**1)What is cloud computing?**

1. **Delivery of computing services over the internet.**
2. Delivery of storage services over the internet.
3. Delivery of websites accessible via the internet.

**2)Which cloud model uses some datacenters focused on providing cloud services to anyone that wants them, and some data centers that are focused on a single customer?**

1. Public cloud
2. **Hybrid cloud**
3. Multi-cloud

**3)According to the shared responsibility model, which cloud service type places the most responsibility on the customer?**

1. **Infrastructure as a Service (IaaS)**
2. Software as a Service (SaaS)
3. Platform as a Service (PaaS)

**4)Which type of scaling involves adding or removing resources (such as virtual machines or containers) to meet demand?**

1. Vertical scaling
2. **Horizontal scaling**
3. Direct scaling

**5)What is characterized as the ability of a system to recover from failures and continue to function?**

1. **Reliability**
2. Predictability
3. Scalability

**6)Which cloud service type is most suited to a lift and shift migration from an on-premises datacenter to a cloud deployment?**

1. **Infrastructure as a Service (IaaS)**
2. Platform as a Service (PaaS)
3. Software as a Service (SaaS)

**7)What type of cloud service type would a Finance and Expense tracking solution typically be in?**

1. Infrastructure as a Service (IaaS)
2. Platform as a Service (PaaS)
3. **Software as a Service (SaaS)**

**8)How many resource groups can a resource be in at the same time?**

1. **One**
2. Two
3. Three

**9)What happens to the resources within a resource group when an action or setting at the Resource Group level is applied?**

1. Current resources inherit the setting, but future resources don't.
2. Future resources inherit the setting, but current ones don't.
3. **The setting is applied to current and future resources.**

**10)What Azure feature replicates resources across regions that are at least 300 miles away from each other?**

1. **Region pairs**
2. Availability Zones
3. Sovereign regions

**11)Which Azure Virtual Machine feature staggers updates across VMs based on their update domain and fault domain?**

1. **Availability sets**
2. Scale sets
3. Update sets

**12)Which Azure service allows users to use a cloud hosted version of Windows from any location and connect from most modern browsers?**

1. **Azure Virtual Desktop**
2. Azure Virtual Machines
3. Azure Container Instances

**13)Which tool automatically keeps files between an on-premises Windows server and an Azure cloud environment updated?**

1. **Azure File Sync**
2. Azure Storage Explorer
3. AzCopy

**14)Which storage redundancy option provides the highest degree of durability, with 16 nines of durability?**

1. Locally redundant storage
2. Zone-redundant storage
3. **Geo-zone-redundant-storage**

**(Geo-redundant storage (GRS) and geo-zone-redundant storage (GZRS) both provide 16 nines of durability.)**

**15)Which Azure Storage service supports big data analytics, as well as handling text and binary data types?**

1. **Azure Blobs**
2. Azure Files
3. Azure Disks

**16)Which Microsoft Entra tool can vary the credentials needed to log in based on signals, such as where the user is located?**

1. **Conditional Access**

**(Conditional Access is a tool that Microsoft Entra ID uses to allow (or deny) access to resources based on identity signals. Conditional Access might challenge you for a second authentication factor if your sign-in signals are unusual or from an unexpected location.)**

1. Guest access
2. Passwordless

**17)Which security model assumes the worst-case security scenario, and protects resources accordingly?**

1. **Zero trust**
2. Defense-in-depth
3. Role-based access control

**18)A user is simultaneously assigned multiple roles that use role-based access control. What are their actual permissions? The role permissions are: Role 1 - read || Role 2 - write || Role 3 - read and write.**

1. Read only
2. Write only
3. **Read and write**

**19)The Cloud Adoption Framework for Azure helps customers make their journey to the cloud. What are the three main stages of the framework?**

1. Plan, Business Justification, and Implementation.
2. Migrate, Test, and Optimize.
3. **Plan, Ready, and Adopt.**

**20)Motivations for cloud adoption include migration and innovation triggers. Migration triggers include such things as cost saving and operations optimization. Which of the following is an example of an innovation trigger which drives cloud adoption?**

