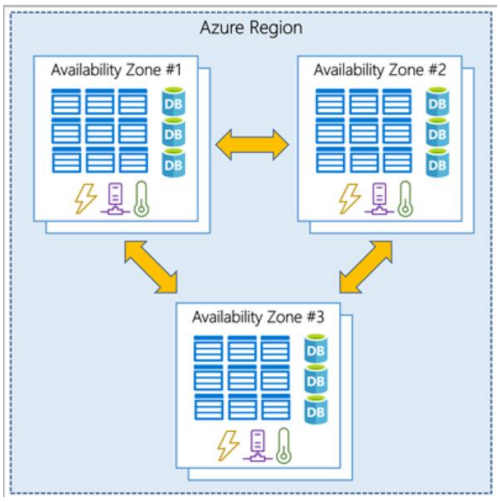
1- Describe Azure architecture and services :

Azure is a continually expanding set of cloud services that help you meet current and future business challenges. Azure gives you the freedom to build, manage, and deploy applications on a massive global network using your favorite tools and frameworks.

Physical Infrastructure :

- **Regions :** A region is a geographical area on the planet that contains at least one, but potentially multiple datacenters that are nearby and networked together with a low-latency network.
- **Region pairs :** Most Azure regions are paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away. This approach allows for the replication of resources across a geography that helps reduce the likelihood of interruptions because of events such as natural disasters, civil unrest, power outages, or physical network outages that affect an entire region. [reliable services, data redundancy.
- **Availability zone :** physically separate datacenters within an Azure region. Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking.
- **Sovereign regions :** are instances of Azure that are isolated from the main instance of Azure. You may need to use a sovereign region for compliance or legal purposes.



Availability zones are primarily for VMs, managed disks, load balancers, and SQL databases. Azure services that support availability zones fall into three categories:

- **Zonal services:** You pin the resource to a specific zone (for example, VMs, managed disks, IP addresses).
- **Zone-redundant services:** The platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).

- **Non-regional services:** Services are always available from Azure geographies and are resilient to zone-wide outages as well as region-wide outages.

Management infrastructure :

It includes Azure resources, resource groups, subscriptions, and accounts.

- **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 :** groupings of resources.
    - A resource is required to be placed under a resource group.
    - 1 resource exist only in 1 resource group.
    - RG cannot be nested.
    - When you apply an action to an RG it will be applied to all the resources within the resource group.
    - If you grant access to an RG, you did to all resources under this RG.
- **Azure subscriptions :** subscriptions are a unit of management, billing, and scale. Similar to how resource groups are a way to logically organize resources, subscriptions allow you to logically organize your resource groups and facilitate billing.
    - **Billing boundary :** create multiple subscriptions for different requirements.
    - **Access control boundary :** at the subscription level, you can create separate subscriptions to reflect different organizational structures.
- **Azure Management group :** If you have many subscriptions, you might need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. *You organize subscriptions into containers called management groups and apply governance conditions to the management groups.* All subscriptions within a management group automatically inherit the conditions applied to the management group, the same way that resource groups inherit settings from subscriptions and resources inherit from resource groups. Management groups give you enterprise-grade management at a large scale, no matter what type of subscriptions you might have. Management groups can be nested.

Important facts about management groups:

- 10,000 management groups can be supported in a single directory.
- A management group tree can support up to six levels of depth. This limit doesn't include the root level or the subscription level.
- Each management group and subscription can support only one parent.

2- Describe Azure Compute and Network Services :

Azure Virtual Machines :

VMs provide infrastructure as a service(Iaas), they give total control over the OS, ability to run custom software, use custom hosting configuration.

To group VMs use scale sets.

- **Scale sets :** lets you to centrally manage, configure, and update a large number of VMs in minutes. It automatically deploy a LB to ensure resources are being used efficiently.
- **Availability sets :** Availability sets are designed to ensure that VMs stagger updates and have varied power and network connectivity, preventing you from losing all your VMs with a single network or power failure.
    - **Update domain :** all machines in one update domain will be updated at the same time (allow to apply updates).
    - **Fault domain :** group VMs by common power source and network switch. (split across up to 3 fault domains)

Azure Virtual Desktops :

- It is a desktop and application virtualization service that runs on the cloud. It enables you to run a cloud hosted version of windows from any location.
- AzVD provides centralized security management for users' desktops with Azure Active Directory, multifactor auth… The data and apps are separated from the local hardware. The risk of confidential data left on a personal device is reduced.
- Windows 11 Enterprise multi-session, that enables multiple concurrent users on a single VM.

Azure Containers :

If you want to run multiple instances of an application on a single host machine, containers are an excellent choice.

