azure recommends 2 or more instances of a VM deployed in an Availability Zone or Availability set to maintain the SLA 99.99 or 99.95 guarantee

For single instance VMs ->

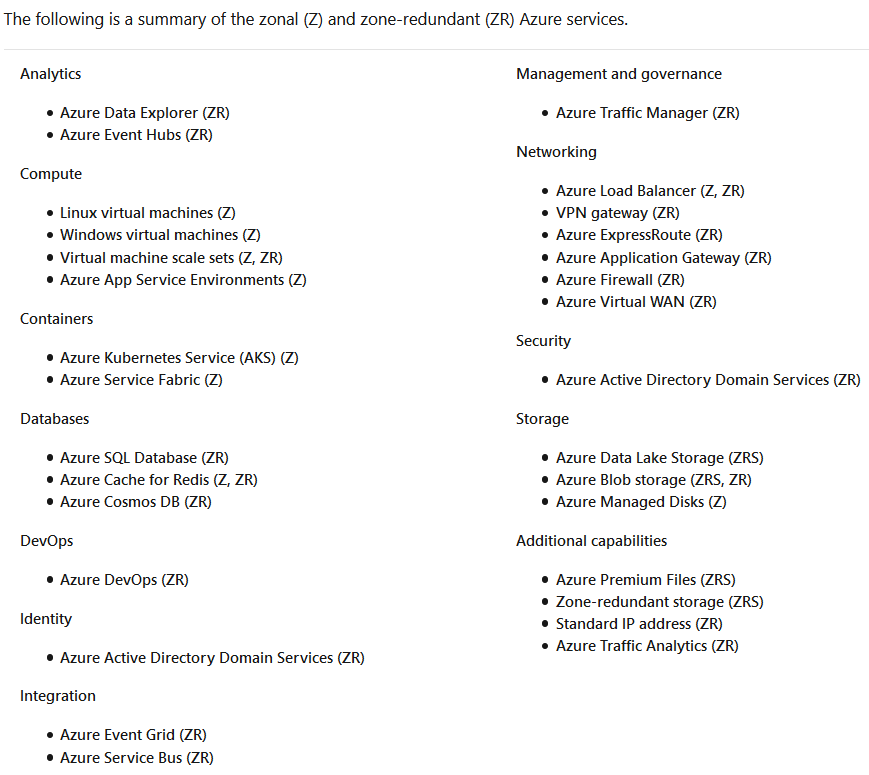
* + 99.9% SLA if using Premium SSD
  + 99.5% SLA if using Standard SSD
  + 95% SLA if using Standard HDD

Zonal

* Allows the user to pick which availability zone the resource is created in
* Resiliency has to be self-architected by the user by manually replicating apps and data to one or more zones within the region
* Typically IaaS services are Zonal (VMs, managed disk, etc)

Zone-redundant

* Automatically creates copies of the resource across different availability zones
* How many copies is dependent on the resource type (3 for storage, 4 for Azure SQL)
* Different services have different options of what they support



Resources

* Objects that are used to represent your services in Azure
* Represent service lifecycle
* All resources are represented by a JSON template (properties and values)
* JSON properties – type, API-version, name, location
* Resource costs can vary by region (electricity, human labor costs, etc)

Resource groups

* Logical container for holding resources
* Allows us to deploy, manage and monitor resources in a group
* Resources can be moved between resource groups (not all of them, and resources are locked until the move is completed)
* Resources can be in different regions than the resource group
* Free
* Help us manage lifecycle for an application, or for organizational purposes
* Resource groups can talk to each other
* By default, Azure will not allow deployment of managed applications (such as VMs) to resource group with resources.
* Cannot be nested
* Resource groups are not backed up
* Can be created using
  + Azure portal
  + Azure PowerShell
  + Azure CLI
  + Templates
  + Azure SDKs (like .NET, Java)
* Strategies to group resources -- by type, application lifecycle, department, billing, location, etc;

Management groups

* Each Azure Active Directory (AD) tenant includes a top level or “root” management group
* a collection of multiple subscriptions
* Helps you with the Governance
* Group of Azure objects that make up a collection
  + This collection can contain subscriptions or other management groups
* manage policies, access and compliance for the entire group
* 1000 management groups in a single directory
* Up to 6 levels of depth
* Subscriptions inherit conditions applied to the management group (policy, RBAC, locks)

Management groups are the parent and can contain multiple sub management groups and/or subscriptions

Azure Subscriptions

* Once you have a subscription, then resources can be created and managed
* Containers for resources
* Subscriptions have owners
* A subscription can only be nested under a single management group
* links directly to Azure Active Directory for authentication and authorization
* You can have multiple subscriptions to one account holder
* Multiple subscriptions can be useful for billing and access control boundaries
* Can have multiple subscriptions in your Azure account to create separation
* Can be different tiers (free, PAYG, student, etc;)
* linked to a payment setup and each subscription will result in a separate bill

Subscriptions options

* PAYG
* Azure free account – $200USD for 1 month and 12 months free with limitations
* EA – Enterprise Agreement (1 or 3 year contract with a discount)
* Student
* An account can have one subscription or multiple subscriptions

Subscription considerations

* service limits for each subscription type
* Example – 10 web apps for free account, unlimited for basic PAYG accounts

Subscription Access Control boundary

* Subscriptions are applied to a specific department inside an organization (IT or HR, etc)

Azure tenants

* Each Azure A/D tenant includes a root management group.
* Tenant is a directory, where a subscription is an object that represents a "folder" that you can put resources in
* associated with a single identity
* A tenant can have many subscriptions, but not vice versa.
* You switch between tenants by switching directory

RBAC – Role Based Access Control (IAM)

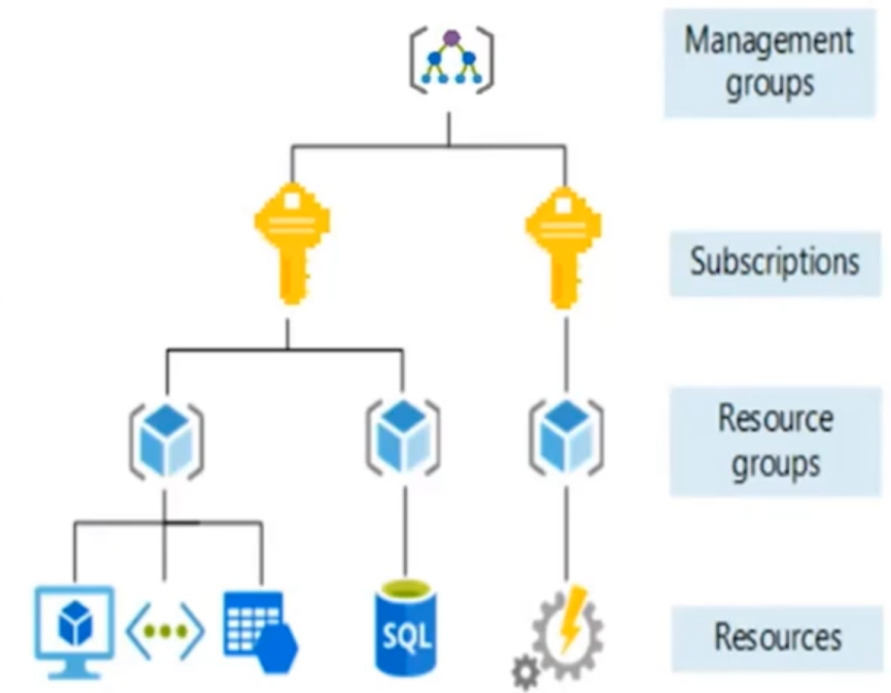
* fine grained access management
* how we grant permissions inside an organization
* can be applied at any level
* **OCR - Owner, contributor, reader**

Azure subscription administrator roles

* Account Administrator (1 per account)
* Service Administrator (1 per subscription)
* Co-Administrator (200 per sub)

Azure Groups

* a basic group is created using Azure A/D and added to a single resource by the resource owner (administrator) and includes specific members (employees) that need to access that resource
* Best practice to grant RBAC to groups and not to individual users



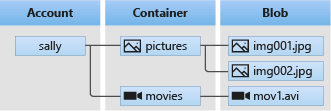
* This hierarchy is useful because policies are inheritable and can be applied at top level management groups for simplicity instead of handling each subscription individually.

Azure Resource manager (ARM)

* Access and manage resources
* Deployment and management service
* Consistent management layer that is used to access and manage Azure resources
* Create, update, delete, organize manage, control and tag resources in the azure subscription
* Accessed using the azure portal, Azure powershell, azure command line interface (CLI or rest clients
* Define dependencies between resources so they are deployed in the correct order
* Uses the REST API (operations that take place over http/https)
* Unified language
* Controls access and resources
* Representation of data using a JSON file

Blob storage offers three types of resources:

1. The storage account
2. A container in the storage account
3. A blob in a container



Resource Locks

* can set the lock type to CanNotDelete (Delete) or ReadOnly
* free
* no latency

Tags

* How we can organize our resources
* Name-value pair (example – fName : Marc ; lName : Labrecque)
* Not all resources support tags
* Use search to find resources easily
* Case insensitive
* Not inheritable by default
* You can add, modify, or delete resource tags through PowerShell, the Azure CLI, Azure Resource Manager templates, the REST API, or the Azure portal.
* Can be enforced through policy
* MS has recommended standards for tags

Azure Roles (OCR)

* Owner, contributor, reader, user access administrator

Azure AD roles

* **Global Administrator**, User Administrator, Billing Administrator

Azure limits

* Tied to subscriptions
* also called quotas
* **Default limit** and **Maximum limit**
* to raise the limit or quota above the default limit, open an online customer support request at no charge thought the Azure portal
* can enable spending limits (budgets)

ARM templates

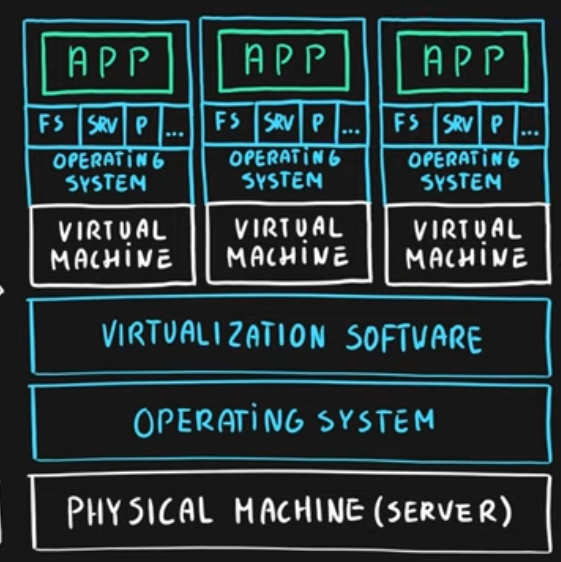
* a JSON file that defines the infrastructure and configuration for your project.
* allows you to create and deploy an entire Azure infrastructure declaratively.
* For example, you can deploy not only virtual machines, but also the network infrastructure, storage systems and any other resources you may need.

