How to approach exam
Basically, a big marketing thing. Just know what Azure is capable of and what it does.

1: Cloud Concepts

Cloud Services: Benefits and Considerations. The cloud provides 7 technical benefits – HA/FT, DR, Scalability, Elasticity, Business Agility, Economies of Scale, and a consumption-based approach.

HA allows for the ability to maintain an acceptable level of performance (albeit degraded) in the event of a failure with the underlying infra. Azure achieves this in 3 ways – through resilient datacenter design (redundant power, cooling, networking, and compute), through usage of AZs, and with Azure regions. **FT** allows systems to continue working normally even if some components fail. There are 2 types of FT proactive vs. reactive. Proactive FT is performed through LB, monitoring, multi-AZ deployments. Reactive FT is achieved via backups and restores.

For **DR,** There are 4 ways to restore failed workloads with the cloud – onprem-to-onprem, onprem to azure, other cloud to Azure, Azure-to-Azure.

The Azure cloud is made of regions, geographies, and availability zones.

The public cloud provides 5 business benefits - elasticity, business agility, economies of scale, opex-based budgeting, and a consumption-based model. **Elasticity** is based on scalability and it's a way to allow you to quickly scale in/out (horizontally), or up/down (vertically) depending on workload. Elasticity can be a manual or automated. It drives cost efficiency b/c you just pay for what you're using at the time. **Azure autoscaling** allows you to achieve this with compute workloads. **Elasticity** paves way for business agility, basically allows the business to rapidly adapt to changing market conditions cost-effectively while ensuring there's enough capacity to meet demands.

Business Agility in Azure is built on **6 principles –** (1) Reduction of **time to value,** (2) focus on **business innovation,** (3) achieving low decision-to-action **latency**, (4) drive **economic effectiveness and efficiency,** (5) **rapidly adapt** to changing market conditions and new technologies, and (6) maintain **flexibility** with deployments and architecture.

The public cloud is built on the concept of **economies of scale –** the cost of an individual item goes down as the number of total quantities you buy at once increases. Azure achieves EoS in 3 ways – (1) supply side savings for raw materials and hardware (MSFT builds DCs in clusters and buys h/w in bulk), (2) demand side savings by having more customers share services offered, and (3) multi-tenancy savings by having lots of businesses become tenants of shared commodity hardware in Azure DCs.

Azure allows to shift IT investment from a Capex to an Opex approach, which is associated with lower-overhead and overall lower costs. This is the core of the **consumption-based model** which has no upfront investment and you pay-as-you-go for services (usually by the minute, by GB of data stored, or per GB of data transferred depending on the service) that you use. With Azure you can still perform reservations if the forecasted workload is known so you can use services at a lower cost.

IaaS vs. PaaS vs. SaaS – think "Host" vs. "Build" vs. "Consume". **IaaS** is when azure manages up to the hypervisor and we bring our own OS. It's the most flexible and gives most control but is more work to deploy/maintain. **PaaS** is when Azure products a pre-made platform that we build our solutions over, like MS SQL databases. It's good for vanilla/common apps where the customer focuses on *building* their solution on platforms offered. **SaaS** is when you just show up, bring your data and users and just start using whatever product they offer.

Azure IaaS products = virtual networks, virtual machines, etc. Azure PaaS products = app service, search, CDN. Azure SaaS = O365

Private vs. Public vs. Hybrid Clouds. A *private cloud* is made of only a single tenant. Usually it's built by one company for their own use within their own datacenter. With Azure, a private cloud is build using **dedicated servers** to host our own VMs. Pros – fully customizable, highly secure, and better performance. Cons – higher capex/opex costs, less elasticity. A *public cloud* is basically Azure/GCP/AWS where many tenants share a common hardware and network infrastructure managed by a cloud service provider. The pros were described earlier. The cons include – less customizability, potentially more latency, and potential governance issues. A *Hybrid Cloud* is when you combine the best of both worlds. Lots of flexibility with no capacity ceiling but you have a higher upfront cost and you risk underutilizing resources. Not to mention compatibility issues may become a factor.

2: Azure Services

Azure Architecture. Made of regions. A region contains multiple AZs. Each AZ contains multiple DCs. A **region** is a geographical location made of many AZs connected together via a regional low-latency network. Deploying solutions in a multi-region approach provides for resiliency at a global scale. An **Availability Zone** is made of a few datacenters that is located within a reasonably close geographical area. While a region provides for global resiliency, AZs provide for resiliency at the datacenter level. With Azure, data can either be locally redundant (replicated btw multiple AZs within one region) or regionally redundant (replicated across many regions). Many Azure services can be set up in a multi-AZ deployment.

The Azure architecture provides 4 benefits. **AZs** allow solutions to be highly available, **Regions** allow apps to reach resiliency at a global scale while maintaining compliance, **Resource Groups** allow resources to be managed and organized administratively, and the **ARM** provides a centralized, consistent method for managing individual resources within Azure.