1. Reduction in IT staff for on-premises hardware.
2. **Transform products or services.**
3. Increase business agility.

**21)What are the five disciplines of cloud governance?**

1. Business risk, process, policy and compliance, resource consistency, and deployment acceleration.
2. Business risk, policy and compliance, security baseline, process, and operations.
3. **Cost management, security baseline, resource consistency, identity baseline, and deployment acceleration.**

**22)The common value drivers that business decision makers can use to justify moving their business to the cloud are Cost, Scale, Productivity, and Reliability. What is the specific value of scale in cloud computing?**

1. **Scale is the ability to deliver the right amount of IT resources.**
2. Scale eliminates capital expense.
3. Scale eases the burden of data backup, disaster recovery, and business continuity.

**23)Financial planning for cloud adoption requires organizations to decide whether to expand on-premises capabilities or move certain workloads and functions off-premises to cloud-delivered services. Microsoft has tools that can help. What Microsoft tool is available for a CFO who's trying to estimate the expected monthly bill and track actual account usage?**

1. The Azure Total Cost of Ownership (TCO) Calculator.
2. **The Azure Pricing Calculator.**
3. Microsoft Cost Management.

**24)What Azure feature can help stay organized and track usage based on metadata associated with resources?**

1. **Tags**
2. Tracers
3. Values

**25)What’s the best method to estimate the cost of migrating to the cloud while incurring minimal costs?**

1. Migrate a small sample to the cloud and track costs over time.
2. **Use the Total Cost of Ownership calculator to estimate expected costs**.
3. Migrate to the cloud, but track usage closely using tags to rapidly understand costs.

**26)How can you prevent creation of non-compliant resources, without having to manually evaluate each resource?**

1. **Azure Policy**
2. Azure Purview
3. Azure Resource Monitor

(**Incorrect. Azure Purview helps you manage your data estate, but won't prevent an out-of-policy resource creation.)**

**27)What's the best way to prevent inadvertent deletion of a resource?**

1. Azure Policy
2. Microsoft Purview
3. **Azure resource locks**

**(A resource lock can be used to prevent a resource from accidentally being deleted.)**

**28)What service helps you manage your Azure, on-premises, and multicloud environments?**

1. **Azure Arc**
2. Azure Policy
3. Azure Cloud Manager

**29)What two components could you use to implement a “infrastructure as code” deployment?**

1. **Bicep and ARM Templates**
2. Azure Policy and Azure Arc
3. Azure Monitor and Azure Arc

**30)Which is not one of the recommendation categories for Azure Advisor?**

1. Reliability
2. **Capacity**
3. Cost

**31)You receive an email notification that virtual machines (VMs) in an Azure region where you have VMs deployed is experiencing an outage. Which component of Azure Service Health will let you know if your application is impacted?**

1. Azure Status
2. Service Health
3. **Resource Health**

**(Correct. Resource Health is a tailored view of your actual Azure resources. It provides information about the health of your individual cloud resources.)**