Azure compute

* on-demand computing service for running cloud-based applications
* 2 of the more common compute services are VMs and Containers

Virtualization

* Emulation of physical machines
* Different hardware config per machine/app
* Different OS per machine/app
* Total separation of environments



Azure VM service

* MS has created VM instances available in the Azure Marketplace (Ubuntu, Windows Server ,etc)
* Or you can customize your own VMs

Virtual Machines

* IaaS
* Total control over the OS and software
* Supports marketplace and uploaded custom images
* VMs can be resized after creation
* Best suited for custom software requiring custom configurations and high degree of control
* Can run any application scenario – web apps, dbs, desktop apps, jumpboxes, gateways
* Customer provides the availability, security and disaster recovery
* VMs are great but they lack scalability
* Customers are responsible for OS patches, but can automate using VM guest patching (public preview)
* Customers are responsible for antimalware, backups, configurations, etc;
* Administrator account – cannot be named “admin” or root; Cannot use password1 for password
* Not every VM size is available in every region
* Lift and shift – moving apps that cannot be containerized
* VMs don’t actually live inside VNets, we attach NIC(s) to VMs and connect the NIC to the VNet; Can have more than 1 NIC and connect different NICs to different subnets within the same VNet, but cannot be connect to multiple VNets
* Max Nodes = 1
* When you create a VM in Azure, a new Virtual Network is also created with a default setting.
* Azure VMs in different subnets in the same virtual network can communicate by default

Template

* When you create a VM from scratch, a template file is saved (in JSON format) so you can save or use the file to recreate a VM in the future
* Can also download custom templates

Azure Marketplace

* 1st and 3rd parties offer customized solutions, services (IaaS, Paas, Saas)
* 800+ solutions available to customers

VM Scale Sets (An alternative to regular VMs)

* Iaas
* Set of Identical VMs created from the same image
* Provides high availability and scalability
* Automatically scaled across multiple VMs, and the VMs are hidden behind a load balancer
* Additional VM instances are added automatically when the workload increases and deleted when the workload decreases (their disks are also deleted)
* Add/Delete VMs can also be handled manually using the Scaling option in Azure portal
* Used in large-scale instances
* Scaling can be based on specific demands – more cpu power or more memory, etc;
* Can use spot instances to save money and name your price
* Ideal for season or sporting events (sporadic traffic) because of autoscaling
* Also ideal for stateless patch processing jobs (ie- once a month you have to do a lot of processing)
* Overprovisioning – by default it will start up more VMs than required in case of failure(s), and then delete them once the request number of VMs have been successfully provisioned
* Instance protection – protection certain instances of the VM (don’t delete certain instances)
* Elastic (scale out and scale in)
* Max nodes = 1000

Container

* Virtualization of the OS, so it runs on top of a VM
* A slimmed down version of a VM (smaller & faster)
* Does not include an OS that can be managed, but the OS files can be referenced to run an app
* Runs an Image with a specific OS, and that image OS has to match the container host OS (cannot mix OSs)
* Includes libraries to run an app
* Sandbox environment for each app
* Portable and fast to start and stop
* Can have multiple containers within a single runtime/OS
* Containers may share a kernel on the same physical machine, but containers cannot see each other
* Much smaller footprint compared to VMs – lightweight, less maintenance
* Docker is a popular container brand
* Typically a container runs a primary process, and when that process finishes, the container finishes as well (the container shares a lifecycle with the process)

1. Azure container instances
   1. PaaS
   2. Serverless containers
   3. Only pay when it is running
   4. multi-tenant service, but containers are isolated and cannot see each other
   5. you can upload your container to azure for execution
   6. Linux or Windows
   7. Can be public or private
   8. Uses Docker
   9. Ideal for simple use cases (web scripts, etc)
   10. Very ideal for burst scenarios
   11. Can integrate with Azure Kuberneties service
   12. SLA - 99.9%
   13. Max nodes = 20
2. Azure Kuberneties service (K8S or AKS)
   1. PaaS
   2. Better orchestrator and integration (allows services to better communicate with each other)
   3. Ideal when we need more than one, isolated container
   4. used to manage and update a large number of containers
   5. Master node and worker/cluster nodes
   6. Open source
   7. Highly scalable and customizable
   8. takes care of scaling and failover for your application, so if one node goes down, another node is created
   9. You don’t pay for the management, only for the worker nodes that can autoscale
   10. SLA - 99.95% for AKS Clusters if you use Availability Zones, and 99.9% if you don’t
   11. Max nodes = 100
3. Azure Container Registry
   1. managed container registry service
   2. provides public and private repositories of container images
   3. different tiers can be purchased (basics, standard, premium)
   4. can be geo-replicated (with premium) - this is important both for resiliency and latency reasons
   5. can run jobs to build the container image

* We typically use Kubernetes when we need more than one isolated container

VM vs Container

* VM has more management
* Container has faster boot times, more efficient
* VM can have multiple OSs on 1 piece of hardware
* VM has partitions
* VM has independent OS/kernel, where containers share the kernel of the underlying OS
* Containers use far less disk space
* Containers are portable

Azure App Service (alternative to the IaaS VM)

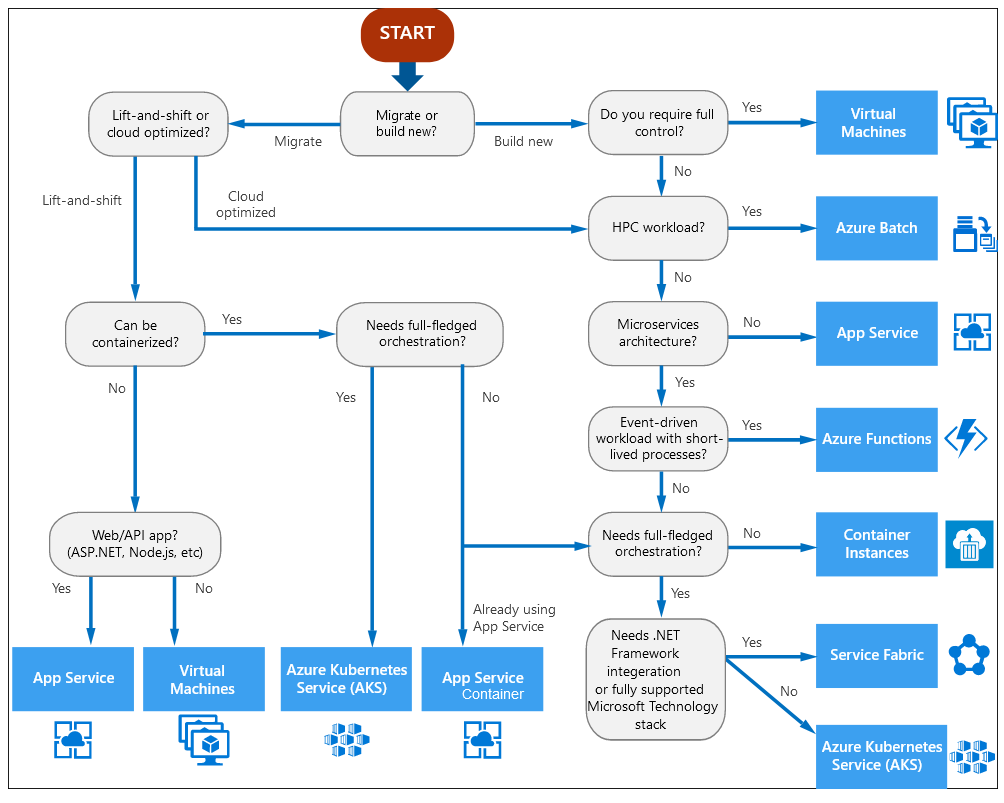
* PaaS – so less control over the hardware underneath
* Build enterprise grade web, mobile and API apps in any platform
* Azure provides a fully managed secure and scalable platform (scale up and scale out)
* Supports multiple programming languages, runtimes, and containers (java, php, C#)
* Focus specifically on code
* Lots of pricing options – different plans have different options (how many instances, how many deployment slots, etc)
* SLA – 99.95%
* Autoscaling
* Max nodes = 100

