#1 CLOUD CONCEPTS

#1.1 Benefits & Considerations of Cloud Services

Benefits of Cloud Computing

High Availability
- Depending on SLA.
- no apparent downtime.
	Scalability
	- app can scale vertically and horizontally.
	  ○ Vertical: Adding compute capacity – RAM or Memory
	  ○ Horizontal: Adding instances

Elasticity - Autoscaling	**Agility** - Deploy and configure cloud-based resources quickly as your app requirements change.
Disaster Recovery - cloud-based backup services, data replication, and geo-distribution. - Fault tolerance.	**Geo-distribution** - Deploy to regional datacentres around the globe.

Capital Expenditure (CapEx) & Operational Expenditure (OpEx)

CapEx	OpEx
- up-front spending of money on physical infrastructure	- spending money on services or products now and being billed for them now.

Consumption-based model (Operational Expenditure Model)

- only pay for the resources that they use, no up-front costs. No need to purchase/manage costly infrastructure that are not use fullest.
- Eg: Serverless computing.

#1.2 Categories of Cloud Services

Shared Responsibility Model

Cloud Services

Infrastructure-as-a-Service (IaaS)	Platform-as-a-Service (PaaS)	Software-as-a-Service (SaaS)

Serverless Computing

#1.3 Types of Cloud Computing

Cloud Computing

- delivery of computing services over the internet by using a pay-as-you-go pricing model.

Cloud services:

1) Servers
2) Storage
3) Database
4) Networking
5) Software
6) Analytics
7) Intelligence

Types of Cloud Models

Public Cloud	Private Cloud	Hybrid Cloud
- Resources owned and operated by a third-party cloud service provider. - delivered over the internet.	- Can be physically located at your organization's on-site (on-premises) data centre, or it can be hosted by a third-party service provider.	- Public + Private

#2 AZURE SERVICES

#2.1 Architectural components

Regions & Region Pairs
- a geographical area on the planet that contains at least one but potentially multiple datacentres that are nearby and networked together with a low-latency network.
- Region Pairs: Each Azure region is always paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away.

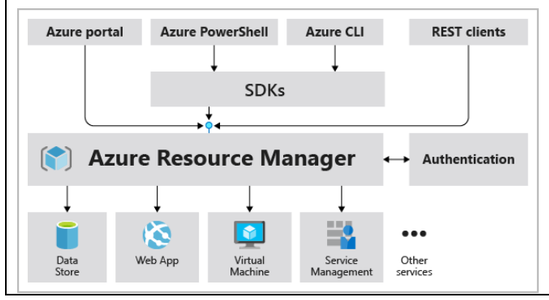
Availability Zones
- physically separate datacentres within an Azure region.
- made up of one or more datacentres equipped with independent power, cooling, and networking.

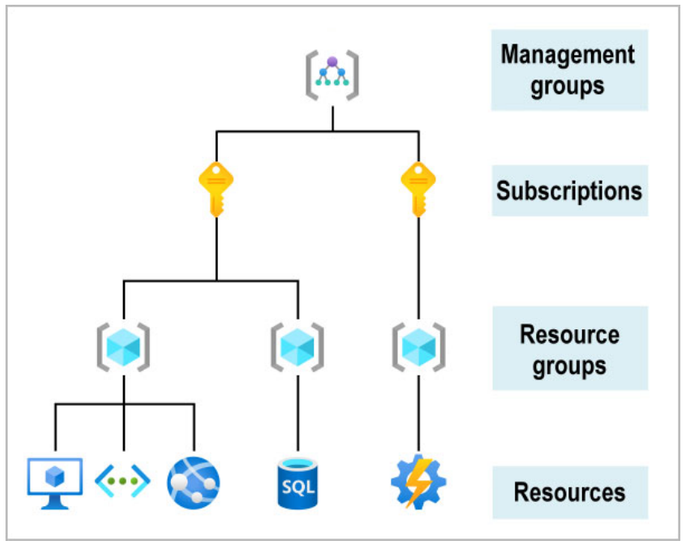
Resource Groups
- a logical container which Azure resources are deployed and managed.
- can view the total cost of all the resources.