**Some Important points to Remember**

1. IaaS places the most responsibility on the consumer.
2. SaaS places most of the responsibility with the cloud provider.
3. PaaS, being a middle ground between IaaS and SaaS.
4. a private cloud may be hosted from your on site datacenter. It may also be hosted in a dedicated datacenter offsite, potentially even by a third party that has dedicated that datacenter to your company. It is used by a single entity.
5. A public cloud is built, controlled, and maintained by a third-party cloud provider. With a public cloud, anyone that wants to purchase cloud services can access and use resources.
6. A hybrid cloud is a computing environment that uses both public and private clouds in an inter-connected environment. A hybrid cloud environment can be used to allow a private cloud to surge for increased, temporary demand by deploying public cloud resources. Hybrid cloud can be used to provide an extra layer of security.
7. Azure Arc is a set of technologies that helps manage your cloud environment.
8. There are two types of expenses to consider. Capital expenditure (CapEx) and operational expenditure (OpEx).
9. CapEx is typically a one-time, up-front expenditure to purchase or secure tangible resources. A new building, repaving the parking lot, building a datacenter, or buying a company vehicle are examples of CapEx.
10. OpEx is spending money on services or products over time. Renting a convention center, leasing a company vehicle, or signing up for cloud services are all examples of OpEx.
11. **Cloud computing falls under OpEx** because cloud computing operates on a consumption-based model. With cloud computing, you don’t pay for the physical infrastructure, the electricity, the security, or anything else associated with maintaining a datacenter. Instead, you pay for the IT resources you use.
12. To put it another way, cloud computing is a way to rent compute power and storage from someone else’s datacenter.
13. Vertical scaling is focused on increasing or decreasing the capabilities of resources.
14. Horizontal scaling is adding or subtracting the number of resources.
15. Reliability is the ability of a system to recover from failures and continue to function.
16. Predictability in the cloud lets you move forward with confidence.
17. Predictability can be focused on performance predictability or cost predictability.
18. Performance predictability focuses on predicting the resources needed to deliver a positive experience for your customers.
19. Cost predictability is focused on predicting or forecasting the cost of the cloud spend.
20. Management in the cloud speaks to how you’re able to manage your cloud environment and resources.
21. Infrastructure as a service (IaaS) is the most flexible category of cloud services, as it provides you the maximum amount of control for your cloud resources.
22. Platform as a service (PaaS) is a middle ground between renting space in a datacenter (infrastructure as a service) and paying for a complete and deployed solution (software as a service).
23. In a PaaS environment, the cloud provider maintains the physical infrastructure, physical security, and connection to the internet.
24. SaaS model may be the least flexible, it’s also the easiest to get up and running. It requires the least amount of technical knowledge or expertise to fully employ.
25. Software as a service (SaaS) is the most complete cloud service model from a product perspective.
26. Some services or virtual machine (VM) features are only available in certain regions, such as specific VM sizes or storage types.
27. There are also some global Azure services that don't require you to select a particular region, such as Microsoft Entra ID, Azure Traffic Manager, and Azure DNS.
28. Availability zones are 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.
29. An availability zone is set up to be an isolation boundary. If one zone goes down, the other continues working. **Availability zones are connected through high-speed, private fiber-optic networks.**
30. To ensure resiliency, a minimum of three separate availability zones are present in all availability zone-enabled regions.
31. You can use availability zones to run mission-critical applications and build high-availability into your application architecture by co-locating your compute, storage, networking, and data resources within an availability zone and replicating in other availability zones.
32. Availability zones are primarily for VMs, managed disks, load balancers, and SQL databases.
33. 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.

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

**35)** Most regions are paired in two directions, meaning they are the backup for the region that provides a backup for them (West US and East US back each other up).

**36)**  some regions, such as West India and Brazil South, are paired in only one direction. In a one-direction pairing, the Primary region does not provide backup for its secondary region.

**37)** 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.

**38)** The management infrastructure includes Azure resources and resource groups, subscriptions, and accounts.

**39)** 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.

**40)** a single resource can only be in one resource group at a time.

**41)** resource groups can't be nested, meaning you can’t put resource group B inside of resource group A.

**42)**  When you apply an action to a resource group, that action will apply to all the resources within the resource group. If you delete a resource group, all the resources will be deleted. If you grant or deny access to a resource group, you’ve granted or denied access to all the resources within the resource group.

**43)** In Azure, **subscriptions** are a unit of management, billing, and scale. subscriptions allow you to logically organize your resource groups and facilitate billing.

**44)** An Azure subscription links to an Azure account, which is an identity in Microsoft Entra ID or in a directory that Microsoft Entra ID trusts.

