Microsoft Azure core concepts

* + Azure Accounts
  + Azure free account includes:
    - Access to popular azure products for 12 months
    - Credit for first 30 days
    - Access to more than 25 products
  + Azure student account has 100$ free credit

* + Why cloud services?

* + Serverless computing lets you run code without maintaining a server, with triggers for specific actions, which is ideal for automated tasks

* + Cloud services characteristics
    - **High availability:** Keep services up for a long time, with very little downtime
    - **Scalability**: Increase/decrease resources for any workload by scaling out (adding more resources) or scaling up (additional capabilities to current resources). Not always done automatically!
    - **Elasticity**: automatically or dynamically increase or decrease resources as needed and is location conscious. A distinction between scalability and elasticity is that elasticity is done automatically.
    - **Agility**. The ability to react quickly. Cloud services can allocate and deallocate resources quickly, without manual intervention
    - **Fault tolerance:** The ability to remain up and running even in the event of a component (or service) no longer functioning thanks to redundancy
    - **Disaster recovery:** The ability to recover from an event which has taken down a cloud service.
    - **Global reach**: The ability to reach audiences around the globe. Cloud services can have a presence in various regions across the globe, giving you a presence in those regions even though you may not have any infrastructure in that region.
    - **Customer latency capabilities**. Cloud services have the ability to deploy resources in datacenters around the globe, which addresses any customer latency issues.
    - **Predictive cost considerations.** The ability for users to predict the costs they will incur for a particular cloud service. Costs for individual services are made available, and tools are provided to allow you to predict the costs a service will incur. You can also perform analysis based on planned growth.
    - Technical skill requirements and considerations. Cloud services can provide and manage hardware and software for workloads.
    - **Increased productivity**. Cloud computing eliminates the need for many of the hardware related tasks and maintenance, so IT can focus on business tasks
    - **Security**. Cloud providers offer a broad set of policies, technologies, controls, and expert technology skills. The result is strengthened security, which helps to protect data, apps, and infrastructure from potential threats.

* + Investment approaches
    - Capital expenditure (Capex):
      * Up front spending of money on physical infrastructure, and then deducting that up front expense over time. The upfront cost from CapEx has a value that reduces over time. e.g. server, network, backup, disaster and continuity tools, tech personnel costs
      * **Advantages**: You plan your expenses at the start of a project or budget period. Your costs are fixed, you know exactly how much is being spent. This is appealing when you need to predict the expenses before a project starts due to a limited budget.
    - Operational expenditure (opex):
      * Spending money on services or products now and being billed for them now. You can deduct this expense in the same year you spend it. There is no upfront cost as you pay for a service or product as you use it. e.g. leasing software, scaling charges based on usage, Billing at the user or organization level - PAYG model
      * **Advantages**: Companies wanting to try a new product or service don't need to invest in equipment. Instead, they pay as much or as little for the infrastructure as required. OpEx is particularly appealing if the demand fluctuates or is unknown - cloud services are agile!

* + Types of cloud models

* + Public cloud
  + Most common deployment model
  + No local hardware to manage or keep up-to-date – everything runs on your cloud provider's hardware.
  + You can save additional costs by sharing computing resources with other cloud users.
  + **OpEx model**
  + **SUMMARY: cheaper and easier, but less flexible and customisable**

* + **ADVANTAGES**
    - No CapEx: You don’t have to buy a new server in order to scale.
    - Agility: Applications can be made accessible or deprovisioned quickly and when needed
    - Consumption-based model: Organizations pay only for what they use, and operate under an OpEx model.
    - Maintenance: No responsibility for hardware maintenance or updates --> increased productivity
    - Skills: No deep technical skills are required to deploy, use, and gain the benefits of a public cloud. Organizations can leverage the skills and expertise of the cloud provider to ensure workloads are secure, safe, and highly available.

* + **DISADVANTAGES**
    - Security: Some security requirements cannot be met using public cloud.
    - Compliance: Government policies, industry standards, or legal requirements which public clouds cannot meet.
    - Ownership: Organizations don't own the hardware or services and cannot manage them as they may wish.