Subscriptions
- groups together user accounts and the resources.
- limits or quotas on the amount of resources that you can create and use.
- Can be used to manage costs and the resources that are created by users, teams, or projects.
    - Can be managed by Azure AD account, not only Microsoft account.
- An Azure AD tenant can have multiple subscriptions, but an Azure subscription can only be associated with one Azure AD tenant.
- Cannot merge, but can move resources to another subscription, transfer ownership.

Management Groups
- manage access, policy, and compliance for multiple subscriptions.
- All subscriptions in a management group automatically inherit the conditions applied to the management group.

Azure Resource Manager





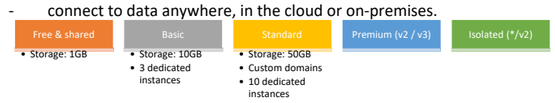
#2.2 Resources available

Compute Resources

Virtual Machines
- software emulations of physical computers.
- include a virtual processor, memory, storage, and networking resources.

VM Scale sets
- an Azure compute resource that you can use to deploy and manage a set of identical VMs

Azure App Services
- build, deploy and scale web apps.
- platform-as-a-service (PaaS)
- connect to data anywhere, in the cloud or on-premises.



Azure Container Instances (ACI)
- lightweight, virtualized application environments.
- provide portable environments for virtualized applications.
- Do not have to manage any virtual machines/adopt a higher-level service.

Azure Kubernetes Services (AKS)
- quickly created, scaled out, and stopped dynamically.

Windows Virtual Desktop
- a desktop and application virtualization service that runs on the cloud.
- a cloud-hosted version of Windows from any location.
- works across devices like Windows, Mac, iOS, Android, and Linux.

Networking Resources

Virtual Networks
- enable Azure resources to communicate with each other, with users on the internet, and with your on-premises client computers.

VPN Gateway
- a type of virtual network gateway.

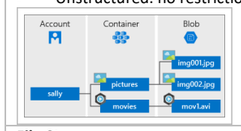
CloudExchange colocation	Point-to-Site (P2S)	Any-to-any
	create a secure connection to your virtual network from an individual client computer.	integrate your wide area network (WAN) with Azure

Virtual Network Peering – Gateway subnet
- The virtual network gateway needs to be located in a dedicated subnet in the Azure virtual network. This dedicated subnet is known as a gateway subnet.

ExpressRoute
- let you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider.
- all inbound data transfer is free of charge.

Storage Resources

Container (Blob) Storage
- an object storage solution for the cloud.
- can store massive amounts of data, such as text or binary data.
- Unstructured. no restrictions on the kinds of data it can hold.



Disk Storage
- provides disks for Azure virtual machines.
- allows data to be persistently stored and accessed from an attached virtual hard disk.

File Storage
- fully managed file shares in the cloud that are accessible via the industry standard Server Message Block and Network File System (preview) protocols.

Storage Tiers

Hot	Cold	Archived
Storing data that is accessed frequently	Data that is infrequently accessed and stored for at least 30 days	Data that is rarely accessed and stored for at least 180 days

Databases Resources

Cosmo DB
- a globally distributed, multi-model database service.

Azure SQL DB
- a relational database service.
- a managed SQL Server Database in Azure.
- to build data-driven applications and websites

Azure DB for MySQL
- a relational database service in the cloud, and it's based on the MySQL Community Edition database engine, versions 5.6, 5.7, and 8.0.

Azure DB for PostgreSQL
- a relational database service

SQL Managed Instance
- a scalable cloud data service that provides the broadest SQL Server database engine compatibility with all the benefits of a fully managed platform as a service.

Azure Marketplace
- provides access and information on solutions and services available from Microsoft and their partners.
- can browse available virtual machine images.

#3 SOLUTIONS & MANAGEMENT TOOLS

#3.1 Solutions

Internet of Things

IoT Hub	IoT Central	Azure Sphere

- bi-directional communication between your IoT application and the devices it manages.
- Processes data from millions of sensors.
- can connect virtually any device to IoT Hub.
- can route messages to:
  ○ Azure Blob Storage
  ○ Azure Data Lake Storage
	- builds on top of IoT Hub.
	- adding a dashboard that allows you to connect, monitor, and manage your IoT devices.
		- creates an end-to-end, highly secure IoT solution for customers that encompasses everything from the hardware and operating system on the device to the secure method of sending messages from the device to the message hub.