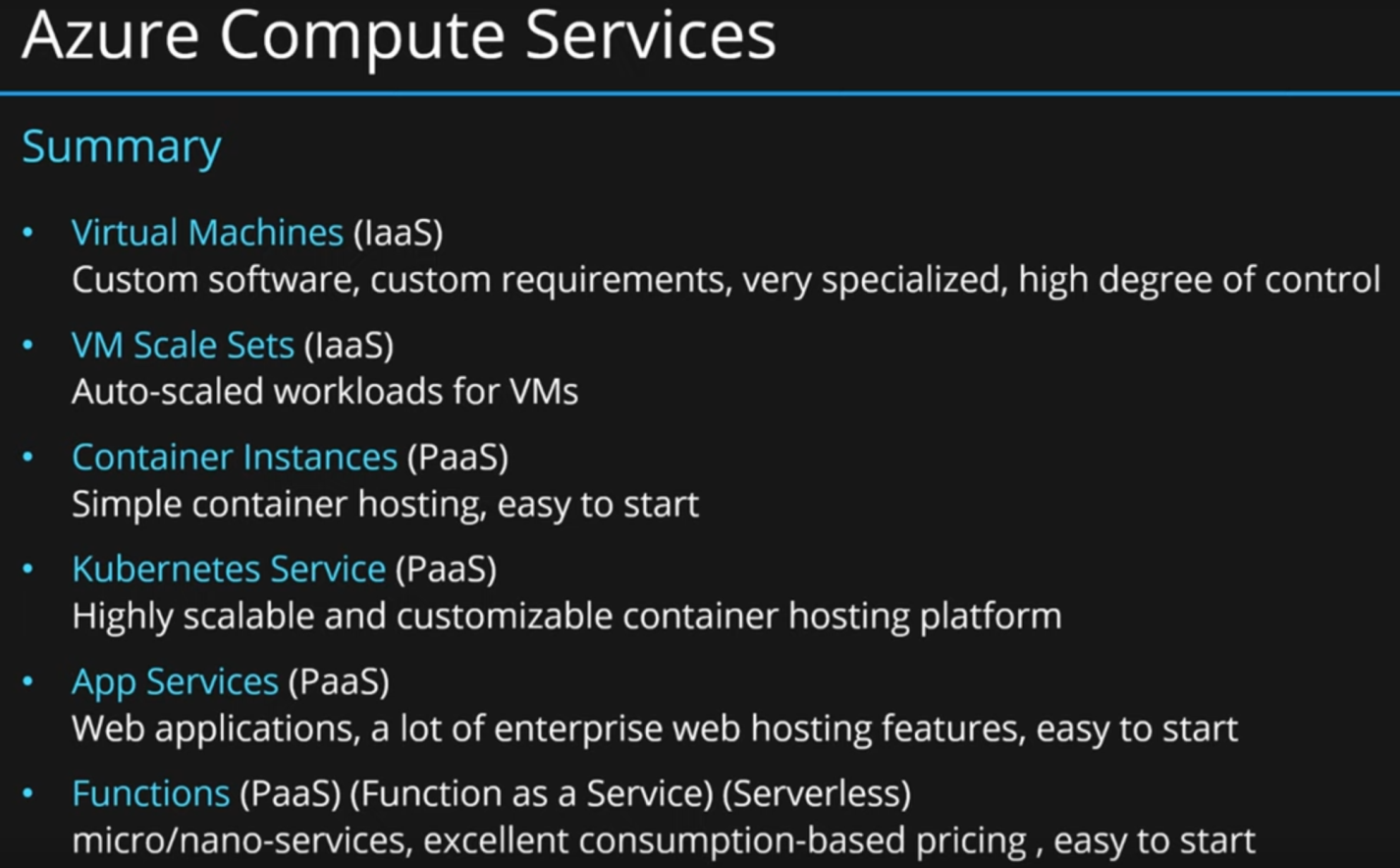
Azure Functions – app service

* Paas
* Serverless web hosting platform / serverless computing
* Runs a small piece of code instead of a full app
* Event, timer, message, or another trigger driven event (http, schedule, etc)
* Typical usage scenarios:, IoT, processing data, and more
* Micro or nano services
* Requires the least maintenance from the IT team
* Pricing
  + Consumption (PAYG)
  + App service plan

Azure Service Fabric (vs Kuberneties)

* Microsoft’s orchestration variant
* focus on building stateful containers and microservices
* variety of languages and programming models
* lacks portability
* Ideal for applications built using Windows Server containers or that need support for the MS technology stack
* VMs virtualize the hardware
* Containers virtualize the OS





Windows Virtual desktop (WVD)

* PaaS managed solution
* Only manage the image and virtual machines, not the infrastructure
* Accessed via Windows, Mac, iPad, iPhone, Android, browser
* Hosted Windows Remote Desktop Services
* Workers can access their desktop wherever they are
* Confidentially advantages
* Apps are fully integrated with the start menu
* Identity based access
* Requires an active Azure A/D to support Windows Virtual Desktop:
* Can have more than 1 user per VM (Windows 10 multisession), with the idea of reducing the number of VMs and OS overhead while still providing the same resources to your users
* Host pools can be assigned to different departments that have different computing needs
* 1 TB storage (One Drive limit)
* Can use existing licenses (Office 365, etc)

OSI model - *“People don't need those stupid packets anyway”*

1. Physical (e.g. cable, RJ45)
2. Data Link (e.g. MAC, switches)
3. Network (e.g. IP, routers)
4. Transport (e.g. TCP, UDP, port numbers)
5. Session (e.g. Syn/Ack)
6. Presentation (e.g. encryption, ASCII, PNG, MIDI)
7. Application (e.g. SNMP, HTTP, FTP)

Azure Virtual Network

* Consists of one or more IP ranges
* Emulation of physical networking infrastructure
* Designed for isolation, segmentation, communication, filtering, routing between resources (on prem and cloud)
* Scoped to a single subscription/region (cannot span subs or regions)
* Can have resources from other regions connected to a VNet
* Can be segmented into one or more subnets which allow customers to divide networks for address allocation and network filtering via NSG or ASG
* By default traffic can flow freely within a VNet and to any connected/peered networks
* By default VNets do not communicate with each other, unless they are connected
* Can be connected to other virtual networks (across different regions) using:
  1. VNet Gateway
  2. VNet Peering
* Provides filtering and routing of network traffic
* Typical to divide Virtual Networks using subnets by tier – Web tier, Business tier, Data tier

Subnets

* A range of IP addresses that can be used to separate VNets from each other
* Subnets are also regional (cannot span regions)
* Subnets cannot be nested
* Good practice to use subnets for organizational purposes

Local network gateway

* represents the hardware or software VPN device in your local network.
* Use this with a connection to set up a site-to-site VPN connection between an Azure virtual network and your local network.

VPN Gateway

* Used to connect on prem resources to Azure over the public internet or to another Azure network
* Also connects VPN1 to VPN2 (although less common)
* Traffic is encrypted
* A VPN gateway supports multiple connections
* Number of connections is based on the SKU
* Each virtual network can have only one VPN gateway
* Always on

VPN Peering

* VPN1 to VPN2 connectivity
* For customers with strict data policies as public internet is not involved
* Makes multiple VNets appear as one VNet
* IP space cannot overlap
* Not transitive (VN1 connected to VN2 connected to VN3; VN1 is NOT connected to VN3)
* does not encrypt traffic (it doesn’t have to since you’re not going over the public internet)
* can span different subscriptions
* Can work one way or both ways (require permissions at one end or both ends, respectively)
* The reason why we need Load balancers or Application gateways is scalability– we have more than 1 resource (example – VM) available to customers with identical content to handle all the traffic we get.
* Also resiliency – if the one of the VMs crashes, we can redirect traffic to the working VMs.
* The load balancer has a public IP rather than the VM or App and distributes traffic accordingly

Load Balancer

* Distributes traffic in, out, and within the network
* Non-http
* can only route traffic inside an Azure region, as it only works with VMs in the same region
* Provides low latency and high throughput
* Public(external) and private(internal) types:
  + Public is exposed to the internet and manages internet traffic
  + Private is internal and manages internal traffic only
* In larger applications, we would have a web tier (external) and data tier (internal), and a separate load balancer for each tier
* Supports inbound and outbound scenarios
* High availability and scalability scenarios
* Supports Layer 4 TCP and UDP (non-http traffic)
* Supports endpoints hosted in Azure only
* Will only route traffic if the resource passes its health check
* Common to use load balancer with VM scale sets

Application Gateway (A type of Load balancer)

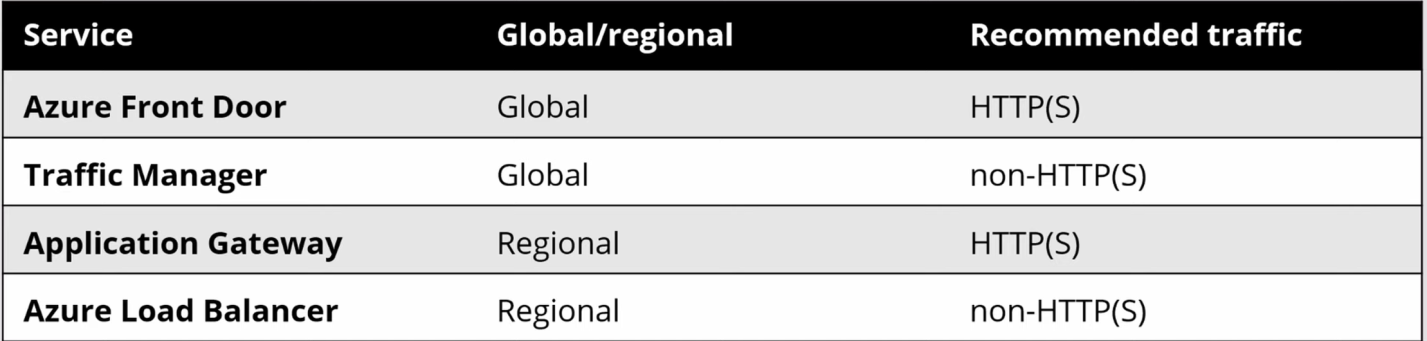
* Load balances web traffic only to web applications (the preferred method of handling web traffic)
* http / regional
* regional – load balance between VMs, containers, or clusters within a region in a virtual network
* layer 7 traffic (http/https)
* More features than load balancers (security, etc.)
* More complicated to set up than load balancers
* More expensive than load balancer
* Routes traffic based on source/dest IP address and port
* Supports URL- based routing
  + Traffic is directed based on the URL (any website /path/ or IP address will work)
* Will only route traffic if the resource passes its health check