* + Private cloud
  + Cloud environment in your own datacenter
  + Good for high security/risk environments, because there is better privacy
  + **Capex model**
  + **SUMMARY: More flexible, secure, customisable, but more upfront costs and maintenance**

* + **ADVANTAGES**
    - Control: Organizations have complete control over the resources.
    - Security: Organizations have complete control over security.
    - Compliance: If organizations have very strict security, compliance, or legal requirements, a private cloud may be the only viable option.
    - Specific scenarios: If an organization has a specific scenario not easily supported by a public cloud provider (such as having to maintain a legacy application), it may be preferable to run the application locally.

* + **DISADVANTAGES**
    - Upfront CapEx: Hardware must be purchased for start-up and maintenance.
    - Agility: Private clouds are not as agile as public clouds, because you need to purchase and set up all the underlying infrastructure before they can be leveraged.
    - Maintenance: Organizations have the responsibility for hardware maintenance and updates.
    - Skills: Private clouds require in-house IT skills and expertise that may be hard to get or be costly.

* + Hybrid cloud
  + Combines public and private clouds, allowing you to run your applications in the most appropriate location.
  + **The most flexible scenario**
  + **Capex upfront**
  + **SUMMARY: More flexible, secure, customisable, but more upfront costs and maintenance**

* + **ADVANTAGES**

Flexibility: An organization can decide to run their applications either in a private cloud or in a public cloud.

Costs: Organizations can take advantage of economies of scale from public cloud providers for services and resources as they wish. This allows them to access cheaper storage than they can provide themselves.

Control: Organizations can still access resources over which they have total control.

Security: Organizations can still access resources for which they are responsible for security.

Compliance: Organizations maintain the ability to comply with strict security, compliance, or legal requirements as needed.

Specific scenarios: Organizations maintain the ability to support specific scenarios not easily supported by a public cloud provider, such as running legacy applications.

* + **DISADVANTAGES**
    - Upfront CapEx for private cloud.
    - Costs: Purchasing and maintaining a private cloud to use alongside the public cloud can be more expensive than selecting a single deployment model.
    - Skills: Deep technical skills to set up a private cloud.
    - Ease of management: Need clear guidelines to avoid confusion, complications or misuse.

* + Types of cloud services

**Shared responsibility model** ensures cloud workloads are run securely and in a well-managed way. Depending on the service you are using, the cloud provider is responsible for some aspects of the workload management, and the customer or end user is responsible for other aspects of the workload management, and in some cases, both share a responsibility.

On-premises 
(Private Cloud) 
u Mana e 
Infrastructure 
(as a Service) 
Compute 
Networking 
Storage 
Cloud Provider 
Manages 
Platform 
(as a Service) 
Runtime 
Operating System 
Virtual Machine 
Compute 
Networking 
Storage 
Software 
(as a Service) 
Applications 
Runtime 
Operating System 
Virtual Machine 
Compute 
Networking 
Storage 

You can use any combination of IAAS, PAAS, or SAAS!

* + IaaS

* + **Complete control over hardware --> most flexible category of cloud service. Opex model and easier to manage.**

* + **User ownership:** The user is responsible for the purchase, installation, configuration, and management of their own software.
  + **Cloud provider ownership:** The cloud provider is responsible for ensuring that the underlying cloud infrastructure (such as virtual machines, storage and networking) is available for the user.

* + Usage scenarios:
    - Migrating workloads: IaaS facilities managed in a similar way as on-prem and provide an easy migration path for moving existing applications to the cloud.
    - Test and development. IaaS makes scaling development testing environments up and down fast and economical.
    - Website hosting. Running websites using IaaS can be less expensive than traditional web hosting.
    - Storage, backup, and recovery. IaaS is useful for managing unpredictable demand and steadily growing storage needs. It can also simplify the planning and management of backup and recovery systems.