Analytics

Azure SQL Synapse Analytics	HDInsight	Azure Databrick
- Cloud-based enterprise data warehouse (EDW), Platform-as-a-Service (PaaS). - a large-scale, distributed, MPP (massively parallel processing) relational database technology.	- a fully managed, full-spectrum, open-source analytics service in the cloud for enterprises.	- A big data analytics service for machine learning. - an Apache Spark-based analytics platform. - Consists of several components, eg: MLib for ML.

Artificial Intelligence

Azure Machine Learning	Cognitive Services	Azure Bot Service
- uses past trainings to provide predictions that have high probability. - visually connect datasets and modules on an interactive canvas to create machine learning models.	- APIs, SDKs, and services available to help developers build intelligent applications without having direct AI or data science skills or knowledge. - Services: Vision, Speech, Language, Web Search, and Decision.	- provides a digital online assistant that provides speech support.

Serverless computing

Azure Functions	Azure Logic Apps
- Platform for serverless code. - run event-triggered code without having to explicitly provision or manage infrastructure.	- a cloud service that helps you schedule, automate, and orchestrate tasks, business processes, and workflows when you need to integrate apps, data, systems, and services across enterprises or organizations.

Version Control

Azure DevOps - Enterprise Development - Microsoft's primary software development and deployment platform. - influences the application lifecycle throughout its plan, develop, deliver and operate phases.	**GitHub** - Open-source code, individual developers.
GitHub Actions	**Azure DevTest Labs** - creates labs consisting of pre-configured bases or Azure Resource Manager templates. - Quickly provision Windows and Linux environments by using reusable templates and artifacts.

#3.2 Management Tools

Main Management Tools

Azure Portal - a web-based, unified console that provides an alternative to command-line tools. - manage your Azure subscription using a graphical user interface. - Create custom dashboards for an organized view of resources. Azure virtual machines page - Maintenance Status - display service issues.	**Azure PowerShell** - PS script: a file that contains PowerShell cmdlets and code. - can be installed on Linux. Automatically has in Windows? As long as it is installed on a PC, then it can be used to run PS script. - can be installed on MacOS but it cannot be installed on an iPhone.
Azure CLI - For Windows, the Azure CLI is installed via an MSI, which gives you access to the CLI through the Windows Command Prompt (CMD) or PowerShell. - can be installed on MacOS but it cannot be installed on an iPhone.	**Cloud Shell** - a browser-based shell experience to manage and develop Azure resources. - can be run on a browser from a tablet that runs the Android operating system. - provides the flexibility of choosing the shell experience that best suits the way you work, either Bash or PowerShell.
Azure Mobile App	

Azure Advisor – Security Recommendations on RESOURCES

- displays security recommendations & optimize and reduce your overall Azure spend by identifying idle and underutilized resources.
- a personalized cloud consultant that helps you follow best practices to optimize your Azure deployments.
- analyses your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.
- generate a list of virtual NOT protected by Azure Backup.
- Not related to Azure AD.

Azure Resource Manager (ARM) templates

- provides a common platform for deploying objects to a cloud infrastructure and for implementing consistency across the Azure environment.
- To automate the creation of the Azure resources.
- Deploying resource through templates is known as "Infrastructure as code".
- Template: a JavaScript Object Notation (JSON) file.
  - Defines the infrastructure and configuration for your project.

Azure Monitor – Metrics & Logs

- collecting, analysing, and acting on telemetry from your cloud and on-premises environments. From multiple subscriptions.
  - Metrics: tell you how the resource is performing and the resources that it is consuming.
  - Logs: record when resources are created or modified.
- Application Insights:
  - to monitor your live applications.
  - detects and diagnoses anomalies in web apps.

Can:
- send Azure AD activity logs to Azure Monitor.
- send an alert when admin stop a VM.

Azure Service Health – Service & Maintenance Issues

- has 3 components: Azure Status, Azure Service Heath and Azure Resource Health.
- provides a personalized view of the health of the Azure services and regions.
- Can set up Service Health alerts to notify via preferred communication channels when:
  - service issues.
  - planned maintenance.
  - other changes.

#4 SECURITY & NETWORK SECURITY FEATURES

#4.1 Azure Security

Azure Security Centre - Compliance
- a unified infrastructure security management system that strengthens the security posture of your data centres.
- provides advanced threat protection across your hybrid workloads in the cloud – Azure & on-premises.
- track and manage compliance and governance over time.
- Some features require payment.

