|  |
| --- |
| **Cloud concepts**   * Cloud language terminologies   + High Availability is core to the cloud   + Fault Tolerance (for zero downtime in case of outages)   + Disaster Recovery (through Time to recovery and Recovery Points)   + Scalability (thru Scaling out/in or Scaling up/down)     - Scale out (non-disruptive)     - Scale up (disruptive)   + Elasticity (ability to quickly expand or decrease computing resources, not just VMs). Elasticity is showing scalability in both directions (in/out or up/down)   + Agility (rapidly develop, test and launch software applications)     - Organization’s ability to rapidly adapt to market and environmental changes * The economy of Cloud computing   + CapEx (Capital Expenditure by business to acquire or maintain fixed assets)   + OpEx (Operational Expenditure is the ongoing cost to run a business)   + Move to cloud is a move from CapEx to OpEx   + Cloud supports consumption-based pricing * Cloud service models   + IaaS     - VMs and servers     - Networks     - Other physical assets   + PaaS     - Middleware     - Tools (databases etc.)   + SaaS     - Apps      * + Serverless     - Azure Functions are best known serverless services * Shared responsibility model |
| **Cloud architecture model**   * Public   + Multi-tenant implementation (many organizations share the same resources)   + Owned and operated by service provider (Azure)   + Lower cost of operation * Private   + Single tenant implementation   + Owned and operated by IT organization   + Fully customizable   + Higher cost of operation * Hybrid   + Best of both world   + Greater flexibility   + Optimal usage of resources   + Greater resilience to outages |
| **Regions and Availability zones**   * Regions   + Geographic area containing a set of data centers linked by high-speed, low-latency network   + Two types of set-ups for multi-region deployment: Active/passive and Active/active * Three main criteria to choose a region   + Location (should be closer)   + Availability of features (check it beforehand)   + Price (defers from region to region) * Each region is paired with exception of Brazil south (as on Dec2020). This pairing is for outage failover * Availability zones   + Unique physical locations within an Azure region made up of one or more data centers   + Each zone has its own power, cooling and networking   + To ensure resiliency, each region should have at least three different availability zones   + The physical separation of availability zones within a region protects application and data from data center failures |
| **Resource groups and Azure Resource Manager**   * Azure Resource group is a logical entity, not a resource itself * Resources in different geographical regions can be nested within one resource group * A single resource can be part of one resource group only * ARM provides centralized deployment and management services for resources * ARM provides the following   + Centralized service to manage any resources on Azure   + Group resource handling   + Consistency in deployment of resources   + Dependency management and mitigation   + Access control   + Tagging of resources   + Billing of resources * Azure portal, Azure CLI, Azure power shell all make use of the services of ARM API * Azure provides four levels of management scopes   + Management groups   + Subscriptions   + Resource groups   + Resource Management Groups |

|  |
| --- |
| **Azure Compute Service**   * Virtual Machines are part of the IaaS offering * Azure Blueprint is a template that guides how a VM should be created * Price for VMs are calculated per hour * You can choose the CPU, RAM size and OS for your VM * A VM is for your exclusive usage * Azure Scale sets are auto scaling pool of VMs * VMs within a scale sets are load balanced by Azure * A baseline VM is what you copy to make up the scale set VMs * App services are PaaS part of Azure Compute * Enables us to build and host web apps, mobile back ends and RESTful APIs * App services come in three main categories   + Web Apps   + Web apps for containers   + API Apps * Azure container instances help you to manage all the dependencies in a container * ACI is the primary Azure service for running container workloads * A workload is your process or application |
| **Azure Kubernetes Service**   * K8s is an open-source container orchestration system for   + Automating application deployment   + Container Scaling   + Container Management * AKS is managed and hosted by Azure to provide all these services * Azure Container Registry (ACR) keeps track of current valid container images * ACR feeds container images to ACI (Azure Container Instances) and AKS * An AKS cluster has a set of machines (nodes) * Nodes run containerized application managed by Kubernetes * Pod is a group of one or more containers with shared storage network and a specification for how to run the containers * Pods are hosted on Nodes     **Azure Functions**   * Smallest compute service on Azure, a single function of compute * It only runs when there is data to process |