* + **ADVANTAGES:**
    - **No CapEx:** no upfront costs.
    - **Agility:** Applications can be made accessible quickly, and deprovisioned whenever needed.
    - **Consumption-based model:**  Organizations pay only for what they use and operate under an OpEx model.
    - **Skills:** No internal deep technical skills are required to deploy, use, and gain the benefits of a public cloud.
    - **Cloud benefits:** Organizations can leverage the skills and expertise of the cloud provider to ensure workloads are made secure and highly available.
    - **Flexibility:** IaaS is the most flexible cloud service as you have control to configure and manage the hardware running your application.

* + **DISADVANTAGES**:
    - Management: Shared responsibility model: the user manages and maintains the services they have provisioned, and the cloud provider manages and maintains the cloud infrastructure.

* + PaaS

An environment for building, testing, and deploying software applications. Create an application as quickly as possible without having to worry about managing the underlying infrastructure. Same considerations as IaaC, but with more benefits

* + **User ownership:** The user is responsible for the development of their own applications. But **NOT** responsible for managing the server or infrastructure.
  + **Cloud provider ownership:** Responsible for OS management, and network and service configuration. Responsible for everything apart from the application that a user wants to run.

* + Usage scenarios:
  + **Development framework:**
    - PaaS provides a framework that developers can build upon to develop or customize cloud-based applications.
    - Lets developers create applications using built-in software components. Cloud features such as scalability, high-availability, and multi-tenant capability are included, reducing the amount of coding that developers must do.
  + **Analytics or business intelligence:**
    - Tools provided as a service with PaaS allow organizations to analyse and mine their data.
    - They can find insights and patterns, and predict outcomes to improve business decisions such as forecasting, product design, and investment returns.

* + **ADVANTAGES:**
    - **No CapEx:** no upfront costs.
    - **Agility:**  **PaaS is more agile than IaaS,** and users do not need to configure servers for running applications.
    - **Consumption-based model:**  Organizations pay only for what they use and operate under an OpEx model.
    - **Skills:** No internal deep technical skills are required to deploy, use, and gain the benefits of a public cloud.
    - **Cloud benefits:** Organizations can leverage the skills and expertise of the cloud provider to ensure workloads are made secure and highly available.
      * **In addition, users can gain access to more cutting-edge development tools and toolsets. They then can apply these tools and toolsets across an application's lifecycle.**
    - **Productivity:**
      * Users can focus on application development only, as all platform management is handled by the cloud provider.
      * Working with distributed teams is easier, as the platform is accessed over the internet and can be made globally available more easily.

* + **DISADVANTAGES**:
    - **Platform limitations**. Limitations that could affect how an application runs. Any limitations should be taken into consideration when considering which PaaS platform is best suited for a workload.

* + SaaS

Software that is centrally hosted and managed for the end customer. Allows users to connect to and use cloud-based apps over the internet. Examples: email, calendars, and office tools such as Microsoft 365. SaaS provides the same benefits as IaaS, but again there some **additional benefits.**

* + **User ownership:** Users just use the application software; they are not responsible for any maintenance or management of that software.
  + **Cloud provider ownership:** Responsible for the provision, management, and maintenance of the application software.

* + Usage scenarios: Examples of Microsoft SaaS: Microsoft 365, Skype, and Microsoft Dynamics CRM Online.

* + **ADVANTAGES:**
    - **No CapEx:** no upfront costs.
    - **Agility:** Users can provide staff with access to the latest software quickly and easily.
    - **Pay-as-you-go pricing model:** Subscription model
    - **Flexibility:** Users can access the same application data from anywhere.

* + **DISADVANTAGES**:
    - **Software limitations:** Since you are using as-is software you don't have direct control of features --> limitations.
      * Business needs and software limitations should be taken into consideration when considering which SaaS platform is best suited for a workload.