Just-in-time (JIT) virtual machine (VM) access
- lock down inbound traffic to Azure VMs.

Key Vault
- a secure store for storage various types of sensitive information.
- for server application users.
- Encrypted.

Azure Sentinel – Security Events
- a scalable, cloud-native, security information event management (SIEM) and security orchestration automated response (SOAR) solution.
- collect and automatically analyse security events from Azure Active Directory.

Azure Dedicated Host
- Dedicated physical servers to host VMs.
- Follow regulatory compliance.

Azure Information Protection
- encrypt documents and emails.
- automatically add a watermark to Microsoft Word documents that contain credit card information.

#4.2 Azure Network

Defence in depth
- Protect information & prevent stolen.
- Slow the advance of attack.

Network Security Groups (NSG)
- Like Firewall: block or allow traffic based on source/destination IP address, source/destination ports and protocol.
- contains security rules that allow or deny inbound network traffic to, or outbound network traffic from, several types of Azure resources.
- Control traffic inside a same virtual network, not a gateway between several networks
- Can associate to:
    - Subnet
    - Network interface

Azure Firewall
- to block or allow traffic based on source/destination IP address, source/destination ports and protocol.
- does not encrypt network traffic.
- uses a static public IP address for your virtual network resources allowing outside firewalls to identify traffic originating from your virtual network.
- restrict traffic to multiple virtual networks in multiple subscriptions.

Azure DDoS protection
- DDoS: attack that tries to exhaust application resources.
- Types of Service:

DDoS Protection Basic	DDoS Protection Standard
- By default - no extra cost	- logging, alerting, and telemetry. - generate reports that contain details of attempted attacks

Extra:
local network gateway - a specific object that represents your on-premises location (the site) for routing purposes.

#5 IDENTITY, GOVERNANCE, PRIVACY & COMPLIANCE FEATURES

#5.1 Identity Services

Authentication vs Authorization

Authentication	Authorization
- verifying a user's credentials. - proving your identity.	- what you are allowed to do once you have been authenticated. - What resources can be accessed?

Azure Active Directory

- a centralized identity provider in the cloud. Primary built-in authentication and authorization service to provide secure access to Azure resources.
- authenticates users and provides access tokens.

Can	Not
- create group polices. - assigns multiple licenses. - sync their passwords to further minimize the impact on users.	- require domain controllers on virtual machines.

Azure Advanced Threat Protection (ATP)
- Monitor threats using sensors.

Identity Protection
- enforce MFA based on a condition.
- sign-in risk policy and user risk policy. Anonymous IP address. Automatic encourage password changes.

Federation
- a collection of domains that have established trust.
- third-party cloud services and on-premises Active Directory can be used to access Azure resources.
- Can join Windows 10 devices to AAD.

Privileged Identity Management (PIM)
- time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions on resources.

Conditional Access	Multi-factor Authentication (MFA)	Single Sign-On (SSO)
- a tool that Azure AD uses to allow (or deny) access to resources based on identity signals. - need an Azure AD Premium P1 or P2 license.	- Not necessary to deploy a federation solution or sync on-premises identities to the cloud. - Valid methods: Password, Microsoft Authenticator App, SMS and Voice call.	- enables you to remember only one username and one password to access multiple applications. - single identity is tied to a user.

#5.2 Governance Features

Role-Based Access Control (RBAC)
- Can create custom roles to control access to resources.
- A user account can be assigned to several roles.
- Owner role can be assigned to multiple users.

Resource
- Can have multiple Delete locks.
    - Inherits locks from its resource group.
    - Must be removed before a resource can be deleted.

Tags
- To label Azure resources.
- metadata elements attached to resources.
- consist of pairs of key/value strings.
- Eg: Location – Office1

Azure Policy
- define rules for what can be deployed and how it should be deployed.
- a service in Azure that you use to create, assign, and manage policies.
- If there are any existing resources that aren't compliant with a new policy assignment, they appear under "non-compliant" resources, but they won't be deleted.

Azure Blueprints
- Each blueprint can consist of zero or more ARM template artifacts.
- can be saved to a management group or subscription.
- Grant permissions to a resource.

