Describe cloud concepts (25—30%)

Describe cloud computing

- Define cloud computing

  Cloud computing is the delivery of computing services over the internet

- Describe the shared responsibility model

  Responsibilities get shared between the cloud provider and the consumer.

  Physical security, power, cooling, and network connectivity are the cloud provider's responsibilities.

  The consumer is responsible for the data and information stored in the cloud.

- Define cloud models, including public, private, and hybrid

  - Private Cloud: hardware only used by a single company, owns the hardware and data center

    Everything built on Cloud Provider

  - Public Cloud: built, controlled, and maintained by a third-party cloud provider. Cloud services for multiple clients.

    Everything is built on the company`s data centers

  - Hybrid Cloud: a combination of public and private cloud, users can flexibly choose which services to keep in the public cloud and which to deploy to their private cloud infrastructure.

    - Multi-cloud: you use multiple public cloud providers, in a multi-cloud environment you deal with two (or more) public cloud providers and manage resources and security in both environments.

Azure Stack Product family can be used for connected or disconnected scenarios. Easy transfer to Azure public or hybrid cloud.

Azure Arc is a set of technologies that helps manage your cloud environment

- Identify appropriate use cases for each cloud model

- Describe the consumption-based model

  there are two types of expenses to consider in the IT infrastructure model;

  Capital expenditure (CapEx)(buying a company vehicle) On-premise

  Operational expenditure (OpEx)(signing up for cloud services) Azure

  Consumption-based model, you only pay for what you use

  This consumption-based model has many benefits, including:

  - No upfront costs.
  - No need to purchase and manage a costly infrastructure that users might not use to its fullest potential.
  - The ability to pay for more resources when they're needed.
  - The ability to stop paying for resources that are no longer needed.

- Compare cloud pricing models

  a pay-as-you-go pricing model

  - Plan and manage your operating costs.

- Run your infrastructure more efficiently.
- Scale as your business needs change.

Describe the benefits of using cloud services

- Describe the benefits of high availability and scalability in the cloud

  High Availability: Azure is a highly available cloud environment with uptime guarantees depending on the service. These guarantees are part of the service-level agreements (SLAs). (99%~99.9%)

  Scalability: the ability to scale means you can add more resources to better handle the increased demand.

    Vertical scaling; CPUs or RAM (scaling up- upgrade to bigger server)

    Horizontal Scaling; a steep jump or a significant drop in demand (scaling out-add more servers of the same size)

- Describe the benefits of reliability and predictability in the cloud

  Reliability: Reliability is the ability of a system to recover from failures and continue to function. It's also one of the pillars of the Microsoft Azure Well-Architected Framework.

  Predictability; can be focused on performance predictability(auto-scaling) or cost predictability.

- Describe the benefits of security and governance in the cloud

  Governance: cloud features support governance and compliance, and set templates to help ensure that all your deployed resources meet corporate standards and government regulatory requirements.

Security: infrastructure as a service max control, platform as a service or software as a service automatically

- Describe the benefits of manageability in the cloud

  Management of the cloud: managing your cloud resources

  Management in the cloud: you're able to manage your cloud environment and resources

Describe cloud service types

- Describe infrastructure as a service (IaaS): maximum amount of control for your cloud resources

- Describe platform as a service (PaaS): a middle ground between renting space in a data center and paying for a complete and deployed solution

- Describe software as a service (SaaS): the most complete cloud service model from a product perspective

- Identify appropriate use cases for each cloud service (IaaS, PaaS, SaaS)

  IaaS; Lift-and-shift migration, Testing, and development,

PaaS; Development framework, Analytics, or business intelligence

SaaS; Email and messaging, Business productivity applications, Finance and expense tracking

Describe Azure architecture and services (35—40%)

Describe the core architectural components of Azure

Most Azure-specific commands will start with the letters az.

The core architectural components of Azure may be broken down into two main groupings: the physical infrastructure, and the management infrastructure.

- Describe Azure regional, regional pairs, and sovereign regions

  Azure Regional: geographical area on the planet that contains at least one, but potentially multiple data centers that are nearby and networked together with a low-latency network

  Regional Pairs: Most Azure regions are paired with another region within the same geography (such as the US, Europe, or Asia) at least 300 miles away.

  Sovereign Regions: Sovereign regions are instances of Azure that are isolated from the main instance of Azure. (related with the government)

- Describe availability zones

  Availability zones are physically separate data centers within an Azure region.

  Each availability zone is made up of one or more data centers equipped with independent power, cooling, and networking.