| **Azure Network service**   * Azure Virtual Network (Azure VNet or AVN)   + No direct control over networking hardware   + Isolate our own network within the Azure worldwide network   + To prevent/permit access to/from other networks or Internet   + Provides the backbone of all other networking solutions provided by Azure * AVN can be further subdivided into subnets or Network Security Groups * An address space is a range of IP address that are allocated to the VNet   + Each resource within the VNet takes a unique address from that address space   + Subnets are further subdivisions of an allocated address space * Every VNet belongs to a single region. Every resource on the VNet must be in the same region too * Each VNet belongs to a single subscription * VNets in the cloud can scale, have high availability and isolation * Azure Load balancer is a front-end tool that balances the inbound network traffic that is coming to your VMs * Inbound flows might be traffic from Internet or local network * Azure VPN (Virtual Private Network) gateway allows   + Encrypted traffic between AVN to an On-prem network over the public internet * Main components of Azure VPN   + An Azure VNet with a VPN gateway attached. This gateway has its own public IP address   + A secure channel called a Tunnel with data encryption mechanism   + An on-prem network with a complementary gateway that can accept the encrypted data        * VPN gateways are instrumental in hybrid cloud architecture * In simplest terms, an Application gateway is a customizable load balancer * It’s a web traffic load balancer which works on HTTP request properties rather than simple IP address/port information * Benefits of Application Gateway   + Scaling   + Encryption   + Zone Redundancy   + Multi-site hosting * Azure Content Delivery Network (CDN) is a distributed network of servers that can deliver web content close to users * Finds closest server to a user (edge servers) to deliver these contents to minimize latency * Benefits of CDN * The central server from which data is replicated to edge servers, is called Origin server * Benefits of CDN   + Better performance   + Scaling   + Distribution * Express Route is the fastest data connection between your on-prem and Azure and it does not goes through the internet * Express Route is a private, secure, high-bandwidth, low-latency connection |
| **Azure Storage Service**   * Storage account name should be unique across Azure * Storage services   + Disks (IaaS service – Hard drive images for Azure Virtual Machines)   + Files (IaaS service – A full scale file system to store and manage any kinds of file)   + Blobs (PaaS service – helps to store unstructured data, cannot query it only by ID)   + Archive |
| * Blobs are stored within containers in a storage account * Azure storage supports three types of blobs   + Block (for text and binary images)   + Append (for log data)   + Page (files up to 8 TB) * Blob store comes in three main pricing tiers   + Hot   + Cool   + Archive * There are four main disk types to choose from for your VMs   + HDD (Hard Disk Drive)   + Standard SSD (Solid State Drive)   + Premium SSD   + Ultra Disk (best in class for demanding applications) * Benefits of Azure File Storage   + Sharing   + Managed   + Resilient * Archive is used for data that are used very rarely. Cost is lowest * Archive storage is a blob storage tier |
| **Azure Database Service**   * Azure Cosmos DB (a NoSQL database), globally distributed, auto-scalable and supports many APIs * Cosmos DB latency is 0-9 milliseconds all over the world * Downside is the cost factor * Azure SQL is basically Database as a Service. It’s a fully managed service * Benefits provided are   + High availability and scalability   + Huge storage space   + Security * MySQL is an open source project maintained by a community * Azure database for MySQL is a PaaS      * PostgreSQL is the default database for MacOS * Some important features are   + Extensions   + Horizontal scaling   + Performance recommendations   + Fully managed * Azure Database Migration service (can be performed in two ways – Online and Offline migration) |

|  |
| --- |
| **Authentication and Authorization**   * Azure Active Directory is the core identity service * For any application, first you get authenticated, then authorized * Authentication process ensures ‘you are you’ by confirming your identity * Authorization is the granular part of identity services to check your access on resources |
| **Azure Active Directory**   * Active Directory was designed for traditional office use with computers and printers * Microsoft Active Directory and Azure Active Directory (AAD) are different products * You cannot have an Azure account without an AAD service * A tenant represents an organization * A tenant is a dedicated instance of AAD that an organization receives when signing up for Azure * Each Azure AD tenant is distinct and separate from other Azure AD tenants * Each user in Azure can only belong to a single tenant, but can be guest in other tenants * Hybrid cloud architecture is when some resources are on-prem and some are on cloud. AAD plays an important role here |
| **Multi-Factor Authentication**   * In MFA, you need at least two ways to authenticate yourself at log-in * MFA is built into AAD. It depends on the following   + Something you know (user id and Password)   + Something you have (a key or mobile app)   + Something you are (biometrics) |