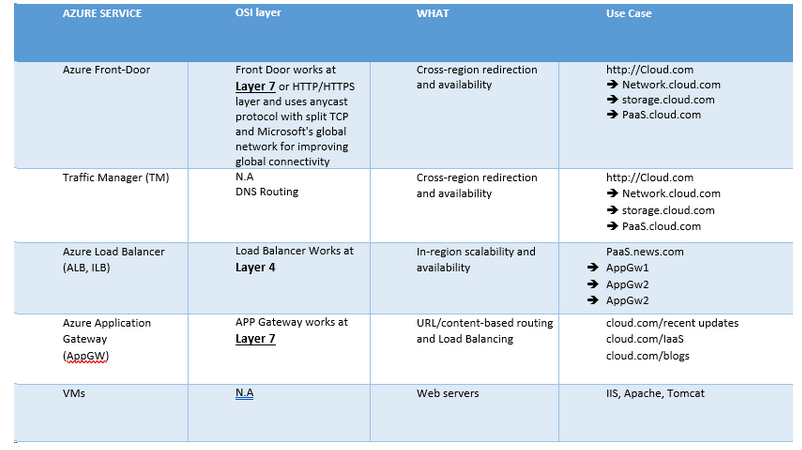
Azure Front Door

* offers a single global entry point for customers accessing web apps, APIs, content and cloud services
* http / Global
* layer 7 traffic (http/https)
* global load balancing, but also enhances performance (site acceleration)
* premium edge performance acceleration and caching via Microsoft’s unique global WAN
* ensures that your end users promptly connect to the nearest Front Door POP (Point of Presence)
* Increase application availability with smart health probes

**Azure Traffic Manager:**

* Load Balancer for geographically distributed Datacenters
* Non-http / Global
* uses DNS to redirect requests to an appropriate geographical location endpoint with the lowest latency (ie the fastest/closest to the user)
* typical usage is load between two endpoints where your first endpoint is in Azure and second endpoint placed  in on-premise datacenter
* The local DNS server makes the request, not the client
* Cannot process IP address endpoints, DNS only





Content Delivery Network (CDN)

* Globally distributed servers used to efficiently deliver web content in the users region
* Minimize latency
* POP (points of presence) locations
* Content will sit on an edge server close to the user
* Content is cashed to minimize legacy
* Typically used when high bandwidth is req’d
  + Example: Multimedia content, videos, etc;
* Reduced buffering because servers are close to users
* Typical usage is for large media files that are statically located (foobar.com/video)
* **AL**
* **FT**

L4 Load balancer

* we are unaware of the data
* delivering messages regardless of the content
* The only thing we have is IPs (source and destination) and ports

L7 Load balancer

* we are aware of the data in our request
* terminates the network traffic and reads the message within.
* makes a smart decision based on the content of the message

Azure Network Watcher

* monitor and repair the network health of IaaS products within a Virtual Network - Virtual Machines, Virtual Networks, Application Gateways, Load balancers, etc.

Connecting OnPrem to Azure

1. Azure ExpressRoute
   1. extend your on-premises networks with Azure data centers with the help of connectivity provider
   2. private connectivity (via gateway)
   3. maximum number of network Azure ExpressRoute circuits per subscription is 10
   4. connection is not encrypted, because it is not going over the internet
   5. no support for IPv6 (yet); only IPv4
2. Secure point to site connectivity
   1. Connects one specific device to a VNet
   2. connect to the network you want to access manually
   3. bidirectional (1-to-many)
   4. typical usages - when we are working remotely
   5. connect a single computer to a network
3. Secure site to site VPN connectivity
   1. connect two networks and keep the communication up all the time via gateways
   2. bi-directional (many to many)
   3. gateways support multiple connections (VNet A connected to B and C)
   4. encrypted data going over the internet
4. VNet Peering
   1. In region VNet to VNet connectivity
   2. **SEE PREVIOUS PAGE 22**

Azure Storage Services

* Storing files, messages and tables
* Massively scalable
* Durable
* Highly available
* Secure
* at least 3 copies
* Supports 3 types of data: Structured, semi structured data, unstructured data
* 2 access keys available (can regenerate)

Structured data

* Has a schema
* Rigid format
* Relational data
* Uses keys to relate a row in one table to a row in another table
* Typically used in db’s

Semi structured data

* Ad-hoc schema
* Nonrelational format
* Known as NoSQL data
* Uses tags for data location
* Typical usages: .csv, XML, JSON

Unstructured data

* The most common data type
* Usages: wpd, jpg, avi

Azure Storage Account

* A collection of services (blob, queue, table, file and disk)
* Designed to allow customers to store files at high scalable in Azure
* High durability
* Cheapest storage per GB
* Always encrypted at rest – you can chose your own key via Key Vault
* Lowercase characters only
* 2 PB (Peta bytes) max storage amount
* Storage V2 supports Blob, File, Queue, Table, Disk, and Data Lake Gen2
* BlobStorage and **BlockBlobStorage** only supports blob storage
* FileStorage supports only File storage types
* So, we almost always choose Storage V2

Storage types in Azure

* Blob (Containers)
* Queue
* Table
* File
* Disk

Blob Storage (Azure calls this containers)

* A blob is just a file (**B**inary **L**arge **Ob**ject)
* Unstructured data
* Highly scalable
* Inside a blob storage you create a container (which acts as a folder) and store files inside the container
* MS recommends blob storage for most uses
* 3 storage tiers – Hot, Cool, Archive
* Set to no public access by default
* You can host a static website via blob storage ($web folder)
* PaaS

Queue Storage

* Designed for scalable Asynchronous processing
* Storage for small pieces of data
* PaaS

Table Storage

* Semi structured/non-relational data into tables
* key-value pairs
* No SQL db’s
* Designed for fast access
* Many programming interfaces and SDKs
* PaaS

File Storage

* File shares in the cloud
* Accessed using SMB protocol (Server message block)
* **File storage = SMB storage**
* Shares can be mounted to a system providing direct access to files in the cloud from anywhere at any time (persistent)
* Supports multiple connections – can be mounted to several systems at one time
* IaaS

Disk storage (VM disk storage)

* Disk emulation is the cloud
* Provides persistent (always available) storage for Azure VM disks
* 2 types of disk storage
  + OS disks – created when you create the VM
  + Data disks - optional
* MS recommend attaching a data disk to your Azure VM for storing data
* Never store anything to the temp disk (non-persistent) as it will be deleted
* Disk can be Managed (on the Azure cloud) or unmanaged (not on the cloud)
* Options - Standard HDD, SSD, Premium SSD and Ultra SSD
* Can be resized (have to turn off VM obv)
* Encrypted by default
* Iaas

Archive storage

* Stores data this is req’d infrequently
* Data is stored offline
* Low storage costs, but highest costs to access the data
* High latency for retrieval
* MS recommends data that can be archived for at least 180 days

Storage replication in Azure

* Data in an Azure Storage account is always replicated 3 times in the primary region
  + synchronous- in region
  + asynchronous- different region
* Locally redundant storage (LRS)
  + copies your data synchronously 3 times within a single physical location in the primary region.
  + Least expensive
* Zone-redundant storage (ZRS)
  + copies your data synchronously across 3 Azure availability zones in the primary region.
* **Geo-redundant storage (GRS)**
  + 3 copies in the primary region within a single physical location using LRS, 3 more copies asynchronously in the region pair
* Geo-zone-redundant storage (GZRS)
  + copies your data synchronously across 3 availability zones using ZRS. Then 3 copies asynchronously to a single physical location in the region pair.

Blob Storage access tiers – the goal is to save money

* Hot
  + frequently accessed data
  + discount on transaction because you are frequently accessing the data, but no discount on footprint (the actual data space)
  + instant access
* Cool
  + infrequently accessed data (30 days)
  + discount on footprint but not on transactions
  + instant access
* Archive
  + rarely accessed data (180 days)
  + data has to be rehydrated to be accessed
  + large discount on footprint, but have to pay for rehydration
  + there is a delay to access data (1-10 hours)

3 copies of any data you run in Azure

Azure Databases

* PaaS
* Fully managed databases
* Built in high availability

Cosmos DB

* *globally distributed*, multimodel database service.
* Semi structured, Non-relational db (nosql, JSON)
* Key-value pairs
* can scale throughput and storage across Azure regions.
* highly responsive at less than 10 ms latency and highly available at 99.999% or five nines.
* Automatically replicate data closest to the users and that's what makes it highly responsive and highly available.
* Typical uses for include web, mobile, gaming, and IoT applications.
* Multiple APIs (SQL, MongoDB, Table Storage)

Azure SQL – a family of products

* SQL Database
* SQL Managed Instance
* Azure Synapse Analytics (SQL Data Warehouse)
* SQL VM
* Db for MySQL
* Db for PostgreSQL

Azure SQL Database

* PaaS
* Structured, relational database service, or DaaS.
* fully managed and secure SQL database.
* highly available by default.
* Because this database is managed, it is automatically backed up for us, we don't have to worry about that.
* Typical uses for a SQL database include any company database, like an HR database, maybe an inventory database, payroll, etc;
* Geo replication
* Vertically scaled

SQL Managed Instance (aka Cloud Lifter)

* PaaS
* Used to ease cloud migration by reducing management overhead
* Online migration

Azure Database Migration Service (part of Azure Migrate)

* can migrate databases from onprem to Azure with little downtime.
* uses the Data Migration Assistant to provide reports and guides to step you through the migration.
* Supports Microsoft SQL Server, MySQL, PostgreSQL, MongoDB and Oracle migration to Azure from on-premises and other clouds
* free

3rd party db’s available in Azure…Azure Enhanced verisons

Azure Database for MySQL

* Relational db
* Oracle

Azure Database for MariaDB

* Relational
* Open source community fork of the MySQL db

Azure Database for PostgreSQL

* Relational
* Open source community

Azure handles Auto patching of these 3rd party db’s

IoT

* Internet of Things
* Any device capable of sending/receiving data and wifi

IoT Hub

* Central message hub for bidirectional communication between IoT devices and apps
* Managed service
* PaaS
* Highly secure, scalable, reliable
* Programming SDKs for popular languages
* Building solutions from scratch

IoT Central

* Globally manage SaaS solution to monitor and manage IoT devices
* Provides a set of templates for building solutions
* Out of the box solutions (no tech knowledge needed)
* Highly secure, scalable, reliable

Azure Sphere

* Set of components which allows you to build IoT components
* Secure end-2-end IoT solutions
* Aims to fix device standardization
* Azure Sphere-certified microcontrollers - MSUs
* Azure Sphere OS - based on Linux
* Azure Sphere Security Service - hardware and software protection
* turnkey security solution for IoT devices

Azure IoT Edge

* fully managed service built on Azure IoT Hub (integrates w/ IoT Hub)
* devices spend less time communicating with the cloud, react more quickly to local changes and operate reliably even in extended offline periods.