The **Azure Resource Manager** is a central back-end service that is used to deploy and manage your assets within Azure. It's made of APIs that allow for mgmt. and deployment functions of Azure services. You interact with the ARM through either the CLI, Web GUI, or APIs. You can use ARM templates to model and repeatedly deploy solutions/apps in a highly consistent manner and state. ARM templates are JSON documents that defines the resources to deploy and the configuration parameters for those resources. The ARM integrates tightly w. AD/ADFS for access controls within Azure. It handles all the intricate low-level technical details to deploy and manage the resources we choose within Azure.

Azure Products and Services. Take note of which are IaaS vs. PaaS vs. SaaS. There are **5 main product groups –** COMPUTE, NETWORKING, STORAGE, DATABASES, and MARKETPLACE.
Compute products incl. VM, VM scale sets for IaaS. App service for PaaS. Networking products incl. VNETs, LBs, VPN GWs, App GWs, and CDN. Storage products incl. blob and file storage. Database offerings incl. CosmosDB, SQL DB, DB Migration Service, and SQL data warehousing. **Marketplace** is not a product, it's where you go to get pre-made solutions from 3rd-party partners of MSFT. It's basically an "app store" equivalent for Azure. Partners list apps/services or pre-made solutions that can be instantly imported to Azure. You can find SaaS apps, VMs, solution templates, and Azure managed apps on there. You select the product to deploy for out-of-the-box functionality.

Azure Compute virtual machines is an IaaS offering that allows VMs to be spun up on-demand. They're cheap b/c a lot of them can fit on a single physical shared platform. You can start a VM small and scale up as needed. You can create a VM scale set which is a pool of VMs that auto-scales based on inbound traffic and demand. You can scale the total number of active VMs based on the load at that time. Azure VM scale set = AWS Auto-scaling groups. It works off a base VM image so all provisioned VMs are consistent within the group. Azure App Service is a PaaS offering that allows to host web apps, mobile back-ends, REST APIs built in any language w/o having to manage the infrastructure. Azure manages the underlying platform (Linux/Windows), autoscaling, and connectivity to Github or public code repos. Azure app service allows you to "just run the app" w/o having to worry about infrastructure.

The Azure Networking Product group is made of virtual networks, load-balancers, VPN gateways, App Gateways, and the Azure CDN.

An **Azure Virtual Network** is the main component of any Azure networking solution. It allows for (1) resources to talk to each other, (2) grouping and isolation of diff. resources for compliance purposes, (3) organizing resources into subnets and security groups for granular traffic flow. On a VNet, **VPN Gateways** can be deployed to allow Azure resources to communicate to/from either on-prem resources or other Azure VNets. For highly available application infrastructure design, **load-balancers** can be used for basic LB, but the **Azure App Gateway** allows for more customization of inbound application traffic flows. **Services deployed at a global scale** can leverage the **Azure CDN** to cache static content around the world to speed up delivery of those content to the end users, which reduces latency of static content delivery.

Azure Networking: https://azure.microsoft.com/en-us/product-categories/networking/

Azure Virtual Network: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview

Azure VPN Gateway: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways

Azure Load Balancer: https://docs.microsoft.com/en-us/azure/load-balancer/load-balancer-overview

Azure Application Gateway: https://azure.microsoft.com/en-us/services/application-gateway/

Azure Content Delivery Network: https://docs.microsoft.com/en-us/azure/cdn/

To store data on Azure **5 products are offered –** *IaaS* storage services incl. Azure storage disks and Azure files. *PaaS* offerings include Azure Blobs, Tables, and Queues.

Storage disks allows you to save VHD images for Azure VMs. The VHDs can be mounted to VMs. You can upgrade to premium storage tier which uses SSD to lower disk access time and provide higher I/O rates. This is the de-facto way to store disk images that will be mounted to Azure VMs. You can only use product this to store VHD images and nothing else.

Storage files is an NFS service that allows you to store both VHD images for VMs as well as everything else. It's a full-fledged file system that you can connect to using SMB or REST endpoints. It's good for when you need to lift and shift legacy file shares from on-prem to Azure.

An **Azure Blob** is an object store for unstructured data, which can be anything like JSON, text, aggregated reports. It's basically a dumping ground for generic data that's not a file. It's not a database. Every item PUT onto a blob becomes just another object. Each object is given an endpoint ID which can be used to GET data out of the blob. It's good for storing metadata, images, and documents. Blobs have 3 storage tiers – HOT tier for highest data access speed (instantly available), COOL tier for some level of access latency, and ARCHIVE tier which can take up to 4 hours to retrieve data.

Azure tables is a NoSQL offering. It gives a bit more control over unstructured data by converting them into tables and rows, but without a normal schema like a regular SQL DB. It's basically a key-value pair and not a relational DB.