* + Azure subscriptions, management groups, and resources

Management 
groups 
Subscriptions 
Resource 
groups 
Resources 

* + **Resources**: Instances of services you create, like VMs or blob storage
  + **Resource groups:** Resources combined into resource groups, which act as logical containers to deploy and manage resources in.
    - Logical grouping: resources of a similar usage, type or location to provide organisation.
    - Life cycle: If you delete a resource group, all resources within it are also deleted --> easy!
    - Authorization: Good for scoping RBAC permissions
  + **Subscription**: Groups together user accounts and resources that have been created by those accounts, for each sub, there are limits on the amount of resources you can use. Subscriptions manage costs and resources!
    - Two types of subscription boundaries:
      * Billing boundary: Determines how an azure account is billed for using Azure - lets you manage and organise costs
      * Access control boundary: Access management policies to reflect org structure for different departments
    - You can also create different subs to separate environments (e.g. dev, testing) org structures (e.g. limit HR to lower cost, but IT at full range) or billing (to manage costs)
    - You can organise subs into invoice sections to separate billing for each sub.
  + **Management group:** Manage access policy for multiple subs. All subs inherit the conditions applied to the management group.
    - You can organise management groups and subs to create a hierarchy for resources. This hierarchy can be used to apply policies, e.g. limit VM locations to US west region in a management group called Production.

* + **Azure resource manager**: Management interface for creating, updating, or deleting resources in Azure.
    - You can manage inf through templates rather than scripts
    - Deploy manage and monitor all the resources for your solution as a group
    - Apply RBAC
    - Apply tags to logically organise and view resources

* + Azure architectural components

* + Resources are created in regions, which are different geographical locations around the globe that contain Azure datacenters.

* + Geographies

A discrete market typically containing two or more regions that preserves data residency and compliance boundaries.

Ensure that data residency, sovereignty, compliance, and resiliency requirements are honoured within geographical boundaries.

Connected to dedicated high-capacity networking infrastructure --> fault-tolerant to withstand complete region failure

Geographies are broken up into the following areas:

* + Americas
  + Europe
  + Asia Pacific
  + Middle East and Africa

* + Region:

A geographical area on the planet containing at least one datacenters that are in close proximity and networked together with a low-latency network

Each region belongs to a single geography and has specific service availability, compliance, and data residency/sovereignty rules applied to it.

Azure has more global regions than any other cloud provider.

Regions provide customers the flexibility and scale needed to bring applications closer to their users.

Regions preserve data residency and offer comprehensive compliance and resiliency options for customers.

For most Azure services, when you deploy a resource in Azure, you choose the region where you want your resource to be deployed.

Each Azure region is paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away, which together make a region pair --> fault tolerance

* + Physical isolation: When possible, Azure prefers at least 300 miles of separation between datacenters in a regional pair, although this isn't practical or possible in all geographies reducing the likelihood of natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once.
  + Platform-provided replication: Some services such as Geo-Redundant Storage provide automatic replication to the paired region.
  + Region recovery order: In the event of a broad outage, recovery of one region is prioritized out of every pair. Applications that are deployed across paired regions are guaranteed to have one of the regions recovered with priority.
  + Sequential updates: Planned Azure system updates are rolled out to paired regions sequentially (not at the same time) to minimize downtime, the effect of bugs, and logical failures in the rare event of a bad update.
  + Each region belongs to a single geography and has specific service availability, compliance, and data residency/sovereignty rules applied to it.

* + Special azure regions for compliance/legal purposes
    - US DoD Central, US Gov Virginia, US Gov Iowa and more: Physical and logical network-isolated instances of Azure for US government agencies and partners. Operated by screened US persons and include additional compliance certifications.
    - China East, China North and more: Unique partnership between Microsoft and 21Vianet, Microsoft does not directly maintain the datacenters.

* + Availability:

* + A single virtual machine with premium storage has an SLA of 99.9%.
  + You can quickly migrate existing virtual machines to Azure through “lift and shift”.
    - Lift and shift is a no-code option where each application is migrated as-is, providing the benefits of the cloud without the risks or costs of making code changes.

* + **Availability sets:**

VM SLA 
99.95% 
AVAILABILITY SETS 
Protecting against failures 
within datacenters 

A logical grouping capability for isolating VM resources from each other when they're deployed. VMs you place within an Availability Set, run across multiple physical servers, compute racks, storage units, and network switches.