**45)** There are two types of subscription boundaries that you can use:

* **Billing boundary**: This subscription type determines how an Azure account is billed for using Azure. You can create multiple subscriptions for different types of billing requirements. Azure generates separate billing reports and invoices for each subscription so that you can organize and manage costs.
* **Access control boundary**: Azure applies access-management policies at the subscription level, and you can create separate subscriptions to reflect different organizational structures. An example is that within a business, you have different departments to which you apply distinct Azure subscription policies. This billing model allows you to manage and control access to the resources that users provision with specific subscriptions.

**46)** Resources are gathered into resource groups, and resource groups are gathered into subscriptions.

**47)** **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.

**48)**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.

**49)** 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.**

**50)** By moving multiple subscriptions under a management group, you can create one **Azure role-based access control (Azure RBAC)** assignment on the management group.

**51)** 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.

**Describe Azure compute and networking services**

1. VMs provide infrastructure as a service (IaaS) in the form of a virtualized server and can be used in many ways. you can group VMs together to provide high availability, scalability, and redundancy.
2. Scale sets allow you to centrally manage, configure, and update a large number of VMs in minutes.
3. Virtual machine scale sets also automatically deploy a load balancer to make sure that your resources are being used efficiently. With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.
4. **Virtual machine availability sets** are another tool to help you build a more resilient, highly available environment.
5. 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.
6. Availability sets do this by grouping VMs in two ways: **update domain** and **fault domain**.
7. **Update domain**: The update domain groups VMs that **can be rebooted** at the same time. This allows you to apply updates while knowing that only one update domain grouping will be offline at a time. All of the machines in one update domain will be updated. An update group going through the update process is given a **30-minute** time to recover before maintenance on the next update domain starts.
8. **Fault domain**: The fault domain groups your VMs by common power source and network switch. By default, an availability set will split your VMs across up to **three fault domains**. This helps protect against a physical power or networking failure by having VMs in different fault domains .
9. **Azure Virtual Desktop** is 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. Azure Virtual Desktop works across devices and operating systems, and works with apps that you can use to access remote desktops or most modern browsers.
10. Azure Virtual Desktop provides centralized security management for users' desktops with Microsoft Entra ID.
11. **With Azure Virtual Desktop**, the data and apps are separated from the local hardware. The actual desktop and apps are running in the cloud, meaning the risk of confidential data being left on a personal device is reduced. Additionally, user sessions are isolated in both single and multi-session environments.
12. Azure Virtual Desktop lets you use Windows 10 or Windows 11 Enterprise multi-session.
13. If you want to run multiple instances of an application on a single host machine, **containers** are an excellent choice.
14. **Containers** are a virtualization environment. Much like running multiple virtual machines on a single physical host**, you can run multiple containers on a single physical or virtual host**. Unlike virtual machines, you don't manage the operating system for a container.
15. Containers are **lightweight** and designed to be created, scaled out, and **stopped dynamically**.
16. Containers are designed to allow you to respond to changes on demand. With containers, you can quickly restart if there's a crash or hardware interruption.
17. One of the most popular container engines is **Docker**, and Azure supports Docker.
18. **Azure Container Instances** offer the fastest and simplest way to run a container in Azure; without having to manage any virtual machines or adopt any additional services.
19. **Azure Container Instances** are a **platform as a service (PaaS)** offering. Azure Container Instances allow you to upload your containers and then the service will run the containers for you.
20. **Azure Container Apps** are similar in many ways to a container instance. They allow you to get up and running right away, **they remove the container management piece, and they're a PaaS offering.**
21. Container Apps have extra benefits such as the **ability to incorporate load balancing** and **scaling**.
22. **Azure Kubernetes Service (AKS)** is a container **orchestration service.** An orchestration service manages the **lifecycle of containers**. When you're deploying a fleet of containers, AKS can make fleet management simpler and more efficient.
23. **Azure Functions** is an **event-driven, serverless** compute option that doesn’t require maintaining virtual machines or containers.
24. 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.
25. Functions scale automatically **based on demand**, so they may be a good choice **when demand is variable**.