| **Single Sign-on (SSO)**   * Using the same username and password combination to login to multiple services * You can enable the SSO service in AAD |
| **Azure solutions**   * Can be used in two different ways   + Prepackaged multiple solution products (bundled together as one unit) that are easy for end user to consume by managing less   + Specific product (e.g. Serverless computing etc.) that can be used individually or interfaced with other systems already in use |
| **Internet of Things (IoT)**     * Made up of one/more IoT devices and one/more back-end services running in the cloud that communicate with each other. This communication is biway * The above communication does not require human-to-human or human-to-computer interaction * Azure IoT Hub: Collects data from millions of devices. Core Azure PaaS (Platform as a Service) * Azure IoT Central – Fully managed SaaS (Software as a Service) solution provided by Azure * Two ways to use IoT in Azure   + Use IoT hub where you need more control on your devices and data processing   + Use IoT central where you just need to configure and use your IoT project * Azure Sphere is an all-in-one solution for IoT devices * Azure Sphere mandates what hardware you can use as it gives you a robust security feature |
| **Big data and Analytics**   * To store huge amount of data and to query it to get specific information in a reasonable amount of time. It is to say how to extract value from really large amount of data * Four stages of Big data and related analytics operations   + Ingest   + Store   + Prepare and Train   + Model and Serve * Azure tools for Big data and Analytics are   + Azure HDInsight (uses all open source frameworks, e.g. Apache Hadoop, Spark and Kafka)   + Azure Data Lake (huge reservoir of data that supports parallel processing)   + Azure Data Bricks (provides computing power of a cluster and integrates with other storage services)   + Azure Synapse Analytics (previously called Azure SQL data warehouse, used for reporting and data analytics. Uses Synapse SQL to work) |
| **Azure AI and Machine Learning services**   * Machine learning is a data science technique that allows computers to use existing data to forecast future behaviors, outcomes and trends * With ML, computers learn without being explicitly programmed * Microsoft focusses three things to make Azure AI capable platform   + Models   + Knowledge-mining (to search for insights in data)   + Built-in apps * The final output from ML program is called a model. It consolidates all the rules that the ML program has figured out * Once model is there, we can supply it with input data. Aided by the Machine learning service it provides the required output for us * The main tool in Azure for ML is Azure Machine Learning Studio (SaaS) * Azure Cognitive Services are   + Vision service   + Decision service   + Speech service * Machine Learning Service is an end-to-end service that provides the following   + Tooling   + Automation |
| **Serverless computing**   * Serverless computing is a misnomer. Servers are there but we don’t have to manage or administer the server to run our application * The steps to run your application are   + Upload your code   + Set up your code to be triggered by other Azure services etc.   + Code is run only when triggered by the Azure service that you have set up   + Pay only for the time and resources it used while running * Serverless computing is event driven. It executes only when the triggering event occurs * There are three types of Serverless computing in Azure   + Azure functions (effective for simple or single step tasks)   + Azure logic apps (effective for huge workflows with a visual designer. Connect systems both inside and outside of the Azure platform)   + Azure event grid (an event routing service. A big network of services to connect almost any services available on Azure) |
| **Azure DevOps**   * Azure DevOps is a platform consisting of five different tools   + Azure boards (keep track of work tasks, timelines and issues)   + Azure pipelines (producing and testing your software continuously)   + Azure Repos (secured and managed way to store all your source codes)   + Azure Test plans (design test plans and their automated executions)   + Azure Artifacts (to share your applications and code libraries with other parties) * Azure DevTest labs allow developers and engineers to create environments for test and development * GitHub was bought by Microsoft in 2018 * GitHub actions are very similar to Azure DevOps pipelines |
| **Security**   * Defense in depth means many layers of defense * On-prem defense means you are in charge of all your hardware, software, infrastructure etc. * There are 7 general layers of security and this is applicable for Azure too   + Physical (data centers)   + Identity and access (Azure AD authentication and authorization)   + Perimeter (protection against DoS, volumetric etc. attacks)   + Network (filter of traffic to/from Azure)   + Compute (protects against intruders trying to get access to your VMs)   + Gateways and Firewalls (provide securities for Azure applications)   + Data (encrypted and properly protected) |