- **Containers :** are a virtualization environment, where you don't manage the operating system unlike VMs. They are an instance of an OS that you can connect to and manage. Containers are lighter, and more agile. One of the most popular container engines is Docker, which is supported by Azure.
- **Azure Containers Instances :** it is a PAAS that offer the fastest and simplest way to run a container in Azure. It allows you to upload your containers and then the service will run them for you.

Azure Functions :

Azure Functions is an event-driven, serverless compute option that doesn't require maintaining virtual machines or containers. If you build an app using VMs or containers, those resources have to be "running" in order for your app to function. With Azure Functions, an event wakes the function, alleviating the need to keep resources provisioned when there are no events.

Using Azure Functions is ideal when you're only concerned about the code running your service and not about the underlying platform or infrastructure. Functions are commonly used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.

- It runs your code when it is triggered and automatically deallocates resources when the function is finished.

Functions are a key component for serverless computing. They are also a general compute platform for running any type of code.

Azure App Service :

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. It offers automatic scaling and high availability. App Service supports Windows and Linux. It enables automated deployments from GitHub, Azure DevOps, or any Git repo to support a continuous deployment model.

Azure App Service lets you focus on building and maintaining your app, and Azure focuses on keeping the environment up and running.

- You can host most common app service styles like :
    - Web apps
    - API apps
    - WebJobs
    - Mobile apps

Azure Virtual Networking :

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.

Azure virtual networks provide the following key networking capabilities:

- Isolation and segmentation
- Internet communications
- Communicate between Azure resources
- Communicate with on-premises resources
- Route network traffic
- Filter network traffic
- Connect virtual networks

Azure virtual network allows you to ***create multiple isolated virtual networks.***

- **Internet communications :** You can enable incoming connections from the internet by assigning a public IP address to an Azure resource, or putting the resource behind a public load balancer.
- **Route network traffic :** By default, Azure routes traffic between subnets on any connected virtual networks, on-premises networks, and the internet. You also can control routing and override those settings, as follows :
    - Route tables allow you to define rules about how traffic should be directed. You can create custom route tables that control how packets are routed between subnets.
    - Border Gateway Protocol (BGP) works with Azure VPN gateways, Azure Route Server, or Azure ExpressRoute to propagate on-premises BGP routes to Azure virtual networks.
- **Filter Network Traffic :** allows to filter traffic using 2 approaches
    - Network Security Groups
    - Network Virtual Appliances : A network virtual appliance carries out a particular network function, such as running a firewall or performing wide area network (WAN) optimization.
- **Connect virtual Networks :** using Virtual Network Peering, network traffic between peered networks is private.

Azure Virtual Private Networks :

A virtual private network (VPN) uses an encrypted tunnel within another network. VPNs are typically deployed to connect two or more trusted private networks to one another over an untrusted network (typically the public internet). Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks.

When deploy a vpn gateway, you specify the VPN type, either :

- **Policy based :** specify statically the IP address of packets that should be encrypted through each tunnel.
- **Route based :** IPSec tunnels are modeled as a network interface or virtual tunnel interface. IP routing (either static routes or dynamic routing protocols) decides which one of these tunnel interfaces to use when sending each packet.
    - Connection between virtual networks
    - Point -to-site connections
    - Multisite connections
    - Coexistence with an Azure ExpressRoute gateway.
- **High availability scenarios :**
    - Active/standby

- Active/active
- ExpressRoute failover
- Zone-redundant gateway

Azure Express Route :

Azure ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection, with the help of a connectivity provider. This connection is called an ExpressRoute Circuit.

Benefits :

- Connectivity to Microsoft Cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with the ExpressRoute Reach.
- Dynamic routing between your network and microsoft via BGP
- Built-in redundancy in every peering location for higher reliability.

Allows direct access to : Office365, Microsoft Dynamics 365, Azure compute services, cloud services …

ExpressRoute connectivity models

ExpressRoute supports four models that you can use to connect your on-premises network to the Microsoft cloud:

- CloudExchange colocation
- Point-to-point Ethernet connection
- Any-to-any connection
- Directly from ExpressRoute sites

Azure DNS :

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records using the same credentials, APIs, tools, and billing as your other Azure services.

Benefits :

- Reliability and performance
    - Azure DNS uses anycast networking, so each DNS query is answered by the closest available DNS server to provide fast performance and high availability for your domain.
- Security : Based on Azure Resource Manager, that :
    - provide Azure rôle-based access control (Azure RBAC) to control who has access to specific actions for your organization.
    - Activity logs to monitor how a user in your organization modified a resource or to find an error when troubleshooting.
    - Resource locking to lock a subscription, resource group, or resource. Prevents other users in your organization from accidentally deleting or modifying critical resources.
- Ease of use
- Customizable virtual networks
- Alias records

Describe Azure Storage Services :

Describe Azure Storage Accounts :

A storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over http or HTTPS. Data in this account is secure, highly available, durable and massively scalable.