For integration and moving data btw. services, **Azure Queues** is used. It's a FIFO queue t hat allows for msgs to be written by one app and read by another app. Queues are used to decouple components from each other. All components read and write to the queues to exchange messages.

There are many ways to approach deployment of **databases within Azure.** You could do PaaS using Cosmos DB or Azure SQL/SQL Data Warehouse. OR you could just go IaaS and spin up a Compute VM then install a SQL server on there.

CosmosDB is a full-featured, globally-distributed, multi-model No SQL DB which works similar to Mongo DB. *Globally distributed* means that the svc automatically handles scaling across multi-regions and data replication for us. *Multi-model* allows the data to be queried in many ways like SQL statements, or through APIs. It supports integration with Apache spark for analytics and is less expensive than SQL offerings.

SQL Data Warehouse is used to store very large amounts of data. The ideal use case would be a data lake where you store the end result from some analytics processes. Big Data solutions take data from many sources and stores it somewhere that's dedicated for very large scale, unstructured, multi-type data (like an Azure Data Lake store). Other apps can then use data from the data lake. Parellel processing is used to rapidly execute complex queries against the data in the lake.

Azure DMS is a service that allows migration of data from other DBs to Azure DBs with minimal downtime. It offers 2 methods of migration – online (via replication) vs. offline (via backup/restore). You can move a SQL database from anywhere to Azure.

Azure Solutions is not the same as Azure products and services. Solutions are pre-built, all-in-one packages made of individual Azure products/services that work together out of the box.. 4 categories of solutions include IoT, Big Data and Analytics, AI, and Serverless Compute.
Azure IoT solutions is made of one or more devices that talk to one or more back-end services running in the cloud. Devices can be home appliances or electronics which do 2-way communication to the Azure IoT service. Azure has 2 IoT offerings, Central and Hub. ***IoT Central*** is a fully managed SaaS solution which allows to connect, monitor, and manage IoT devices at scale. It comes with a pre-built workspace that can be used to deploy IoT solutions w/o any coding. ***IoT Hub*** is a PaaS offering that is the back-end for IoT Central. It's the messaging service that connects devices to the IoT Central for communication. You can built your own custom IoT management infrastructure on top of IoT hub.

Big Data refers to technologies that deal with petabyte-scale data. Typically used for business insight and forecasting. It includes technologies that allow to store petabytes of data and query those within a reasonable amount of time.

A typical big data lifecycle has 5 phases – starting from many **data sources,** a mechanism **ingests** data from those sources and **stores** it in either Azure Datalake storage or Blob storage. Once stored, data is **prepped** for analysis and ML models are then **trained** to analyze that data. Once trained, the models **serve** the analysis of that data for reporting/dashboarding. (Ingest, Store, Prep, Train, Serve).

Azure Big Data and Analytics offerings include SQL Data Warehouse, HDInsight, Data Lake, and Data Lake Analytics. **SQL Data Warehouse** is an enterprise data warehouse used to store results from the analysis of Big Data queries and analysis. It's typically used at the end of the big data lifecycle. It can perform parallel processing to quickly run complex queries across petabytes of data. **HDInsight** is the Azure-implementation of the Hadoop framework. It works on a cluster of servers which uses nodes to perform the same work on a subset of a larger amount of data in a divide-and-conquer approach. This allows for massively parallel processing to be executed on the data. Once processing is done, the results from each processing stream is aggregated into a single resulting dataset.

Azure DataLake is made of 2 individual products – **Data Lake store** which allows unstructured, semi-structured, and structured data to be stored within Azure. While **DataLake analytics** provides a web portal to create analytics jobs which can be run on-demand. You use **HDInsight** if you want to engineer a custom Big Data query from start to finish, and you use **DataLake Analytics** if you want Azure to help create and manage the analytics jobs for you.

AI in Azure consists of Azure ML and ML Studio. **ML** is a data science technique that allows computers to use existing data to try and predict what may happen in the future. The ML program goes through data to find patterns and start correlating them to make learning rules automatically. You don't need to make those rules, just provide the ML engine with your data, and it will automatically determine the rules based on the patterns within that data. The output from a ML program is called a *model,* which is an aggregate of all the rules that the ML engine has figured out, that can be used to process more data in a streamlined manner. You can publish your ML models on Azure marketplace as a service.

Azure ML Service is a PaaS offering. It's good if you already work in a Python environment, you need control over the ML algos, or if you need to use OSource ML libraries. Good for custom ML solutions. **Azure ML Studio** is a SaaS offering that allows to build, train, and deploy ML programs without having to code. You just define workflows and connect pre-built components together into an ML flow.