They are made up of:

* + Update domains. When a maintenance event occurs (such as a performance update or critical security patch applied to the host), the update is sequenced through update domains. Update domains are a logical section of the datacenter, and they are implemented with software and logic.
  + Fault domains. Fault domains provide for the physical separation of your workload across different hardware in the datacenter. This includes power, cooling, and network hardware thus in the event of an outage only that rack of servers would be affected by the outage.

* + **Availability zones:** Physically separate locations within an Azure region that use availability sets to provide additional fault tolerance within a region.

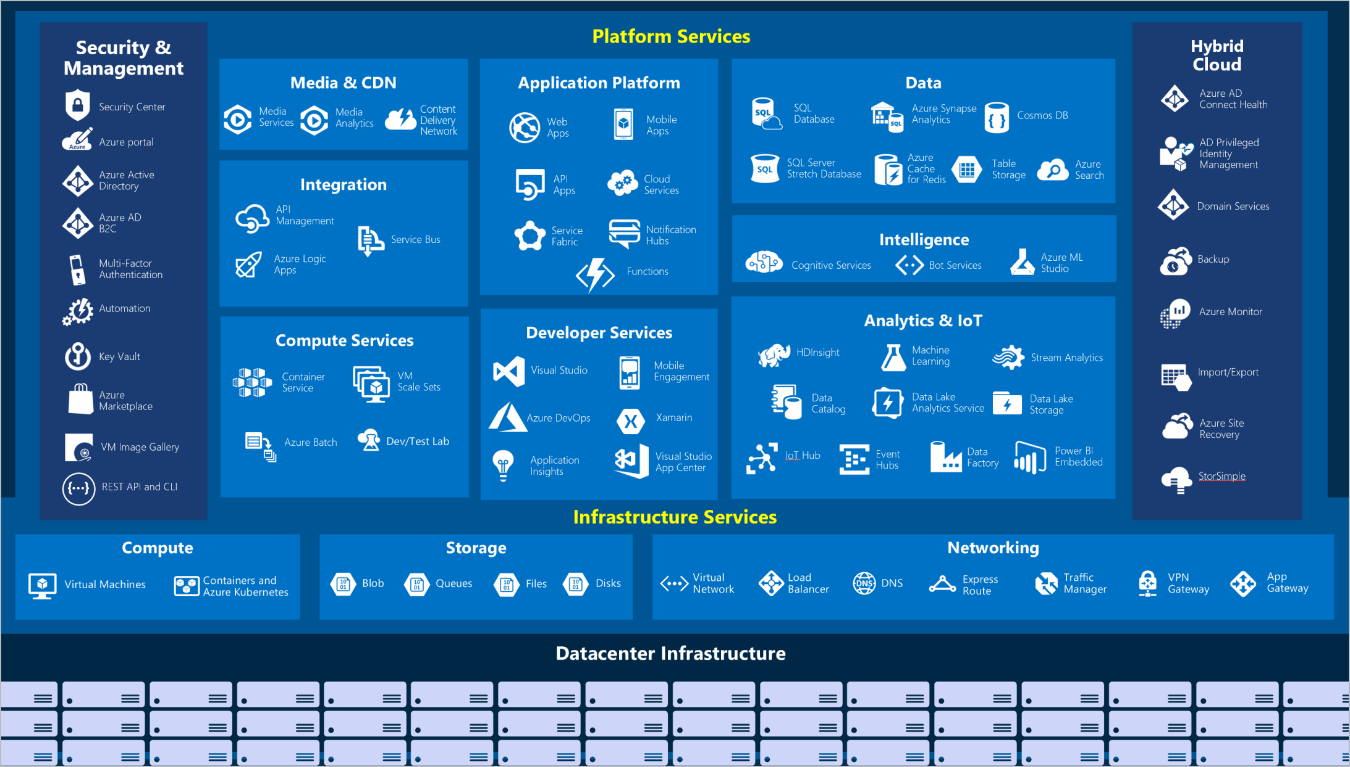
VM SLA 
99.99% 
AVAILABILITY ZONES 
Protection from entire 
datacenter failures 