Type	Supported services	Redundancy Options	Usage
Standard general-purpose v2	Blob Storage (including Data Lake Storage), Queue Storage, Table Storage, and Azure Files	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios using Azure Storage. If you want support for network file system (NFS) in Azure Files, use the premium file shares account type.
Premium block blobs	Blob Storage (including Data Lake Storage)	LRS, ZRS	Premium storage account type for block blobs and append blobs. Recommended for scenarios with high transaction rates or that use smaller objects or require consistently low storage latency.
Premium file shares	Azure Files	LRS, ZRS	Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both Server Message Block (SMB) and NFS file shares.
Premium page blobs	Page blobs only	LRS	Premium storage account type for page blobs only.

Azure storage redundancy

- **Redundancy in the primary region**
  - **Locally redundant storage (LRS) :** replicates your data three times within a single data center in the primary region. Is the lowest cost, and offers the least durability compared to other options.
  - **Zone redundant storage (ZRS) :** replicates your Azure Storage data synchronously across three Azure availability zones in the primary region. Microsoft recommends using ZRS in the primary region for scenarios that require high availability. ZRS is also recommended for restricting replication of data within a country or region to meet data governance requirements.
- **Redundancy in a secondary region :**
  - **Geo-redundant storage (GRS):** copy 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 using LRS.

- **Geo-zone-redundant storage (GZRS):** running ZRS in the primary region and LRS in the secondary region.

Read access to data in the secondary region

Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is available to be read only if the customer or Microsoft initiates a failover from the primary to secondary region. However, if you enable read access to the secondary region, your data is always available, even when the primary region is running optimally. For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).

Describe Azure Storage Services :

Benefits :

- Durable and highly available : ensured by redundancy if trabsient hardware failures occur.
- Secure : data is encrypted.
- Scalable
- Managed
- Accessible

Azure Storage platform includes the following data services :

- **Azure Blobs**: A massively scalable object store for text and binary data. Also includes support for big data analytics through Data Lake Storage Gen2.
- **Azure Files**: Managed file shares for cloud or on-premises deployments.
- **Azure Queues**: A messaging store for reliable messaging between application components.
- **Azure Disks**: Block-level storage volumes for Azure VMs.

Describe Azure Data migration options :

- **Azure migrate :** a service that helps you migrate from an on-premises environment to the cloud. Azure Migrate functions as a hub to help you manage the assessment and migration of your on-premises datacenter to Azure.
- **Azure Data Box :** is a physical migration service that helps transfer large amounts of data in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device that has a maximum usable storage capacity of 80 terabytes. The Data Box is transported to and from your datacenter via a regional carrier.
    - **Export data out from Azure ?**
        - Disaster recovery
        - Security requirements
        - Migrate back to on-premises or to another cloud service provider.
    - Export data to Azure ?
        - Onetime migration - when a large amount of on-premises data is moved to Azure.
        - Moving a media library from offline tapes into Azure to create an online media library.
        - Migrating your VM farm, SQL server, and applications to Azure.
        - Moving historical data to Azure for in-depth analysis and reporting using HDInsight.
        - Initial bulk transfer - when an initial bulk transfer is done using Data Box (seed) followed by incremental transfers over the network.
        - Periodic uploads - when large amount of data is generated periodically and needs to be moved to Azure.

Identify Azure file movement options :

Azure also has tools designed to help you move or interact with individual files or small file groups. Among those tools are AzCopy, Azure Storage Explorer, and Azure File Sync.

- **AzCopy :** a command-line utility to copy blobs or files to or from your storage account. You can upload files, download files, copy files between storage accounts, and even synchronize files. Can be configured to work with other cloud providers to help move files back and forth between clouds.
- **Azure Storage explorer :** Azure Storage Explorer is a standalone app that provides a graphical interface to manage files and blobs in your Azure Storage Account. It works on Windows, macOS, and Linux operating systems and uses AzCopy on the backend to perform all of the file and blob management tasks. With Storage Explorer, you can upload to Azure, download from Azure, or move between storage accounts.
- **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. It's almost like turning your Windows file server into a miniature content delivery

network. Once you install Azure File Sync on your local Windows server, it will automatically stay bi-directionally synced with your files in Azure.

Describe Azure Identity, Access, and Security

Describe Azure directory services

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

For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your organization. Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally. If you've worked with Active Directory, Azure AD will be familiar to you.

- Who uses Azure AD ?
    - It administrators
    - App developers (add SSO functionality to an app, or enabling an app to work with a user's existing credentials)
    - Users
    - Online service subscribers
- What does Azure AD do ?
    - Authentication
    - Single sign-on
    - Application management
    - Device management

Azure Active Directory Domain Services (Azure AD DS) : is a service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. You get the benefit of domain services without the need to deploy, manage and patch domain controllers (DCs) in the cloud.