Azure serverless compute products include Functions, Logic Apps, and Event Grid. **Serverless compute** is a way to use Azure-managed servers to run our code, thereby making it "serverless" to us. You upload your code and configure triggers that will cause that code to run. Pay for only when the code is running and nothing more = true on-demand model. There are 3 ways to use serverless computing – web app backends, mobile app backends, and real-time file processing. It allows for event-driven, automated, auto-scaling compute. **3 Azure serverless offerings are functions, logicApps,** and **EventGrid.**

Azure Functions is the most common, you upload code, configure event triggers to process data – is good for simple workloads. LogicApps is used to create entire workflows and processes to perform more complex tasks. So you can create individual functions, then create LogicApps to sequence each function together into a single workflow. EventGrid is a fully managed serverless event routing service which helps handle event routing from any source to any destination, for any application. It's a fully automated, serverless, event processing service which eliminates the need for queue reads. As messages arrive, they're immediately processed.

The **benefits of Azure solutions** is that it's fully managed for us, this helps reduces costs and shortens time-to-market. It also frees up time as we don't need to manage reliability, security, scalability, or individual resources.

Azure Management Tools consists of 4 common tools – the Azure CLI, Azure powershell, Azure portal, and Azure advisor. All run on the ARM in the back-end. The **Azure CLI and Powershell** platforms are both installed on the local PC, both are open source and supports Windows/Mac/Linux. It gives a command line way to manage Azure resources. They basically call out to the ARM which gives access to each of the Azure APIs. **Azure Portal** is the GUI way to manage Azure from a web browser and is the default. **CloudShell** is a component within the Azure Portal which provides a CLI within the web browser.

The **Azure Advisor** is not a management tool but rather a personalized recommendation tool that analyzes existing deployments for optimization. It uses ML and analytics to provide recommendations as to how to improve cost effectiveness, performance, security, availability of our resources (which are the 4 categories it offers advice on).

3: Security, Privacy, Compliance, and Trust

Network Security in Azure consists of 3 products – The Azure Firewall, Azure NSGs, and Azure DDoS protections.

Azure Firewall is a managed, cloud-based security service that protects VNet resources. Deployed in a hub-and-spoke model. All VNets connect to the Azure firewall which performs rule-based inspection. The Azure Firewall has 6 features – (1) built-in HA, (2) unlimited traffic scalability, (3) filtering HTTP traffic using FQDNs, (4) filtering layer 3 traffic using NSGs, (5) integration with MSFT TI, (6) integration with Azure Monitor and Sentinel logging.

Azure DDoS protection prevents **3 types of attacks – volumetric (floods) attacks, protocol (protocol exploits) attacks, and resource attacks (application exploits).** The issue with deploying elastic cloud services is that resources scale up with demand. In a DDoS attack, resources will auto-scale up to accommodate traffic volume, which incurs a huge cost at the end. Azure DDoS protection prevents this from happening. Comes in **2 editions** – **basic and standard.** Standard provides real-time monitoring, analytics, deeper metrics/logging and more customization. Price is per GB.

NSGs are a part of the Azure firewall that allows us to create rules to define ingress/egress traffic. Basically a stateful firewall. They **do not support deny rules, only permit rules.** Each NSG has **4 properties – the name, the region, its resource group, and the rules defined within that group.** NSG rules can be applied to **(1) the internet, (2) VNets, or (3) LBs.**
Inbound rules are processed first, then outbound. Rules **can be configured with a priority – lower priority numbers *before* higher priority numbers.**

Neither NSGs or the Azure FW perform traffic encryption. Use App GW instead.

4 **rules** for deploying Azure security – **isolation** (use diff. VNETs to segment network and isolate resources), **least privilege** (limit traffic and rules to only

what's required), **use NSGs** to enforce network level least privilege, **use Azure FW and DDoS protection** at the perimeter.

Azure Identity Services handle AuthN and AuthZ. The primary Azure Identity service is **Azure AD (AAD).** AuthN is proving you are who you say you are, and AuthZ is specifying what you're allowed to access and what actions you're allowed to perform. You start the process with AuthN by providing a username and credential (password, OTP, biometrics). Once validated, you get a security token that proves your identity to the system. Security tokens contains claims which is the part of the token that determines what permissions you have within the system.

Within a JSON formatted token, the scope section is the identity's claim, and is used to provide authorization for the user into various systems. Tokens allow an identity to only have to authenticate once to AAD and use its identity assertion to access various systems in Azure, provided it has the authorization to do so.

https://docs.microsoft.com/en-us/azure/active-directory/develop/authentication-scenarios

Authenticate > Get security token > Use claims within the token to access resources.

Azure MFA allows for providing your identity using 2 of 3 available methods – something you know, something you have, or something you are. Has a separate cost and is added-on to the price of AAD.

Azure AD (AAD) is an online identity store in Azure that keeps usernames/passwords and is used as means to authenticate/authorize users. It's a comprehensive, highly available, and fully scalable IAM solution. Built around users and groups. A user is the basic object that we pay for (price is per user). Multiple users can be placed into groups for organization, but groups cannot be used directly for authentication, only users can authenticate.

Licensing is per user. Multiple license levels are available, and is set on a per user basis. A user can have multiple licenses assigned and the one with the most features will take effect.