IoT Solution

* IoT solution is made up of one or more IoT devices that communicate with one or more back-end services hosted in the cloud.

The goal of big data is to uncover hidden patterns

Big Data is storage over 1TB

Big Data is multiple tools working together

Cluster computing

* massively parallel processing

Big Data – what is is?

* Velocity – how fast is our data arriving
* Volume – how much data
* Variety – how structured is our data

Azure Synapse Analytics (Formerly Azure SQL Data Warehouse)

* Big data analytics platform (PaaS)
* brings together enterprise data warehousing and Big Data analytics
* Massively parallel processing
* Ingest - > Transform - > store - > serve
* Synapse studio includes embedded Apache Spark/Synapse SQL/Synapse Pipelines
* Synapse pipelines allows you to visually build your data injection and data transformation workload
* enterprise data warehouse, or EDW.
* run complex queries across petabytes of data using massively parallel processing, or MPP
* We use Azure SQL Data Warehousing for big data.
* Typical usage: online retailers
* Integrated with Azure Data Lake Storage

Azure HDInsight – The analytics service in Azure

* Flexible multi-purpose big data platform (PaaS)
* Service for open source analytics such as Apache Spark or Apache Hadoop
* Provides open source big data clusters

Azure DataBricks – similar to HD insights but only support for Spark (no Hadoop)

* Big data collaboration platform (PaaS)
* Similar to HDInsight except the clusters we create are based on Apache Spark alone
* Help with data transformation at large scale
* Integration with Azure resource manager
* Unified workspace for notebook, luster, data, access management and collaboration
* zero-management
* typical usage - data source for machine learning algorithms

Data Lake Analytics

* On demand analytics job service
* no hardware is req’d, everything handled by Azure
* IoT Hub can route messages to Azure Data Lake
* Large volumes of variable data
* Pool of data with an unknown purpose or insight

Apache Hadoop

* The original big data analytics product family
* Batch processing
* Replaced by Apache Spark which is much faster

Apache Spark

* Next gen – replaces the slower Apache Hadoop
* In memory query processing and data analytics
* Meant to be used interactively

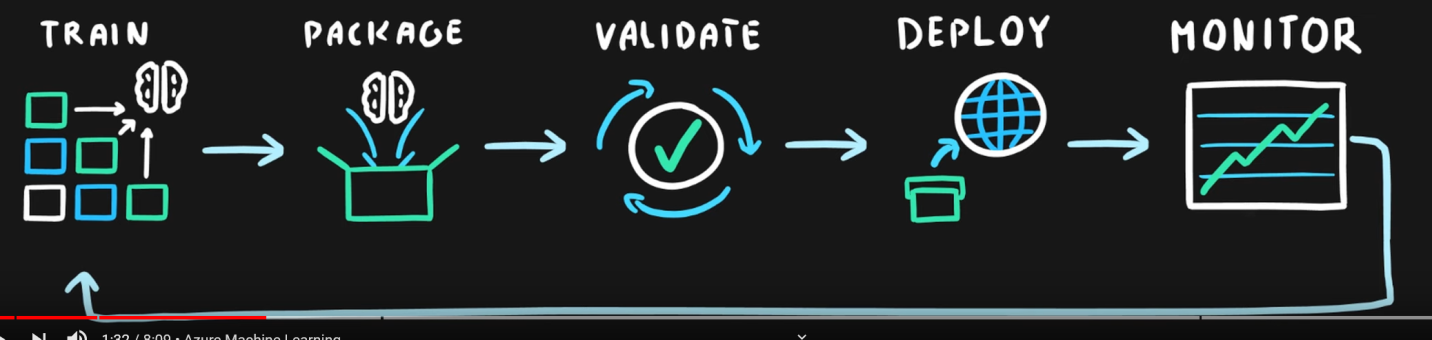
AI is the simulation of human intelligence and capabilities by computer software

M/L is a subcategory of AI where computer software is taught to draw conclusions and make predictions from data. The process is called “building a model”.

Use existing data to forecast future behaviors

AI – 2 services

1. Azure M/L Service
   1. PaaS
   2. Build, train deploy manage and track models
   3. Tools provided in Notebook (Python/R), Automated ML or designer
   4. Pipeline – end 2 end solution for building M/L models
   5. M/L Workspace ties everything together
   6. Ideal for Data Scientists
   7. Code in Python or R
2. Azure M/L Studio Service (legacy product, no longer supported)
   1. Visually interactive workspace to build and deploy M/L solutions
   2. No code req’d (drag and drop)
   3. Model you create in ML studio cannot be deployed or managed in ML service

****

Azure Cognitive Services

* SaaS
* APIs and SDKs that enable AI for non-developers
* Libraries that users can plug in and use cognitive services
* Examples (VSLDS)
  + Vision (face recognition)
  + Speech (text to speech)
  + Language (LUIS)
  + Decision (content moderator, personalizer)
  + Search (Bing search lol)

Azure Bot service

* Applications with human like interactions
* Chat bot between human and computer

Serverless Computing

* is a cloud hosted executing environment that allows customers to run their apps in the cloud while completely abstracting underlying infrastructure
* Out of the box products available in Azure
* Let MS scale up and down to match demand

Azure Functions

* Serverless coding platform (FaaS)
* Runs code only on the host
* Users can upload raw source code
* Respond to an event, such as a trigger from IoT device
* Typically used for processing incoming data
* Highly scalable
* Supports popular languages and frameworks (.NET, Java, Python, Powershell, etc)

Logic Apps

* PaaS
* Build orchestrated workflows using a visual interface (similar to MS Flow)
* Automatic tasks, process, and more for integrating with other services such as apps data, systems and services
* Can trigger flows by 200 connectors (web, mail, 365, Azure, etc)
* No code req’d
* Integrate with cloud or on prem services

Azure Event Grid

* Event routing service for sending messages (messages are called topics) between services
* takes an event source such as IoT Hub, or storage, and sends the event handler for processing
* uses publish-subscribe model
* designed for event based and near-real time apps
* scalable

Event Hub

* Hosted event telemetry stream processing platform

Azure Power Platform

1. Power Apps
2. Power Automate
3. Power BI

DevOps aims to shorten the development life cycle by providing continuous integration and deliver (CI/CD) capabilities while ensuring high quality of deliverables

The pipeline builds code, runs tests (CI), and safely deploys a new version of the application (CD).

Azure DevOps solutions:

1. Azure DevOps
   1. A set of services including - Boards, Repos, Pipelines, Artifacts, Test plans
   2. Continuous delivery of code
   3. End to end platform
   4. Devs, sys-admins and testers working together
   5. Software development and software delivery in an automated fashion
   6. Additional Cloud hosted tools from different vendors
   7. Integrated with Git repos
   8. version updates of a PaaS application hosted in Azure
   9. In any language targeting any platform
2. Azure DevTest Labs
   1. A workspace for devs and testers
   2. PaaS
   3. Cloud based sandbox environments
   4. Self-service VM and environment provisioning
   5. creates labs consisting of pre-configured bases or ARM templates
   6. Granularity control access and cost
   7. Auto start and shutdown of VMs
   8. Integrated with Azure DevOps Pipeline
   9. Allows devs/testers the self-service experience where they can claim a VM from a list of claimable and start developing/testing
   10. Save time and money
   11. Create once, use everywhere

Github Actions (vs DevOps)

* Automated workflows initiated by Github events
* Events can spin up one or more Containers for you in the cloud
* CI/CD capabilities
* .yml files

Azure Management tools

Azure Portal

* Website to manage Azure services
* Designed for self service
* customizable
* Limited automation, more suited for simple tasks

Azure cloud shell

* Browser based scripting environment
* Can be accessed…
  + from the portal (can select PowerShell or CLI)
  + using a mobile device
  + via browser (shell.azure.com)
  + from Visual Studio Code
  + from Windows terminal
* Does require a storage account (persistent storage)
* Based on the Ubuntu container
* Can run Powershell or Bash

Azure Powershell

* Command based shell scripting language
* Great for automation and repetitive tasks
* Code is cross platform (PowerShell Core)
* Simple to use
* Commands are objects
* Windows, Linux or MacOS

Azure Command line interface (CLI) aka BASH

* Cross platform scripting program for Azure
* Great for automation of repetitive tasks
* Preferred by admins with Linux/Mac experience
* Simple to use (all commands start with az)
* Commands are strings