* + Each availability zone is an isolation boundary containing one or more datacenters equipped with independent power, cooling, and networking.
  + Min. 3 zones within a region
  + If one availability zone goes down, the other continues working.
  + The availability zones are typically connected to each other through very fast, private fiber-optic networks.
  + Availability zones allow customers to run mission-critical applications with high availability and low-latency replication.
  + Availability zones are offered as a service within Azure, and to ensure resiliency, there’s a minimum of three separate zones in all enabled regions.

* + Availability Zones are primarily for VMs, managed disks, load balancers, and SQL databases. Azure services that support Availability Zones fall into two categories:
    - **Zonal services** – you pin the resource to a specific zone (for example, virtual machines, managed disks, IP addresses)
    - **Zone-redundant services** – platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).
    - **Non regional service:** Services always available from azure geographies and are resilient to zone-wide outages and region-wide outages

* + **Azure region pair**

* + Min 3 zones within a region, but a disaster could wipe out all 3. Azure therefore creates region pairs.
  + Each azure region is paired with another region within the same geo, e.g. US or Asia at least 300 miles away, e.g. West US and East US
  + This helps replication of resources across a Geo that can help reduce likelihood of interruptions - pair of regions are directly connected and far enough apart to be isolated from regional disasters.
  + If a region in a pair was affected by natural disaster, services would failover to the other region in the region pair.



* + QUESTIONS

* + Which of the following terms describe a benefit of cloud services?
  + **Economies of scale**
  1. Fixed workloads
  2. Unpredictable costs

* 1. Which of the following terms refer to spending money upfront and then deducting that expense over time?
  2. **Capital expenditure**
  3. Operational expenditures
  4. Supply and demand

* 1. Which of the following terms refer to making a service available with no downtime for an extended period of time?
  2. Agility
  3. Fault tolerance
  4. **High availability**

* 1. Which term from the list below would be viewed as benefits of using cloud services?
  2. Unpredictable costs
  3. Local reach only
  4. **Elasticity**

* 1. From the choices below, what is one of the advantages of moving your infrastructure to Azure?
  2. **The move reduces Capital Expenditures. (CapEx)**
  3. The move reduces Operational Expenses (OpEx).
  4. The move allows for complete control of infrastructure resources.

* 1. Which cloud model provides the greatest degree of ownership and control?
  2. Hybrid
  3. **Private**
  4. Public

* 1. Which cloud model provides the greatest degree of flexibility?
  2. Public
  3. Private
  4. **Hybrid**

* 1. Which of the following describes a public cloud?
  2. Is owned and operated by the organization that uses the resources from that cloud.
  3. Lets organizations run applications in the cloud or on-premises.
  4. **Provides resources and services to multiple organizations and users, who connect through a secure network connection.**

* 1. Microsoft Skype is an example of which cloud service type?
  2. Infrastructure as a Service
  3. Platform as a Service
  4. **Software as a Service**

* 1. Which of the following describes Platform as a Service (PaaS)?
  2. Users are responsible for purchasing, installing, configuring, and managing their own software (operating systems, middleware, and applications).
  3. **Users create and deploy applications quickly without having to worry about managing the underlying infrastructure.**
  4. Users pay an annual or monthly subscription.

* 1. Which of the following requires the most user management of the cloud services?
  2. **Infrastructure as a Service**
  3. Platform as a Service
  4. Software as a Service

* 1. You are running a virtual machine in a public cloud using IaaS. Which model correctly reflects how that resource is managed?
  2. **Shared responsibility model**
  3. Cloud user management model
  4. User management model

* 1. You're developing an application and want to focus on building, testing, and deploying. You don't want to worry about managing the underlying hardware or software. Which cloud service type is best for you?
  2. Infrastructure as a Service (IaaS)
  3. Software as a Service (SaaS)
  4. **Platform as a Service (PaaS)**