- A managed domain is configured to perform a one-way synchronization from Azure AD to Azure AD DS. You can create resources directly in the managed domain, but they aren't syncrhonized back to Azure AD.

Describe Authentication methods

Azure supports multiple authentication methods, including standard passwords, single sign-on (SSO), multifactor authentication (MFA), and passwordless.

- **What is Single Sign-On (SSO) ?**
    - Enables a user to sign in one time and use that credential to access multiple resources applications from different providers.
    - You need to remember only one ID and one password. Access across applications is granted to a single identity that's tied to the user, which simplifies the security model.
- **What is Multifactor Authentication ? (MFA)**
    - Multifactor auth is the process of prompting a user for an extra form of identification during the sign-in process.
- Azure AD Multi-Factor Authentication : is a Microsoft service that provides multifactor authentication capabilities.
- **What is Passwordless authentication ?**
    - Features like MFA are great way to secure your organization. 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.
    - Passwordless authentication needs to be set up on a device before it can work. For example, your computer is something you have. Once it's been registered or enrolled, Azure now knows that it's associated with you. Now that the computer is known, once you provide something you know or are (such as a PIN or fingerprint), you can be authenticated without using a password.
    - 3 options :
        - Windows Hello for business : biometric and PIN credentials are directly tied to the user's PC.
        - Microsoft Authenticator App : use phone to become passwordless authentication method.
        - FIDO2 security Keys : FIDO (Fast Identity online) helps to promote open authentication standards and reduce the use of passwords as a form of authentication. FIDO2 is the latest standard that incorporates the web authentication standard. These FIDO2 security keys are typically USB devices, but could also use Bluetooth or NFC.

Describe Azure 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.

During sign-in, Conditional Access collects signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.

Describe Azure Rôle-based access control :

Azure allows to access control using Azure RBAC similar to rôle based in Oracle. Each rôle has an associated set of access permissions that relate to that rôle. Then you assign individuals or groups to one or more roles, and they receive all the associated access permissions.

Role-based access control is applied to a scope, which is a resource or set of resources that this access applies to.

- Scopes include :
    - Management group (a collection of multiple subscriptions)
    - A single subscription
    - A resource group
    - A single resource
- Azure RBAC is hierarchical, in that when you grant access at a parent scope, those permissions are inherited by all child scopes.
- Azure RBAC doesn't enforce access permissions at the application or data level. Application security must be handled by your application.

Describe Zero trust model :

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.

Based on these guiding principles :

- Verify explicitly – Always authenticate and authorize based on all available data points.
- Use least privilege access – limit user access with just-in-time and Just-enough-acces, data protection, risk-based adaptative policies.
- Assume breach – minimize blast radius and segment access.

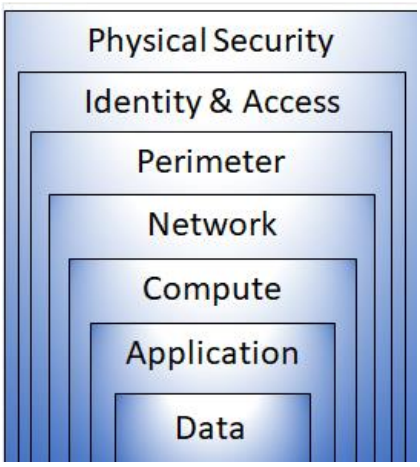
The Zero Trust model flips that scenario. Instead of assuming that a device is safe because it's within the corporate network, it requires everyone to authenticate. Then grants access based on authentication rather than location.

Protect assets anywhere with central policy.

Describe defense in-depth :

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 that aims at acquiring unauthorized access to data.



Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection. It slows down an attack and provides alert information that security teams can act upon, either automatically or manually.

Here's a brief overview of the role of each layer:

- The physical security layer is the first line of defense to protect computing hardware in the datacenter.
- The identity and access layer controls access to infrastructure and change control.
- The perimeter layer uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- The network layer limits communication between resources through segmentation and access controls.
- The compute layer secures access to virtual machines.
- The application layer helps ensure that applications are secure and free of security vulnerabilities.
- The data layer controls access to business and customer data that you need to protect.

Describe 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 to Azure.

We distinguish :

- Azure native protections
- Defend your hybrid resources
- Defend rsources running on other clouds

Defender for clouds fills 3 vital needs as you manage the security of your resources and workloads in the cloud and on-premises :

- **Continuously assess –** Know your security posture. Identify and track vulnerabilities
- **Secure –** harden resources and services with azure security benchmark
- **Defend –** detect and resolve threats to resources, workloads, and services.