Cloud Adoption Framework

#5.3 Privacy & Compliance Resources

Core tenets

Security	Privacy	Compliance
		Compliance Manager in the Service Trust Portal: - a workflow-based risk assessment tool - track, assign, and verify organization's regulatory compliance activities.

Microsoft Privacy Statement	Product Terms Site	Data Protection Addendum (DPA)
- what personal data Microsoft processes? - how Microsoft processes the data. - the purpose of processing the data.		

Trust Centre
- has more than 90 compliance certifications.
- can view a list of compliance certifications, to determine whether Azure meets your regional requirements.

Azure compliance documentation
- GDPR: European policy that regulates data privacy and data protection.

Azure Sovereign Regions

Azure Government cloud services	Azure China cloud services
- hosting United States government solutions on its cloud. - operated using completely separate physical infrastructure within Azure. National Institute of Standards and Technology (NIST) - defines standards used by the US government.	- operated by 21Vianet. - a physically separated instance of cloud services located in China.

#6 COST MANAGEMENT & SERVICE LEVEL AGREEMENTS

#6.1 Planning & Managing Costs

Factors Affect Costs

Resource Types	Services
	- Storage: charged for read and write operations in general-purpose v2 storage accounts.
Locations	**Ingress & Egress Traffic**
- Storage: price of Azure storage varies by region.	- Data ingress: NO CHARGE - Data egress: EXTRA CHARGE

Extra:
- No additional cost for resource group.

Factors Reduce Costs

Reserved Instances	Reserved Capacity
- commit to pay for a resource for 1 or 3 years. - Get discounted price.	- Reserve server capacity at a specific data centre. - No charge for deallocated VMs. But got charge for storage.
Hybrid Use Benefit	**Spot Pricing**
- a licensing benefit that helps you to significantly reduce the costs of running your workloads in the cloud. - letting you use your on-premises Software Assurance-enabled Windows Server and SQL Server licenses on Azure.	

Calculator

Pricing Calculator	Total Cost of Ownership (TCO) Calculator
Free: - Network Interface - User account - Resource groups/Azure Active Directory Groups - Ingres traffic - Data traffic between Azure services within same regions Charged $$$: - public IP addresses - Egress traffic	- Estimate the cost saving of operating solutions on Azure over time. - Compare on-premises vs Azure cost.

Azure Cost Management

- Only for customers with Enterprise Agreement (EA), Microsoft Customer Agreement (MCA), or Microsoft Partner Agreement (MPA).
- Only Billing Administrator or Global Administrator can transfer ownership of Azure subscription.
- Spending limit: Can be removed, increased or decreased.

Extra:
- Free account/subscription:
  - expire after 12 months.
  - can only create one free Azure account per Microsoft account.

Azure Free Trial:
- Spending limit: 200 USD
- 5 GB blob storage limit and a 5 GB file storage limit.
- 10 web, mobile or API apps

#6.2 Service Level Agreements (SLA) & Service Lifecycles

Purpose of Azure Service Level Agreement (SLA)

- Microsoft guarantee at least 99.9% availability of the Azure Active Directory Premium.
- No SLA is provided for the Free tier of Azure Active Directory.
- can claim credit if the availability falls below the SLA, deducted from your monthly bill for that service.

Uptime:
- (Max Available Minutes – Downtime) / Max Available Minutes * 100%

Actions that impact SLA – Availability Zones

Service lifecycle in Azure

Public Preview	Private Preview	General Availability
- the service is in public beta. - can be tried out by anyone with an Azure subscription. - Often with discounted price. - the service may have faults and may be withdrawn without notice. - Exclude from SLA.	- can be viewed in the regular Azure portal. - need to be signed up for the feature in private preview before you can view it. - Usually by invitation only. - Most services go to private preview then public preview before being released to general availability.	- Cost increased when the service from Private -> Public.

Modern Lifecycle Policy
- covers products and services that are serviced and supported continuously.
- Microsoft will provide a minimum of 12 months' notification prior to ending.

Azure Support Plans
- An Azure free account comes with a basic support plan.
- any type of Azure subscription (pay-as-you-go, Enterprise Agreement, Microsoft Customer Agreement etc.) can get support from the MSDN forums.
- can open support cases on Azure Portal in the following plans: Premier, Professional Direct, Standard, and Developer only, not for Basic.