  If one zone goes down, the other continues working. (High Availability)

- Describe Azure datacenters

  The physical infrastructure for Azure starts with data centers.

  They’re facilities with resources arranged in racks, with dedicated power, cooling, and networking infrastructure.

- Describe Azure resources and resource groups

  Resources: A resource is the basic building block of Azure.

  Anything you create, provision, deploy, etc. is a resource. Virtual Machines (VMs), virtual networks, databases, cognitive services, etc. are all considered resources within Azure.

  Resource Groups: Resource groups are simply groupings of resources.

  When you create a resource, you’re required to place it into a resource group.

- Describe subscriptions

  Subscriptions are a unit of management, billing, and scale.

  subscriptions allow you to logically organize your resource groups and facilitate billing.

- Describe management groups

  manage access, policies, and compliance for subscriptions

- Describe the hierarchy of resource groups, subscriptions, and management groups

Describe Azure compute and networking services

three of the compute options virtual machines, containers, and Azure functions

- Compare compute types, including container instances, virtual machines (VMs), and functions

  VM: provide infrastructure as a service (IaaS) in the form of a virtualized server

  An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs the VM.

  Containers: virtualized environments for running applications

  Only libraries and components to run applications

You don't manage the operating system for a container.

Azure Container Instances offer the fastest and simplest way to run a container in Azure. (PaaS)

Azure Functions: an event-driven, serverless compute option that doesn’t require maintaining virtual machines or containers.

Functions scale automatically based on demand, so they may be a good choice when demand is variable.

- Describe VM options, including Azure Virtual Machines, Azure Virtual Machine Scale Sets, availability sets, and Azure Virtual Desktop

  VM Scale Sets: Automatically increase or decrease identical VMs in response to demand or a defined schedule. (High Elasticity)

  VM Availability Sets: for the highly available environment

  Azure Virtual Desktop: a desktop and application virtualization service that runs on the cloud. It enables you to use a cloud-hosted version of Windows from any location.

- Describe resources required for virtual machines

  Size (purpose, number of processor cores, and amount of RAM) Storage disks (hard disk drives, solid state drives, etc.) Networking (virtual network, public IP address, and port configuration)

- Describe application hosting options, including the Web Apps feature of Azure App Service, containers, and virtual machines

  VMs and containers provide excellent hosting solutions. VMs give you maximum control of the hosting environment and allow you to configure it

exactly how you want. VMs also may be the most familiar hosting method if you're new to the cloud. Containers, with the ability to isolate and individually manage different aspects of the hosting solution, can also be a robust and compelling option.

App Service: enables you to build and host web apps, background jobs, mobile back-ends, and RESTful APIs in the programming language of your choice without managing infrastructure.

Web App: App Service includes full support for hosting web apps by using ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, or Python.

- Describe virtual networking, including the purpose of Azure Virtual Networks, Azure virtual subnets, peering, Azure DNS, Azure VPN Gateway, and Azure ExpressRoute

  Azure virtual networks and virtual subnets enable Azure resources, such as VMs, web apps, and databases, to communicate with each other, with users on the internet, and with your on-premises client computers.

  Site-to-site virtual private networks link your on-premises VPN device or gateway to the Azure VPN gateway in a virtual network

  Azure VPN Gateway: VPN connection between Azure virtual network to your local network.

  Azure ExpressRoute provides dedicated private connectivity to Azure that doesn't travel over the internet. ExpressRoute is useful for environments where you need greater bandwidth and even higher levels of security.

  A private connection between your on-premise to Azure cloud (super fast)

  Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure

- Define public and private endpoints

Describe Azure storage services

Describe storage account:

- Core storage for big data
- Disk storage form VMs
- File system service for cloud
- Messaging storage
- No SQL

- Compare Azure storage services

  Azure Blobs: an object storage solution for the cloud. It can store massive amounts of data, such as text or binary data.

  Blob storage is ideal for:

  - Serving images or documents directly to a browser.
  - Storing files for distributed access.
  - Streaming video and audio.
  - Storing data for backup and restore disaster recovery, and archiving.
  - Storing data for analysis by an on-premises or Azure-hosted service.

  Azure Files: Managed file shares for cloud or on-premises deployments.

  Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) or Network File System (NFS) protocols.

  Azure Queues: A messaging store for reliable messaging between application components.

  Azure Disks: Block-level storage volumes for Azure VMs

Azure Table: NoSQL storage for unstructured data independent of any data schema.