Azure Mobile App

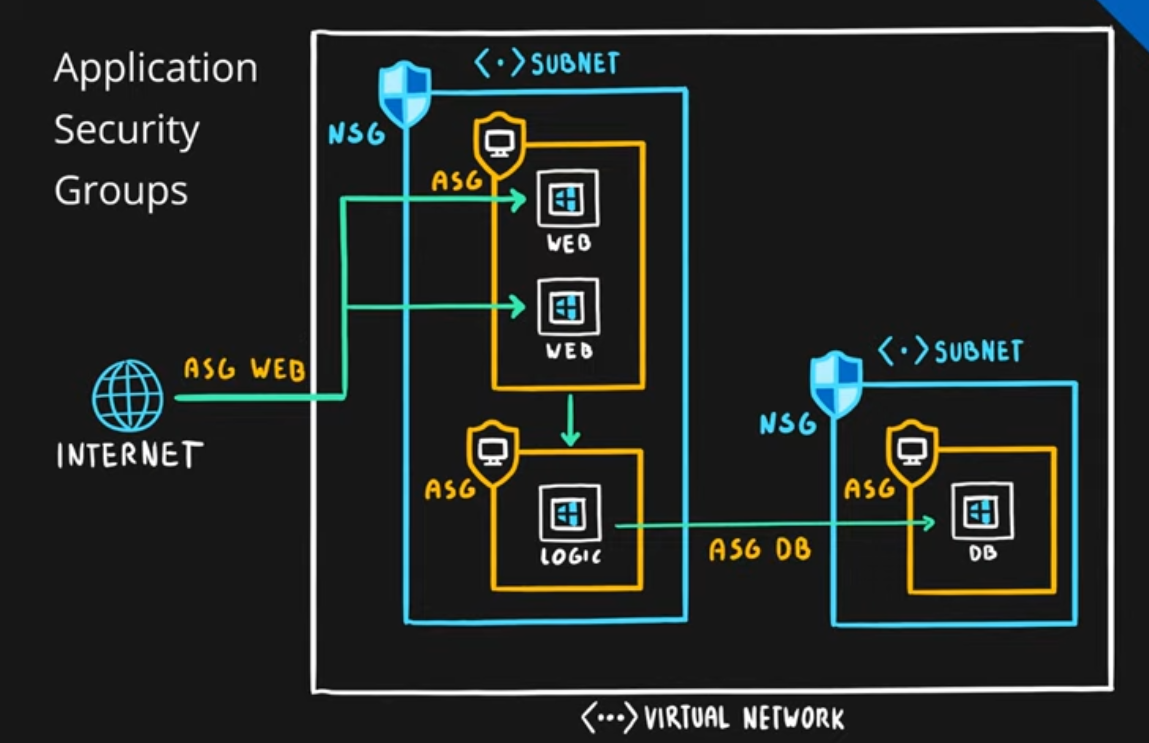
* IOS and Android
* Powering off VMs
* Cloud shell
* By default traffic can flow freely within a VNet and to any connected/peered networks
* To control the traffic inside (and outside) our Virtual Network we can use Azure Firewall, NSG, ASG or Service Tags

Network Security Groups (NSG) - managing traffic using VNets

* Determining who can talk to who inside a Virtual Network
* Filters inbound and outbound traffic inside a network to and from your VMs
* 5-tuple hash depending on the
  + Source IP,
  + Source Port,
  + Destination IP
  + Destination Port
  + Protocol Type
* A NSG can be applied to a virtual subnet or individual VM (NIC card), but one per subnet and one per VM
* When you apply a rule to a virtual subnet, that rule gets applied to any resources inside of it
* When applied to a VNet or subnet an NSG it is not an edge firewall, but instead applied to the objects within the VNet or subnet (at the NIC level)
* Preferred method is to apply NSGs to Subnets instead of individual VMs so it’s easier to manage (VMs should be inside subnets anyways)
* A very basic filter that filters traffic at the network layer (L4)
* Can use ranges of IP addresses or service tags in rules
* Will only allow certain traffic to reach a certain VM within a subnet inside a virtual network
* Allow or deny network traffic to and from resources in an Azure VNet subnet using rules
* Typically, each subnet will have its own NSG with different rules (example - we want users to be able to connect to our web app but not to our db)
* Allow some services and disallow others
* Stateful packet inspecting firewalls – if you allow traffic in from port 80 or port 443 or port xx, then any return traffic from that port will automatically be allowed.
* Rules are similar to Windows firewall rules
* Rules are processed in priority order (lower numbers first)
* Ability to have multiple inbound and outbound rules (incoming and outgoing traffic)
* Rules are created by specifying
  + Source/Destination (IP addresses, service tags, application security groups)
  + Protocol (TCP, UDP, any)
  + Port (or Port Ranges, ex. 3389 – RDP, 22 – SSH, 80 HTTP, 443 HTTPS)
  + Direction (inbound or outbound)
  + Priority (order of evaluation)
* The last rule you cannot delete is to deny all traffic (lowest priority)

Application Security Group (ASG) – managing traffic using VMs instead of VNets

* group virtual machines across virtual networks
* allows us to filter traffic to the virtual machines (NIC) in the security group, not to the network itself
* Tags applied to NICs which can be used instead of IP ranges in rules which may be easier to utilize
* allows us to segment the virtual machines based on application



Routing

* Process of finding/selecting a path for a traffic in one or across multiple networks

Azure routing is set up by default

User-defined Routes

* A way for a customer to create user defined custom routers (UDRs) which are static
* Designed to override Azure defaults routing or add new routers
* Managed via Route Table
* Associated with zero or more Virtual Network subnets

Route table

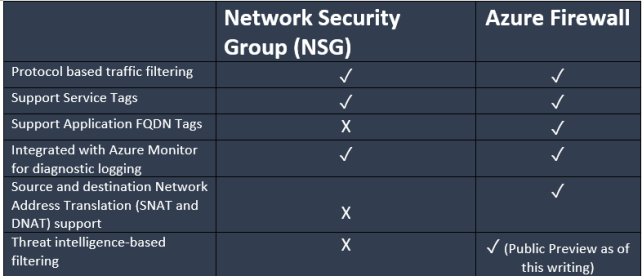
* Allow us to manage and override the default routes in Azure by creating our own Routes
* Used to redirect the traffic from the webserver to API through NVA server (network virtual appliances)
* Both internal and external traffic can be routed
* The problem with NSGs is that you are not getting enough flexibility.
* NSGs are also problematic to troubleshoot and repair.

Firewall

* a network security service that monitors and controls incoming and outgoing traffic
* Prevent from unwanted traffic

Azure Firewall

* PaaS (Firewall as a service)
* A Managed service that allow us to focus on the network configuration instead of administration
* across multiple subnets and Virtual Networks
* Highly available, scalable
* Inbound and outbound traffic filtering rules
* Grants/Denies server access based on originating IP to protect network resources
* Integrated with Azure monitor for logging and analytics
* Azure Firewall will block all traffic because the default (lowest priority) rule is set to ‘deny’
* Much more robust that NSG
* filter and analyze L3-L4 traffic, as well as L7 application traffic
* Stateful and real time firewall
* Support for FQDN (Fully qualified domain name) example- Microsoft.com
* OR can use network rules, which use source and target addresses, protocol, a destination port, and destination addresses. Our next tool in our defense line is network security groups



Typical use cases

* use NSGs when you are protecting network traffic in or out of a subnet
* use Firewall when filtering traffic to a VNet from the outside
* NSG – protection of infrastructure at a basic level
* Firewall – more robust protection, HA, threat intelligence

Azure DDoS Protection

* No configuration
* Distributed Denial of service
* SLA – 99.99%
* 2 tiers
  + Basic tier (free)
    - Automatic of public ipv4 and ipv6 addresses
    - all Azure services are protected by the Basic DDoS Protection
  + Standard tier (paid)
    - Additional mitigation and monitoring capabilities
    - Users M/L to analyze traffic patterns for better accuracy
    - $2.944/month for protection of 100 resources

Azure Security Services

* 2 components – Authentication and Authorization

Authentication (AuthN)

* Typically a username and password
* Verification of identity

Authorization (AuthZ)

* Once you are authenticated, you are now granted resources
* Authorization is what you are allowed to do
* When and where
* Implemented with RBAC

SSO

* Users remember only one username and one password to access multiple applications

Azure Active directory

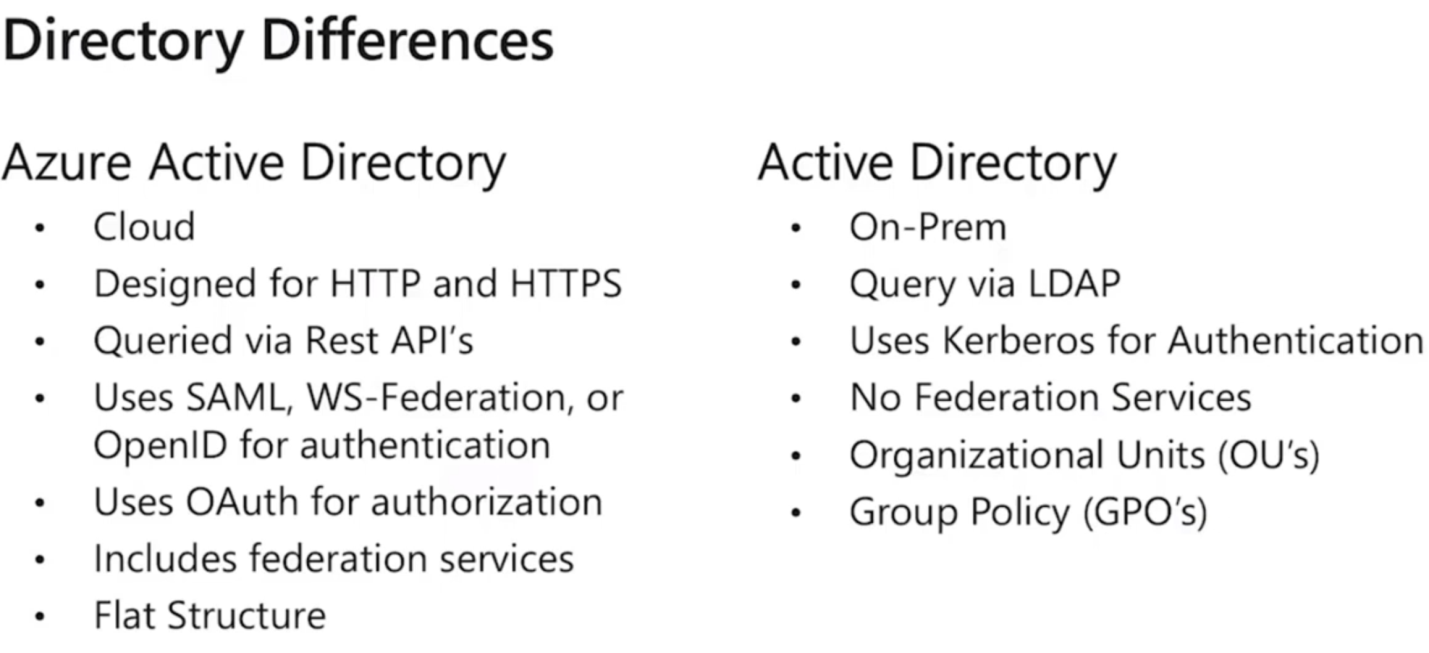
* Users and groups
* Cloud based identity and access management solution
* It provides authentication, single sign on(SSO), application management, B2B identity services, B2C identity services and decide management
* The backbone of Azure and Office 365 and other SaaS apps
* Multi-tenant – so identities from multiple tenants
* Tiers – free, basic (Office 365 Apps), Premium P1, Premium P2
* Free version can create 5,00,000 users or groups (they call them objects)
* P1 and P2 has MFA and Conditional Access
* P2 has identity protection
* Premium has SLA of 99.9%, free has no SLA
* Users are licensed on a per month/per user basis
* AAA – AuthN, AuthZ, Accounting (record keeping – ie who did what, who tried to sign on, access attempts both successful and failed, etc)
* Managed though the Azure Portal or Office 365 Portal
* Global Administrator is the highest privilege role
* There are 2 sets of RBAC role sets in Azure, one for the Resources, and one in Azure Active Directory
* RBAC roles are used to manage access to Azure resources like VMs and storage accounts, Azure AD Administrator roles are used to manage administrative or sub administrative tasks that you would do within AD