You can sync on-prem AD over to AAD using Azure AD Sync. AAD supports self-service, SSO, and MFA. Free limits to 500k users, 10 free apps, no metrics/reporting . Can upgrade to Premium P1 or P2 for advanced IAM functions.

Azure Security Tools and Features

Service	Description
Azure Security Center	A cloud workload protection solution that provides security management and advanced threat protection across hybrid cloud workloads.
Azure Key Vault	A secure secrets store for the passwords, connection strings, and other information you need to keep your apps working.
Azure Monitor logs	A monitoring service that collects telemetry and other data, and provides a query language and analytics engine to deliver operational insights for your apps and resources. Can be used alone or with other services such as Security Center.
Azure Dev/Test Labs	A service that helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost.

Service	Description
Azure Storage Service Encryption	A security feature that automatically encrypts your data in Azure storage.
StorSimple Encrypted Hybrid Storage	An integrated storage solution that manages storage tasks between on-premises devices and Azure cloud storage.
Azure Client-Side Encryption	A client-side encryption solution that encrypts data inside client applications before uploading to Azure Storage; also decrypts the data while downloading.
Azure Storage Shared Access Signatures	A shared access signature provides delegated access to resources in your storage account.
Azure Storage Account Keys	An access control method for Azure storage that is used for authentication when the storage account is accessed.
Azure File shares with SMB 3.0 Encryption	A network security technology that enables automatic network encryption for the Server Message Block (SMB) file sharing protocol.
Azure Storage Analytics	A logging and metrics-generating technology for data in your storage account.

Service	Description
Azure SQL Firewall	A network access control feature that protects against network-based attacks to database.
Azure SQL Cell Level Encryption	A database security technology that provides encryption at a granular level.
Azure SQL Connection Encryption	To provide security, SQL Database controls access with firewall rules limiting connectivity by IP address, authentication mechanisms requiring users to prove their identity, and authorization mechanisms limiting users to specific actions and data.
Azure SQL Always Encryption	Protects sensitive data, such as credit card numbers or national identification numbers (for example, U.S. social security numbers), stored in Azure SQL Database or SQL Server databases.
Azure SQL Transparent Data Encryption	A database security feature that encrypts the storage of an entire database.
Azure SQL Database Auditing	A database auditing feature that tracks database events and writes them to an audit log in your Azure storage account.

Service	Description
Azure Role Based Access Control	An access control feature designed to allow users to access only the resources they are required to access based on their roles within the organization.
Azure Active Directory	A cloud-based authentication repository that supports a multi-tenant, cloud-based directory and multiple identity management services within Azure.
Azure Active Directory B2C	An identity management service that enables control over how customers sign-up, sign-in, and manage their profiles when using Azure-based applications.
Azure Active Directory Domain Services	A cloud-based and managed version of Active Directory Domain Services.
Azure Multi-Factor Authentication	A security provision that employs several different forms of authentication and verification before allowing access to secured information.

Service	Description
Azure Backup	An Azure-based service used to back up and restore data in the Azure cloud.
Azure Site Recovery	An online service that replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location to enable recovery of services after a failure.

Service	Description
Network Security Groups	A network-based access control feature using a 5-tuple to make allow or deny decisions.
Azure VPN Gateway	A network device used as a VPN endpoint to allow cross-premises access to Azure Virtual Networks.
Azure Application Gateway	An advanced web application load balancer that can route based on URL and perform SSL-offloading.
Web application firewall (WAF)	A feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities
Azure Load Balancer	A TCP/UDP application network load balancer.
Azure ExpressRoute	A dedicated WAN link between on-premises networks and Azure Virtual Networks.
Azure Traffic Manager	A global DNS load balancer.
Azure Application Proxy	An authenticating front-end used to secure remote access for web applications hosted on-premises.
Azure Firewall	A managed, cloud-based network security service that protects your Azure Virtual Network resources.
Azure DDoS protection	Combined with application design best practices, provides defense against DDoS attacks.
Virtual Network service endpoints	Extends your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection.

Azure Security Center is a SIEM. It's a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises. Uses **Microsoft Monitoring Agents** that can be installed on any host regardless of OS or location (on-prem vs. Cloud). The MMA collects events, telemetry, and metrics from servers and aggregates them to the ASC

which then forwards those events over to the SAE (Security Analytics Engine). **SAE** provides threat alerts and recommendations on how to secure workloads. All Azure PAAS services' underlying VMs are protected by ASC as they all have MMA installed. The ASC is built on top of **Azure Policy Controls** which can be defined and applied to mitigate security risks. The ASC monitors all Azure resources security posture against policies in Azure policy controls for non-compliance and provides trending data over time.