- Describe storage tiers

  Hot access tier: Optimized for storing data that is accessed frequently (for example, images for your website).

  Cool access tier: Optimized for data that is infrequently accessed and stored for at least 30 days (for example, invoices for your customers).

  Archive access tier: Appropriate for data that is rarely accessed and stored for at least 180 days, with flexible latency requirements (for example, long-term backups).

- Describe redundancy options

  Locally redundant storage (LRS) replicates your data three times within a single data center in the primary region (11 nines)

  Zone-redundant storage (ZRS) replicates your Azure Storage data synchronously across three Azure availability zones in the primary region (12 nines- offline available)

  For applications requiring high durability, you can also copy the data in your storage account to a secondary region that is hundreds of miles away from the primary region.
  Azure Storage offers two options for copying your data to a secondary region:
  - Geo-redundant storage (GRS) copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region (the region pair) using LRS (16 nines)

    - Geo-zone-redundant storage (GZRS) storage account is copied across three Azure availability zones in the primary region (similar to ZRS) and is also replicated to a second geographic region, using LRS, for protection from regional disasters (16 nines)

- Describe storage account options and storage types

- Identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync

  In addition to large-scale migration using services like Azure Migrate and Azure Data Box, Azure also has tools designed to help you move or interact with individual files or small file groups.

  AzCopy is a command-line utility that you can use to copy blobs or files to or from your storage account.

  Azure Storage Explorer is a standalone app that provides a graphical interface to manage files and blobs in your Azure Storage Account.

  Azure File Sync is a tool that lets you centralize your file shares in Azure Files and keep the flexibility, performance, and compatibility of a Windows file server.

- Describe migration options, including Azure Migrate and Azure Data Box

  How to get your data and information into Azure

  Azure Migrate is a service that helps you migrate from an on-premises environment to the cloud.

  Azure Data Box is a physical migration service that helps transfer large amounts of data in a quick, inexpensive, and reliable way.

  You can order the Data Box device via the Azure portal to import or export data from Azure.

  Azure Archive Storage is for long-term storage.

Describe Azure identity, access, and security

- Describe directory services in Azure, including Azure Active Directory (Azure AD) and Azure Active Directory Domain Services (Azure AD DS)

  Azure Active Directory (Azure AD) is a directory service that enables you to sign in and access both Microsoft cloud applications and the cloud applications that you develop. Azure AD can also help you maintain your on-premises Active Directory deployment.

  Azure AD identity and access management service

  The method of connecting Azure AD with your on-premises AD is using Azure AD Connect. Azure AD Connect synchronizes user identities between on-premises Active Directory and Azure AD.

  Just like Azure AD lets you use directory services without having to maintain the infrastructure supporting it, with Azure AD DS, you get the benefit of domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

- Describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication, and passwordless

  Authentication is the process of establishing the identity of a person, service, or device

  Single sign-on (SSO) enables a user to sign in one time and use that credential to access multiple resources and applications from different providers (only one ID and one password)

  Multifactor authentication is the process of prompting a user for an extra form (or factor) of identification during the sign-in process (phone call or mobile app notification)

  You have to use a second device

  Passwordless authentication methods are more convenient because the password is removed and replaced with something you have, plus

something you are, or something you know.

- Describe external identities and guest access in Azure

  An external identity is a person, device, service, etc. that is outside your organization. Azure AD External Identities refers to all the ways you can securely interact with users outside of your organization.

- Describe Azure AD Conditional Access

  Conditional Access is a tool that Azure Active Directory uses to allow (or deny) access to resources based on identity signals. These signals include who the user is, where the user is, and what device the user is requesting access from.

- Describe Azure role-based access control (RBAC)

  Azure enables you to control access through Azure role-based access control (Azure RBAC).

  Azure RBAC helps you manage who has access to Azure resources.

  Role assignments: the way you control access to resources

  Azure provides built-in roles that describe common access rules for cloud resources. You can also define your own roles. Each role has an associated set of access permissions that relate to that role. When you assign individuals or groups to one or more roles, they receive all the associated access permissions

- Describe the concept of Zero Trust

  Zero Trust is a security model that assumes the worst-case scenario and protects resources with that expectation. Zero Trust assumes breach at the outset, and then verifies each request as though it originated from an

uncontrolled network.

- Describe the purpose of the defense-in-depth model

  The objective of defense-in-depth is to protect information and prevent it from being stolen by those who aren't authorized to access it.

  A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack aiming to acquire unauthorized access to data.