RBAC Scope can be an the management group level, subscription, resource group or resource

Azure AD role scope is always a the tenant level (one per directory)

Drastic differences between Azure A/D and A/D (OnPrem)

* With onprem A/D, Microsoft doesn't monitor sign-in attempt
* Azure AD does not have group policy or organizational units
* Use federate to link your on-premises environment with Azure AD and use this federation for authentication and authorization (Azure has a federation built in or use a 3rd party provider)



Azure AD Connect sync

* Can sync users and groups from your on prem AD to Azure AD
* ensures that identity information stored in the cloud is consistent with onprem
* Hybrid identity – single sign on for onprem and cloud

Azure Multi-Factor Authentication

* Supported by Azure Active directory by default (can be turned off is desired)
* Require 2 or more auth methods

1. Something you know (password)
2. Something you have (phone)
3. Something you are (fingerprint, iris scan, BIOmetric)

Azure MFA Verification options

* Microsoft Authenticator app
* OATH Hardware token
* SMS
* Voice call

Azure AD Conditional Access

* A way for admins to shape the authentication context to protect Azure AD Backend apps
* brings signals together, to make decisions, and enforce organizational policies
* Admin sets up specific policies to force users to do certain things to validate their identity under certain conditions
* Available only in P1, P2 tiers (Not in free)
* Example1 - trigger a MFA when the user logs in from a different location
* Example2 – allowing users to access company applications only from approved tablet devices

Azure security center

* policy compliance, security alerts, secure score, and resource hygiene (healthy, unhealthy, N/A)
* **Security, compliance, threat detection, resource hygiene**
* Continuously scanning your Azure services (PaaS and IaaS)
* evaluates security of current resources
* provides recommendations & security solutions
* Shows a Compliance score (higher is better)
* security management system that works in cloud and on prem (or hybrid)
* provides threat prevention recommendations and threat detection alerts
* Azure Advisor provides security recommendations that are actually Azure security center recommendations
* Uses intelligence to detect threats and gives us ways we can respond
* Investigation path based on detections
* Just in time VM access
* Protects azure resources in a hybrid cloud environment
* 2 tiers
  + Free (Azure Defender OFF)
  + Paid (Azure Defender ON) – pay per resource that you enable

Vs. Azure Sentinel

* For full time security professionals / infosec professionals
* A SIEM/SOAR solution that integrates w other vendors products and services.
* Can integrate w/ AWS, CloudTrail, Citirix Analytics, F5, Barracuda Firewall
* Jupyter notebooks
* Kusto Query Language (KQL)
* Logic apps

Azure Dedicated Host

* **Dedicated servers for compliance reasons**
* physical servers that host one or more Azure VMs
* Your server is dedicated to your organization and workloads – capacity isn’t shared with other customers
* helps address compliance requirements



Azure Key Vault

* PaaS
* Managed service for securing sensitive information
* Central repo to store keys, secrets and certificates
* Types of secrets: tokens, passwords, certificates, etc
* Highly integrated with Azure services such as VMs, Logic apps, Web Apps, etc
* Certification management (public and private SSL/TLS certificates)
* HSM – hardware security models
* All disks created by Azure are encrypted by default
* Centralization
* Monitoring and logging (who accessed what and when)

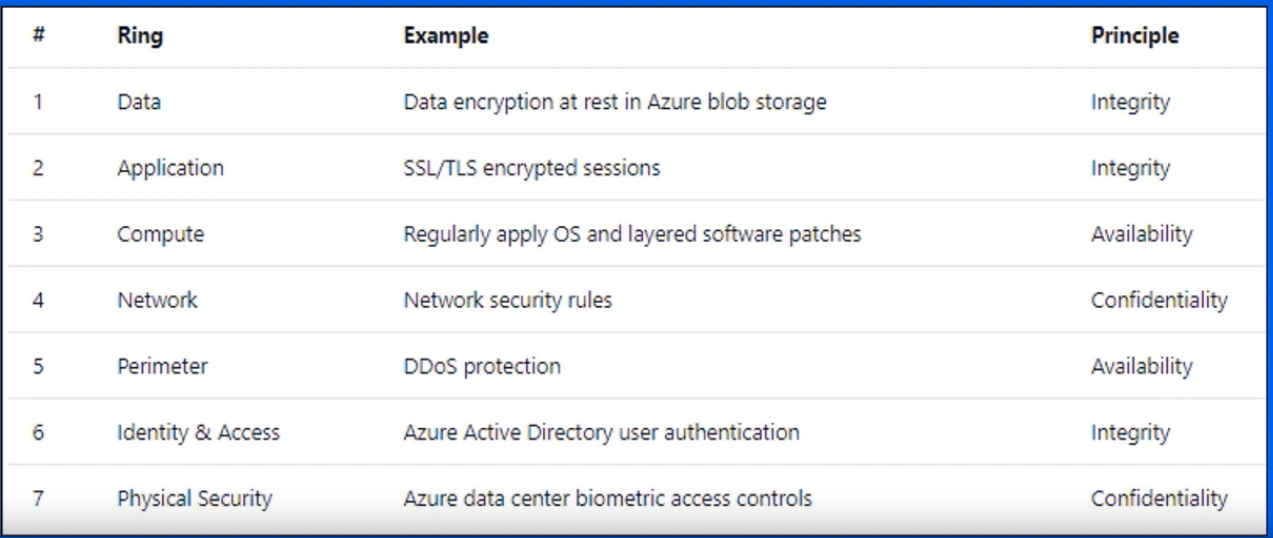
Azure Information Protection (AIP) – powered by Azure M/L

* Organizes and classifies MS Office documents and emails by applying labels
* Can label automatically when using rules OR label manually by users
* Labels both classify and optionally protect
* Can embed metadata, footers, identity watermarks, etc; in documents
* Extends the labeling and classification functionality of MS 365

Microsoft Defender for Identity (formerly Azure Advanced Threat Protection)

* Sensors to help prevent attacks and compromised identities
* Only available in premium services (P1, P2)
* Identify compromised identities and detect advanced threats
* Identify malicious attacks and insider actions
* Built in sensors to help prevent attacks
* Combines with existing services such as MS 365 Defender
* *Prevent – Detect – investigate - Respond*

Defense in Depth Model – 7 layers, each layer is isolated



Zero trust – never assume trust, always require validation

CIA Security principles

* Confidentially – least privilege principle
* Integrity – prevent unauthorized changes
* Availability

Azure policies

* enforce rules over Azure resources, ensuring compliance
* a set of conditions
* Example - in which region VMs can be created, sizing, proper tags, etc;
* govern how we create things inside Azure
* assign a policy to a management group, a single subscription, a resource group, or an individual resource(s)
* Create a policy definition -> Assign the definition to resources -> review the evaluation rules
* inheritable

Policy Initiatives

* a group of policies that are managed as a single unit to reduce the complexity of managing multiple policies
* grouping related policies into one set

Role Based Access Control (RBAC)

* Enables allowing or disallowing access to Azure portal, and controlling access to resources
* provides granular access to your resources
* Role assignment is a combination of the role definition, security principle and scope
* default roles in Azure are - *owner > contributor > reader*
* can also create custom roles
* can be applied at subscription level, resource group level, or individual resource level
* roles are inheritable and additive
* AuthZ

Access Control (IAM)

* the page in Azure portal you use to assign roles to grant access to Azure resource
* add role assignments
* roles can be applied to subscriptions, resource groups, or individual resources.

Azure Locks

* 2 types
  + Read only (denying changing of properties including deleting)
  + Can Not Delete (no Delete)
* Used to prevent unexpected changes
* As with RBAC, can be applied at subscription, resource group, or individual resource level
* Locks are inherited
* Management groups cannot be locked
* Used in conjunction w/ RBAC
* Affects users in all roles
* Need Owner or User Access Administrator role to create or delete management locks
* Example - Read only lock cannot turn off a VM inside Azure

Azure security advisor security assistance

* analyze your Azure subscriptions and make security recommendations based on Microsoft best practices

Azure Blueprints (vs ARM templates or vs Azure Policy)

* packages of entire environments including ARM templates, policies, RBAC, and resource groups applied at the subscription level.
* apply the same scope or rules to a set of Azure resources to meet compliance
* Works well with Azure DevOps
* Powerful Locking feature

RBAC – who can do stuff

Policy – what they can do or how they must do it

Budget – how much I can do financially$$$

Inheritance in Azure

* RBAC is inheritable, Policy is inheritable, Locks are inheritable
* Tags are NOT inheritable

Azure Advisor

* RECOMENDATIONS
* Accessed from the azure portal
* ProActive
* Best practices for optimizations
* Answers the question – how would MS do this?
* Recommendations (5) include cost, performance, operational excellence, reliability, and security (Azure security center) -- **CPORS**
* Recommendations should be checked weekly
* Recommendations can be saved as a pdf or csv file
* Recommendations can be sent to admins/devs when they become available
* Impacts: high, medium, low
* Actionable recommendations
* FREE!
* Always running and cannot turn off
* Not available on android mobile device

Azure Monitor

* THE HEALTH OF YOUR APPS
* Collect, analyze, and act on telemetry from cloud and on prem environments to maximize your apps availability and performance
* monitor availability and performance of resources using metrics and logs
* service failure notifications
* help you respond to alerts
* monitors usage
* Insights -> Visualize -> Analyze -> respond -> Integrate