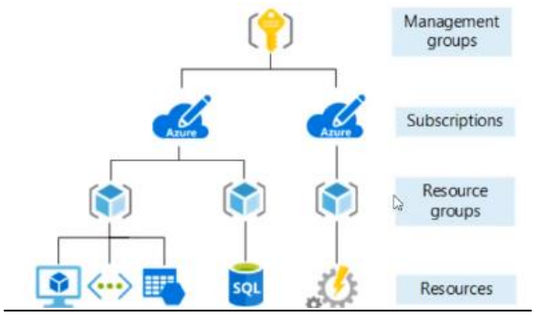
2 pricing tiers – free and standard. Standard provides security event collection, more customization, and built-in and custom alerts. Standard tier pricing varies per hour depending on type of resource being managed.

Azure Key Vault encrypts and safeguards keys – auth, storage account, data encryption keys, SSL certs, and passwords. *The worst way to use credentials in apps is to hard-code them into the apps themselves.* Key vault separates key management from key usage. Works with AD service accounts. You create a key vault and store your keys there. You create a service account for the app. The app uses the service account to auth to Azure AD and pass its security token along with the URL of the key it's trying to access. Key vault authorizes usage of that key. The app uses the key to access resources without the developers ever needing to know or code in the keys manually. Premium level uses an HSM to store keys. Most operations with key vault surrounds usage of secrets and certs.

AIP is Azure Info Protection which is a cloud based DLP solution that helps classify and protect docs and emails. An agent is installed on PCs that auto-classify data and protects them in docs and emails. Policies can be applied to data based on classification. Can look through content to search for patterns of data that might fit into a classification. Can point to manually scan a specific folder. Billed per user/month for premium features. 4 editions – free, O365, premium P1 and P2.

ATP is a cloud based threat prevention solution that identifies, detects and helps investigate advanced threats, compromised identities, and malicious insider actions. Uses data from other Azure svcs and aggregates them into a consolidated view – most of the data comes from Azure AD, Azure Monitor, and ASC. ATP works closely with Azure AD to detect brute force attacks, infected devices, config vulns, leaked creds, and suspicious login attempts. It can aggregate all discovered vulns and threats to give mitigation recommendations or auto-block active attacks.

Azure Governance is a set of products that allow for management of Azure resources at a large scale. It's made of Azure Policies, Azure Initiatives, RBAC, Resource Locking, and Azure Advisor.



Azure Policies is used to enforce rules on various resources or resource groups. It comes with a built-in policies available for quick start. Policies can be applied at the mgmt. group, subscription, or resource level and those policies will be inherited downwards. Policies allow us to do 2 things – evaluate resources against an established compliance standard and mark non-compliant resources, and to audit/effect policies against resources. *Non-compliant resources are NOT auto-remediated, just alerted.* You can create many Azure policies and them together into a single **Azure Initiative.** A single policy can belong to multiple initiatives

Azure Initiatives is a collection of many Azure Policies tailored at achieving a single strategic goal. I.E.: an initiative to reduce cost within Azure might contain a policy to restrict larger VM sizes, and another policy to limit storage sizes. Initiatives are **applied to mgmt. groups, resource groups, or subscriptions.** A resource needs to be compliant to all policies within an initiative to pass the initiative. You might have an initiative that **enables vuln monitoring within the Azure cloud environment.** Within this initiative you have 3 policies – **monitor unencrypted SQL DB in security center, monitor VM OS vulns in security center, and monitor for missing endpoint protection in security center.**

RBAC is an authorization system built on ARM to provide fine-grained access mgmt. of every Azure resource. 3 roles are provided – **owner** (can do anything on the resource), **contributor** (can create resources but can't grant/deny access to any existing resources to other users), and **reader** (only read existing resources, no ability to create new resources). RBAC if applied to the subscription level takes effect for all resources within that sub. When you create a subscription, you automatically become the owner of that sub. When you try to create a new resource, ARM checks that you have permissions in that sub to create resources within it.

Resource locking is a way to prevent users from accidentally deleting critical resources. Can set to **CannotDelete** (prevents deletion but not modification), or **ReadOnly** (prevents deletion and modification). Can be config'd via portal, resource manager templates, Azure Powershell, CLI, or REST API.
In Azure, subscriptions and resource groups are mandatory. Management groups are optional.

Azure Advisor provides 4 categories of recommendations – availability, security, performance, and ops excellence. It takes data from security center and provides a more holistic picture. It goes above the security center to give a single dashboard for all Azure related recommendations.

Monitoring and Reporting in Azure can be done using 2 tools – Azure Monitor, and Azure Service Health. You use Azure monitor to keep an eye for your own applications and workloads. A lot of Azure svcs already integrate with it. You get a single monitoring platform for all of your Azure resources. Data can be imported as either metrics (measures perf. Over time), or logs (raw events). 5 types of data can be collected – app mon. data, guest OS mon. data, Azure resource mon. data, Azure subscription mon. data, and Azure tenant mon. data. Monitoring data can provide insights for dashboarding – export to PowerBI. Rules can be set up based on metrics collected and can alert automatically when a criteria is met. Collected events can be used to monitor trends and respond to events as they come in.