| **Securing Network Connectivity**   * Rules in the Firewall protects the system from illegitimate traffic * DDoS is one the most common forms of attacks against the services of Internet * Azure has a DDoS protecting service * Network Security Group (NSG) is a personal resource firewall * Application Security Group is an extension of NSG. It secures an application |
| **Azure Security Center**   * A portal within the Azure portal * To use security centre, we generally use a three-step procedure   + Define security policies   + Actively protect your resources   + Respond to any security alerts |
| **Azure Key-vault**   * A secured place to store passwords and other secrets * Key vault features   + Secure hardware (not even Mircosoft can access the keys in it   + Application isolation   + Global scaling |
| **Azure Information Protection**   * This service helps to   + Classify data (automatically based on policies or manually)   + Track activities on shared data   + Share data with others   + Integration with other apps |
| **Advanced Threat Protection**   * Monitor users * Baseline behavior * Suggest changes * Cyber-attack kill-chain acts on   + Reconnaissance   + Brute Force   + Increasing Privileges |
| **Azure Sentinel**   * A security information and event-management tool * It carries out the following steps   + Data collection   + Data is aggregated and normalized (make it more usable)   + Analysis and threat detection * Sentinel uses AI to learn if any detected behavior is unusual * Can integrate with AWS * Can take advantage of cloud scale |
| **Azure Dedicated Host**   * Hardware control (you get control of entire physical server on Azure) * It is yours and yours alone * Maintenance (you can choose when to install updates to your dedicated host) * Cloud benefits of using Azure dedicated host   + Compliance   + Global infrastructure   + OS of your choice |

|  |
| --- |
| **Governance**   * Is a set of policies and rules to set up acceptable usage of Azure resources * It is implemented through   + Azure policies (a set of rules to ensure resource are compliant)   + RBAC is a critical component in the governance of usage of resources   + Role assignment through RBAC has three elements     - Security Principle (object representing user/group to access resources)     - Role definition (collection of permissions e.g. Read, Write, Delete)     - Scope (the set of resources to which the access applies to)   + Resource usage are managed through locks that are applicable to subscriptions     - Read-Only lock means user cannot make any changes to that resource     - Delete lock means user cannot delete the resource * Azure Blueprints are templates for creating resources * Azure Blueprints contain   + Resource Templates   + RBAC   + Policies   + Samples for Common regulations * Cloud Adaption Framework is a collection of documents that guide you through entire process of cloud adaption for your organization * Azure Advisor for Security assistance is a part of Security center to assist governance |
| **Azure Monitor**   * Single monitoring platform for every types of Azure resource possible * Azure Monitor helps you find resources that aren’t performing 100% * Azure Monitor receives constant feeds (telemetry data) from all resources in use * All monitoring information goes to Azure monitor in form of   + Metrics   + Logs * Metrics mainly contains performance data with respect to date and time * Textual information coming out from applications that are needed to debug in case anything goes wrong * Monitoring data provides insights to the application * Outcome of using Azure Monitor   + Maximize availability   + Maximize performance   + Identify issues |
| **Azure Service Health**   * Provides view about the health of all Azure services and all Azure regions * Notifies you about all planned and unplanned incidents about Azure platform * There are three different ways to track health issues   + Service issues   + Planned Maintenance   + Health advisors * Azure service health status is shown to you through   + Azure Portal   + Azure Monitor   + A status web page dedicated for this (status.azure.com) * Azure Service Health is a free service |
| **Compliance**   * Industry compliance   + General Data Protection Regulation (an EU standard)   + International Standardization Organization (a global standards body)   + National Institute of Standards and Technology (a US Federal standard for techs) * GDPR aims to give control to individuals residing in EU over their personal data   + Azure data subject requests for the GDPR   + Azure Policy   + Compliance manager   + Azure information protection   + Azure security center * ISO (International Organization for Standardization) sets standards for organizations to be compliant * Azure leads the cloud industry in ISO certifications * NIST (National Institute of Standards and Technology) sets standards for US government levels * Over NIST, Microsoft also provides FedRAMP (Federal Risk and Authorization Management Program) * Azure Compliance manager is the tool to help you out here * Azure Government Cloud provides dedicated datacenters to US Government bodies |