Azure Service Health

* THE HEALTH OF AZURE
* Customizable dashboard to tracking the state of services in the regions you use
* provides insight into Azure and our resources
* components of Azure Service health:

Azure Status

* Global overview of Azure services state of health

Service Health

* Customizable dashboard for tracking the state of service in the regions you use

Azure Resource health

* Diagnose and obtain support for Azure service issues affecting your individual resources
* Status levels - Available, Unavailable, Unknown, Degraded

Azure Resource health

* Micro notification for specific azure resources (attached to individual resources)
* Status levels
  + Available
  + Unavailable
  + Unknown
  + Degraded

Cloud Adoption Framework for Azure

* collection of documentation, implementation guidance, best practices, and tools designed to assist with cloud migration

MS Privacy statement – **CPU**

1. what personal data is collected (Collection)
2. how is that data processed or used (Processing)
3. what will it be used for, including sharing (Using, sharing)

* what personal data Microsoft processes, how Microsoft processes the data, and the purpose of processing the data

Azure Trust Center

* **Security, Compliance, Privacy**
* Protection information on security, privacy, compliance, GDPR, data location, and transparency
* Regulatory standards
* CJIS, HIPAA, CSA, ISO, GDPR, NIST, etc

Service Trust portal

* Public for publishing audit report
* Regulatory compliance guides
* Compliance manager and trust documents
* **Where security advisors go to read audit reports**

Compliance Manager

* Is a Tool
* displays Microsoft and the customers data protection
* compliance for a standard or regulation
* compliance score is shown as x / y (higher score is more compliant)
* Customer managed actions / Microsoft managed actions

Azure compliance documentation

* Searchable list of legal or regulatory standards to help users should they need to comply with specific standards

Online Service Terms

* a legal agreement between Microsoft and the customer

Data Protection Amendment (DPA)

* Microsoft’s obligations with respect to the processing and security of Customer Data and Personal Data

Purchasing options for Azure

1. Web direct (directly through the website)
   1. Requires a cc
   2. Monthly billing
2. Cloud service provider (CSP – Cloud Service Provider)
   1. MS partner that handles Azure solutions
   2. Billing is handled by the CSP
   3. The CSP has help the client build solutions, troubleshoot, etc;
3. Enterprise agreements
   1. only available for large enterprises and it requires signing a contract with Microsoft.
   2. Commits to spending a specified amount of $$ of Azure services
   3. Billed annually

Factors affecting costs

1. Resource type
2. Services you receive (what tier of customer you are- free or EA for example)
3. Location Location Location (region)
4. Billing Zone

Billing Zones

* Typically, MS does not bill you for data coming into a data zone (ingress data)
* MS does charge for outgoing data (egress data) leaving the data center, and that $$ is based on zone

Geographical zones

1. Zone 1
   1. West US, East US and Europe
2. Zone 2
   1. Australia Central, Japan West, Central India
3. Zone 3
   1. Brazil south only
4. DE Zone
   1. Germany Central and Germany NE

Ingress data, data transfer between Zones, within the same Zone = free

Egress data = $$$

* 0-5 Gb/month is generally free, but paid after that
* varies by bandwidth- you get a deal for transferring a lot)

Azure pricing calculator (Online pricing calculator)

1. estimate costs prior to migration
2. Build custom quotes
3. Save estimates, share them with your team
4. Provides examples
5. Does not equal an actual bill
6. Separated by individual resources (VMs, Storage accounts, db’s, etc)
7. Azure Hybrid benefit – save money by bringing your existing on-premises Windows Server and SQL Server licenses to Azure w/ no additional cost

Total cost of ownership (TCO) calculator

* predicts the cost savings by migrating from on-premises to Azure
* provide you a comparison between the on-premises cost to running those services in Azure
* much longer and involved process
* can factor in hardware costs, software costs, electricity costs, IT staffing costs, etc

Azure cost management +Billing (located in Azure portal)

* Calculator for your resources already running in Azure
* Predicts future costs of services
* Analyze cloud costs
* Create budgets
* Optimize using recommendations
* Reporting
* Alerting

Azure Portal > Azure Advisor > Cost

* Provides cost savings recommendations for your services already running in Azure

Best practices for reducing costs

* Use existing services
* Azure advisor and implement recommendations
* Tag resources to identify an owner or department
* Spending limits and quotas on certain subscriptions (not all subscriptions allow this)
* Add alerts to subscriptions that do not support spending limits or quotas
* The person who starts a subscription becomes the default billing administrator

Azure reservations

* prepay for one or three years of service on certain Azure resources
* save up to 75% vs PAYG

Azure support: All Plans

* MS Docs

Support plans

1. Free
   1. Available to everyone
   2. No access to tech support by email or phone
2. Developers ($29/mo)
   1. is available for trial and nonproduction environments
   2. support via email only during business hours
   3. severity scale- C
3. Standard ($100/mo)
   1. used for production environments
   2. Support is available via phone and email seven days a week, 24 hours a day
   3. Response time < 1 hour
   4. Severity level - A
4. Professional direct ($1000/mo)
   1. business critical applications and includes everything included in Standard support plus onboarding services, service reviews, and Azure Advisor consultants
   2. allows for escalation of priority issues and it also includes architectural and proactive guidance
5. Premier
   1. Technical account manager
   2. used when you're heavily dependent on Azure and other Microsoft services
   3. includes everything in the Professional Direct support plan plus an initial response time of less than 15 minutes
   4. also includes custom architectural support, implementation assistance, and support for all other Microsoft products
   5. can only be purchased by companies that have an Enterprise Agreement (EA), and the pricing is variable

Not all support plans are available to all customers

Dependent on your subscription and your agreements with MS

Open a support ticket in Azure

* 4-step process
  1. Provide basic information about the problems you’re having
  2. You will be provided some solution based on your scenarios
  3. If the solutions do not rectify the problem, Provide more details - this will be dependent on the subscription type and your support plan
  4. your ticket will be reviewed and created

Other support channels

* Stack Overflow for assistance, Server Vault, Twitter, Azure feedback forums, MSDN Azure forums

Azure Knowledge center

* Searchable Online db

Azure SLAs (Service Level Agreements)

* Contains performance details of an Azure service (how many nines)
* also contains information on what happens if that SLA is not met
* measured in uptime
* Public/Private preview, free and shared tiers do not have SLAs
* No SLAs for Visual Studio subscribers who get free monthly credit (as they are not really paying anything)
* Service credit on your next invoice if MS violates an SLA – service credit is either 10% or 25%
* Downtime per week/month/year shows the maximum
* Range from 99.9 to 99.99%



Azure VM SLA Example

* 99.95% connectivity to at least one instance for all VMs that have 2 or more instances deployed in the same availability set

Components of an SLA

* Connectivity guarantees
* Uptime
* Service credits (%)

Composite SLA

* Combining 2 or more SLAs for different services
* Multiplication shows us the maximum downtime
* Web app (99.95%) X SQL DB (99.99%) = 99.94%

Application SLA

* The SLA provided to clients that we offer
* 2 considerations
  + Response time
  + Is this realistically achievable?

Azure Service Lifecycle

* Private Preview > Public Preview > GA
* Not all preview products make it to GA

Preview features (coming soon)

* MS does not recommend using previews into production environment
* Gives time to evaluate the service before it becomes generally available (GA)
* Preview products don’t have an SLA, cost or support (not supported)
* 2 types of previews
  1. Public
     1. Indicated as preview in the portal
     2. Available to all Azure users, but not available in all regions
  2. Private
     1. Only available to certain Azure users
     2. Must request access to test these features
     3. Must be opted into

GA

* When a preview feature has been evaluated, it becomes Generally Available
* Available to all Azure users
* SLA guarantee

Portal Preview

* Updates to the portal (navigation, etc)
* [http://preview.portal.azure.com](http://preview.portal.azure.com/) instead of [http://portal.azure.com](http://portal.azure.com/)

Feature updates

* A website that shows previews, in development

Azure deployment

* organizing structure for resources in Azure has four levels
  1. management groups
  2. subscriptions
  3. resource groups
  4. resources
* Criminal Justice Information Services (CJIS) – Azure is one of the largest cloud provider that contractually commits to conformance with the CJIS Security Policy, that commits Microsoft to adhering to the same requirements that law enforcement and public safety entities must meet.
* Cloud Security Alliance (CSA) STAR Certification – Azure, Intune, and Microsoft Power BI have obtained STAR Certification, that involves a rigorous independent third-party assessment of a cloud provider’s security posture. This STAR certification has been based on achieving ISO/IEC 27001 certification and meeting criteria specified in the Cloud Controls Matrix (CCM).
* General Data Protection Regulation (GDPR) – GDPR in effect from May 25, 2018 imposes new rules on companies, government agencies, non-profits, and other organizations that offer goods and services to people in the European Union (EU), or that collect and analyze data tied to EU residents.
* EU Model Clauses – Microsoft offers customers EU Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU.
* Health Insurance Portability and Accountability Act (HIPAA) – Azure offers customers a HIPAA Business Associate Agreement (BAA), stipulating adherence to certain security and privacy provisions in HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH) Act. In order to assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.
* International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) 27018 – Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, covering the processing of personal information by cloud service providers.
* Multi-Tier Cloud Security (MTCS) Singapore – After rigorous assessments conducted by the MTCS Certification Body, Microsoft cloud services received MTCS 584:2013 Certification across all three service classifications—Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).
* Service Organization Controls (SOC) 1, 2, and 3 – Microsoft-covered cloud services are audited at least annually against the SOC report framework by independent third-party auditors.Microsoft cloud services audit covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.
* National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) – NIST CSF is a voluntary Framework that consists of standards, guidelines, and best practices to manage cyber-security-related risks. Microsoft cloud services have undergone independent, third-party Federal Risk and Authorization Management Program (FedRAMP) Moderate and High Baseline audits, and are certified according to the FedRAMP standards.
* UK Government G-Cloud – UK Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom. Azure has received official accreditation from the UK Government Pan Government Accreditor.