Azure service health is a service that tracks MS Azure global infra health. It gives 3 key info – (1) service issues, (2) planned maintenance, and (3) health advisories or changes to Azure svcs

You use the Azure monitor to collect log data for your own apps and visualize performance/optimization over time. Service health is used to see if an issue with our workloads is caused by a larger problem within Azure. *Use both as a best practice.*

Azure Privacy, Compliance, and Data Protection Standards. 4 main compliance standards that Azure complies to are the GDPR (EU), the ISO, NIST, and FedRAMP.

GDPR is for EU that states how PII and sensitive data bout EU citizens should be protected. It's applicable to anyone that does busn. In the EU or holds info about EU citizen. Azure maintains GDPR compliance in 5 ways – (1) Providing a **Data Subject Request in the GDPR portal** that can be used to service request for PII from individuals, (2) **Azure policy and initiatives** to configure resources in consistent manner (i.e.: ensuring data encryption), (3) **compliance manager** to track/assign/verify org's compliance with GDPR, (4) **AIP** to ensure data is encrypted, (5) **ASC** to respond to threats to data.

ISO is an intl' standard setting org, they don't enact laws but sets standards for orgs to meet to become ISO-copmliant. ISO 27000 is the relevant set of standards that Azure complies to.

NIST is a standard setting org for gov't agencies. They provide the NIST cyber framework. They help comply w/ other areas for govt agencies like HIPAA and SOX. Compliance with NIST allows Azure to service government agencies.

FedRAMP is another framework set by NIST to ensure cloud vendors used by agencies comply with standards.

The MSFT Privacy statement explains what PII is collected and how it's processed when using MSFT services. It puts MSFT's commitment to privacy in writing and details policies and procedures in plain English. Basically, MSFT will only use customer data for the purposes of providing services to the customer as agreed upon.

Trust Center > Service Trust Portal > Compliance Manager.

MSFT Trust Center is a portal to all things security, compliance, and privacy related. It puts together security, privacy, compliance, transparency, products/svcs, service trust portal and other privacy related resources in one place. The **Service Trust Portal** is important as it contains audit reports that can be used to verify Azure cloud's compliance to various regulations.

The **Service Trust Portal** is part of the MS Trust center. It the place that contains audit reports of all privacy/compliance/audit reports of Azure's infrastructure. You can request 3rd-party audit reports like SOC, PCI-DSS, ISO 270001, FEDRAMP. It also contains results of prior internal audit and risk assessments, and gives an updated view of the compliance state for the Azure infrastructure.

Within the Service Trust Portal (STP) is the **MS Compliance Manager**. It's a tool that can be used to ensure that our org is compliant to whatever standards we need to comply with. It allows us to cross-compare all the info MSFT provided to the auditors with our own internal self-assessment. It's the go to process of how MSFT meets regulatory and compliance requirements, and sets a real-life example of how Azure customers can follow. The MS compliance manager allows customers to track their own compliance progress and produce reports for auditor to prove compliance to standards. Real-time, on-demand assessments can be run to check our Azure environment against a compliance standard. A compliance score is also available.

Use the STP as the starting point for evaluating and scoping required cloud compliance activities. These are where whitepapers, FAQs, and guides are located.

Azure Government Services is a completely physically separate instance of Azure. It's a government-only cloud with a few regions that are physically separated from the "consumer" Azure cloud. It has "Secret" locations to host sensitive government info. Azure government has 2 services – **Azure government and Azure secret.** Both have higher level of security and supports hybrid cloud.

Germany is the only country with its own isolated instance of Azure Cloud because Germany is the only country whose laws state that info about its citizens must be owned by German companies only. This cloud is being phased out and a local Germany trustee is being brought in to be the custodian of German data. So no longer accepting new customers in Azure Germany.

4: Azure Pricing and Support

Azure Subscriptions An Azure account is a unique global entity that gives access to 1/+ subscriptions. A subscription is an object that holds 1/+ resource groups and that provides boundaries for billing, organization, and management. Subscriptions come with *offers* and will only have 1 offer type that defines the type of that subscription - enterprise agreement, certified solution partner, pay-as-you-go, etc.

Regardless of the offer type, a subscription always come with hard limits on number of resources permitted. If it's a very large organization, multiple subscriptions may be needed. Each subscription can then be grouped together in a management group. A management group is a high level object that holds all the enterprise's subscriptions together to give a total view of Azure spending across multiple subscriptions.