| **Privacy**   * Microsoft Privacy Statement explains   + What personal data Microsoft processes from the user   + How they process it   + For what purpose they process it * Puts Microsoft’s commitments in writing and details data protection policies and practices in clear English |
| **Trust**   * Two main services   + Trust Center (to learn about MS efforts in Security, Privacy, Compliance etc.)   + Service Trust Portal (to review all the independent reports and Audits) * Microsoft Trust Center a hub of information about trust in each product and service * The following sections are available within the trust center   + Security   + Privacy   + Compliance   + Transparency   + Products and Services * Service Trust Portal (to review all the independent reports and audits performed on Microsoft’s products and services * Azure complies with more standards than any other cloud provider |
| **Pricing**   * Subscription is the basic unit of managing your Azure billing * Azure reservation is a way to save money while using Azure subscriptions * Azure Enterprise Agreement has some premium features like Azure Active Directory premium etc. |
| **Subscriptions**   * At the root of every invoice is the subscription * Every resource within Azure lives within a subscription * An Azure account can have multiple subscriptions * Offer type is the type of subscription * Management groups can group many subscriptions in a large organization * Management groups can be nested in a hierarchy |
| **Cost Management**   * Some costs are regular, predictable and some are dynamic, on-demand type * Cost management options for free is free account * Azure Cost management tool is accessible from Azure Portal * Spot VM usage gives you deep discounts (as you are tapping unused capacities) |
| **Pricing Factor**   * Influencing factors on pricing are   + Resource Size   + Resource Type   + Location   + Bandwidth * Azure has three billing zones worldwide containing regions * Data transfer between regions of each billing zone is free * Data transfer between different billing zones are charged as   + Ingress data (data coming in) – free   + Egress data (data going out) – charged * Microsoft provides a tool to calculate cost – the Pricing calculator * Total Cost of Ownership (TCO) is the cost calculator provided by MS in the long run * TCO calculates and shows how much you can save by migrating your workload from On-Prem to Azure cloud |
| **Best Practices**   * Spending limits restricts user to go beyond a certain limit of usage that incurs charge * Pay-as-you-go does not have any spending limits * Quota is another way to provide a predictable usage on Azure services * Pay-as-you-go often gets expensive if not managed properly * Reserved instances can save a lot of money over a specified period * Azure Cost Advisor is a tool to save you some costs for resource usage |
| **Support Plans**   * There are five support plans available for Azure   + Basic   + Developer   + Standard   + Professional Direct   + Premier * The following services are included with all support plans free of charge   + 24/7 access to billing and subscription support   + On-line self help   + Forums (to connect with other Azure users)   + Azure advisor   + Service Health * The more you pay, the more services you get with less time |
| **Tickets**   * A ticket is a support enquiry with a unique identifier * Ticket types can be of the following four types   + Billing   + Service and subscription limits   + Subscription management   + Technical |
| **Channels**   * Azure documentation * Forums * Social media |
| **Azure Knowledge Center**   * Answers common questions that people new to Azure might have * You cannot add a new question to the knowledge center, but can only search |
| **Azure Service Level Agreement**   * A service level agreement is a contract between a service provider and the client * SLA ensures confidence in the uptime and reliability of the services * It is a commitment contract from Microsoft for uptime * In general, there is no SLAs for free products and services * Uptime is guaranteed (but not Performance, Bandwidth or Feature availability) * Expressed as a percentage of total time per month that the service is guaranteed to be up * The formula to calculate SLA is   **Monthly uptime % = ((Max. Available mins – downtime) / Max Available mins) \* 100**     * Every product and service within Azure have their own distinct SLAs |
| **Azure Service Lifecycle**   * Public and Private preview states (to check a service before its available to all) * General availability (features available for everyone to use) * The rollout of general availability features can be gradual through region by region * Check the Azure Update feed for preview features |

|  |
| --- |
| **How to prepare for AZ-900 exam (Microsoft Certified Azure Fundamentals)**   * 44 questions to be answered in 60 minutes * Costs 99 USD * Question pattern: MCQ, true/false, Drag and drop (no case studies)      * Exam parts are as shown below:        * Results are shown to you immediately after you have taken the exam * You need 700 points out of 1000 allocated points to pass the exam |