- Describe the purpose of Microsoft Defender for Cloud

  Defender for Cloud is a monitoring tool for security posture management and threat protection. It monitors your cloud, on-premises, hybrid, and multi-cloud environments to provide guidance and notifications aimed at strengthening your security posture.

  Defender for Cloud provides the tools needed to harden your resources, track your security posture, protect against cyber attacks, and streamline security management. Deployment of Defender for Cloud is easy, it’s already natively integrated into Azure.

Describe Azure management and governance (30—35%)

Describe cost management in Azure

- Describe factors that can affect costs in Azure

  Resource Type: The type of resources, the settings for the resource, and the Azure region will all have an impact on how much a resource costs.

  Consumption: Pay-as-you-go

  Maintenance:

Geography: Global deployment comes with global pricing differences

Network Traffic: For outbound data transfers (data leaving Azure datacenters), data transfer pricing is based on zones.

Subscription Type: Some Azure subscription types also include usage allowances, which affect costs.

Azure Marketplace: Azure Marketplace lets you purchase Azure-based solutions and services from third-party vendors. (Like Apple store)

- Compare the Pricing calculator and the Total Cost of Ownership (TCO) calculator

  The pricing calculator is designed to give you an estimated cost for Azure products.

  The TCO calculator is designed to help you compare the costs for running an on-premises infrastructure compared to an Azure Cloud infrastructure. (Estimate the cost savings)

- Describe the Azure Cost Management and Billing tool

  Cost Management provides the ability to quickly check Azure resource costs, create alerts based on resource spending, and create budgets that can be used to automate the management of resources.

- Describe the purpose of tags

  Resource tags are another way to organize resources. Tags provide extra information, or metadata, about your resources.

Describe features and tools in Azure for governance and compliance

- Describe the purpose of Azure Blueprints

  Azure Blueprints lets you standardize cloud subscription or environment deployments. Instead of having to configure features like Azure Policy for each new subscription, with Azure Blueprints, you can define repeatable settings and policies that are applied as new subscriptions are created.

- Describe the purpose of the Azure Policy

  Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources.

  Policy Definitions (JSON Format)

- Describe the purpose of resource locks

  A resource lock prevents resources from being accidentally deleted or changed.

- Describe the purpose of the Service Trust Portal

  The Microsoft Service Trust Portal is a portal that provides access to various content, tools, and other resources about Microsoft security, privacy, and compliance practices.

Describe features and tools for managing and deploying Azure resources

- Describe the Azure portal

  The Azure portal is a web-based, unified console that provides an alternative to command-line tools. With the Azure portal, you can manage your Azure subscription by using a graphical user interface

- Describe Azure Cloud Shell, including Azure CLI and Azure PowerShell

  Azure Cloud Shell is a browser-based shell tool that allows you to create, configure, and manage Azure resources using a shell. (Command line)

  Azure Cloud Shell supports both Azure PowerShell and the Azure Command Line Interface (CLI), which is a Bash shell.

  Azure CLI can be downloaded to your computer(terminal)

- Describe the purpose of Azure Arc

  Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.

- Describe Azure Resource Manager and Azure Resource Manager templates (ARM templates)

  Azure Resource Manager (ARM) is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account.

By using ARM templates, you can describe the resources you want to use in a declarative JSON format.

ARM allows you to programmatically(code) create Azure resources via JSON template.

Describe monitoring tools in Azure

- Describe the purpose of Azure Advisor

  Azure Advisor evaluates your Azure resources and makes recommendations to help improve reliability, security, and performance, achieve operational excellence, and reduce costs. (Personalized cloud consultant)

- Describe Azure Service Health

  Azure Service Health helps you keep track of Azure resources, both your specifically deployed resources and the overall status of Azure.

  Information about current and upcoming issues

  Azure status informs you of service outages in Azure

  Service Health provides a personalized view of Azure services and regions you are using

  Resource Health provides information about the health of your individual cloud resources (ex. VMs)

- Describe Azure Monitor, including Log Analytics, Azure Monitor alerts, and Application Insights

  Azure Monitor is a platform for collecting data on your resources, analyzing that data, visualizing the information, and even acting on the results. Azure Monitor can monitor Azure resources, your on-premises resources, and even multi-cloud resources like virtual machines hosted with a different cloud provider.

Azure Monitor Alerts are an automated way to stay informed when Azure Monitor detects a threshold being crossed.

Application Insights, an Azure Monitor feature, monitors your web applications. Application Insights is capable of monitoring applications that are running in Azure, on-premises, or in a different cloud environment.