Azure Reservations is a way to pre-pay for services by committing to 1-3 year terms for up to 72% discount from pay-as-you-go pricing. You commit to a minimum number of resources but can scale to more as needed. A medium-large org may also choose to have an ***Enterprise Agreement*** with Microsoft which provides enterprise level features like the EA portal designed to manage all subscriptions under that EA. An EA **is mandatory to access premium features like Azure AD premium.**

An enterprise agreement starts with an Enterprise enrollment account which is the master account for all of the enterprise's *other* Azure accounts. Departments ca be created within the EA portal. In each department, Azure accounts can be assigned. Within each Azure account, individual subscriptions can be created. From there resources groups and so on.

EA > Departments > Accounts > Subscriptions > Resource Groups.

A **Resource Group** is a container of related Azure services that we can group together. A resource can only exist within the same resource group. A resource group can have resources from diff. regions. It's only an administrative boundary. You can create a resource group for a specific application or workload for instance. Permissions can be assigned to a resource group to enforce what actions that group is allowed to perform in the Azure cloud. But at a high-level, it's a *business-grouping of Azure resources.*

Planning and Managing Azure Costs. There are 2 ways to buy Azure services – directly using the Azure portal, or through a MS partner (Cloud Solution Provider). You can use the Azure pricing calculator to calculate pay-as-you-go pricing for services. If committing to a service the overall price would be lower the longer the commitment term (1-3 years).

The **Azure Free Account** gives free access to free services and others in a 30-day trial. 3 caveats – (1) there are 25 products in Azure that are "always free", (2) you get a $200 credit to use on any Azure service within 30 days, and (3) you get 12 month of free services for Azure products on top of the $200 credit which incl. 750 hours of VMs/month, 5 GB Blob storage, 250 GB SQL DB, 5 GB Cosmos DB – as long as you stay within these limits you don't get charged for 12 months.

Within 30 days of creation, all free Azure accounts need to upgrade to pay-as-you-go or they'll be disabled. You still keep the credits and the free quotas after upgrading.

There 2 categories of product pricing in Azure – (1) things that are always free, and (2) things that cost. **Things that are always free** incl. mgmt. tools, VM NICs, Azure AD Groups, NSGs, Inbound data transfer to Azure. **Things that cost money** are all the other products and services like VMs, AAD users, Public IPs, etc.

Billing Zones is only used for bandwidth pricing for data transfers in/out of Azur. 5 zones in total –

- **Zone 1** - Canada, EU, UK, US, USGOV, USDOD
- **Zone 2 -** Asia, AUS, India, Japan, Korea
- **Zone 3 -** Brazil
- **DE Zone -** Germany
- **China**

Each zone has a different bandwidth pricing rate.

The **Pricing calculator** can be used to estimate Azure costs for each individual product/service in a solution. It automatically adds related pre-requisite products as part of the solution as well.

The **TCO Calculator** helps highlight the cost diff. btw running workloads in Azure vs. on-prem. You first define workloads like DBs, servers, etc. then adjust assumptions for 5 categories (Compute, DC, networking, storage, and labor). From there TCP calc will give an Azure breakdown summary for on-demand vs. 1 year reserved vs 3 year reserved vs on-prem.

Azure Cost Management is a service that gives dashboard view of all mgmt. groups, subscriptions, to allow visibility into where costs are going. Allows to create/manage budgets and enable automation to prevent cost overruns like auto-disabling resources. Recommendations are also given on how to optimize and improve efficiency by identifying idle/under-utilized resources. It's based on the Cloudyn service which is integrated into Azure portal. A separate Cloudyn enterprise portal can be purchased separately for usage with other cloud vendors.

Azure Support Options. There are 5 levels of support plans – Basic, Developer, Standard, Professional Direct, and Premier. **Free** is included in all Azure subscriptions. Higher plans add more features and customer service. Microsoft consulting services are available in the highest level support plans. https://azure.microsoft.com/en-us/support/plans/ . support is available throughout the entire software development lifecycle - Plan, build, test, publish, connect, evaluate. Several support options incl. Azure knowledge center, Azure forums, and support plans. **The Azure Knowledge center is a knowledgebase for Azure in one spot** in a question/answer format.

Azure SLAs.
*Monthly uptime % = (Maximum available minutes - Downtime in minutes) / Maximum available minutes * 100.*

In Azure, the only thing that's guaranteed is the uptime/availability of each Azure service. **Performance is not guaranteed.** Uptime is displayed as a percentage of uptime in a month. Every Azure product/service has an SLA. Some IaaS/PaaS products can be configured in a way that enhances SLA – i.e.: deploying a DB instance in a multi-region replication architecture. **Free/shared tiers may not have guaranteed SLAs for certain products.** If Azure is unable to maintain the SLA, credit is given in the bill for the month.

The Azure Service Lifecycle. Azure features follow 2 phases – preview and General Availability (GA). **Preview features have 2 types – public and private preview features**. Public preview is when the feature is available to test-drive by all customers, private preview is only available for very large Azure customers who work directly w/ Azure engineering teams, and limited preview is for customers who have access to the preview program.

General Availability (GA) is achieved when a service is thoroughly tested and is OK for launch to the public. GA products vary by region.