26. Functions can be either **stateless** or **stateful**. When they're **stateless (the default),** they behave as if they're restarted every time they respond to an event. When they're **stateful (called Durable Functions)**, a context is passed through the function to track prior activity.
27. Functions are a **key component** of **serverless computing**. They're also a general compute platform for running any type of code.
28. If you need to host your application on Azure, you might initially turn to a **virtual machine (VM)** or **containers**. Both VMs and containers provide excellent hosting solutions.
29. **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.
30. **Containers**, with the ability to **isolate and individually manage** different aspects of the hosting solution, can also be a **robust** and **compelling** option.
31. **Azure 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.
32. **Azure App Service** lets you focus on **building and maintaining** your app, and Azure focuses on keeping the environment up and running.
33. **Azure App Service** is an **HTTP-based** service for hosting web applications, REST APIs, and mobile back ends.
34. It supports multiple languages, including .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. It also supports both Windows and Linux environments.
35. App Service handles most of **the infrastructure decisions** you deal with in hosting web-accessible apps.
36. App Service includes full support for hosting **web apps** by using **ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, or Python**. You can choose either **Windows or Linux** as the host operating system.
37. **WebJobs** are often used to run background tasks as part of your application logic. They can be scheduled or run by a trigger.
38. **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.
39. Azure virtual networking supports both **public** and **private** endpoints to enable communication between external or internal resources with other internal resources.
40. **Public endpoints** have a **public IP address** and can be accessed from anywhere in the world.
41. **Private endpoints** exist within a virtual network and have a **private IP address** from within the address space of that virtual network.
42. When you set up a virtual network, you define a **private IP address space** by using either public or private IP address ranges.
43. The IP range only exists within the virtual network and isn't internet routable.
44. **Virtual networks** can connect not only VMs but other Azure resources, such as the App Service Environment for Power Apps, Azure Kubernetes Service, and Azure virtual machine scale sets.
45. Service endpoints can connect to other Azure resource types, such as Azure SQL databases and storage accounts. This approach enables you to link multiple Azure resources to virtual networks to improve security and provide optimal routing between resources.
46. **Azure virtual networks** enable you to link resources together in your on-premises environment and within your Azure subscription.
47. **Point-to-site** virtual private network connections are from a computer outside your organization back into your corporate network. In this case, the client computer initiates an **encrypted VPN** connection to connect to the Azure virtual network.
48. **Site-to-site** virtual private networks link your **on-premises VPN device or gateway to the Azure VPN gateway** in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet.
49. **Azure ExpressRoute** provides a 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.
50. **Route tables** allow you to define rules about how traffic should be directed.
51. **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.
52. **Network security groups** are Azure resources that can contain multiple inbound and outbound security rules.
53. You can link virtual networks together by using **virtual network peering.**
54. **Peering** allows two virtual networks to connect directly to each other.
55. **Network traffic** between peered networks is **private,** and travels on the Microsoft backbone network, never entering the public internet. Peering enables resources in each virtual network to communicate with each other. These virtual networks can be in separate regions, which allows you to create a **global interconnected network** through Azure.
56. **User-defined routes (UDR)** allow you to control the routing tables between subnets within a virtual network or between virtual networks. This allows for greater control over network traffic flow.
57. **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).
58. Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks. VPNs can enable networks to **safely and securely** share sensitive information.

* **A VPN gateway** is a type of virtual network gateway. Azure VPN Gateway instances are deployed in a **dedicated subnet** of the virtual network and enable the following connectivity: Connect **on-premises datacenters** to virtual networks through a **site-to-site connection**.
* Connect **individual devices** to **virtual networks** through a **point-to-site connection.**
* Connect **virtual networks** to **other virtual networks** through a **network-to-network connection.**

1. All data transfer is encrypted inside a **private tunnel** as it crosses the internet.
2. When setting up a **VPN gateway**, you must specify the type of VPN - either **policy-based or route-based**.
3. **Policy-based VPN gateways** specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP addresses to choose the tunnel where that packet is going to be sent through.
4. **In Route-based gateways**, 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. **Route-based VPNs** are the preferred connection method for **on-premises devices**. They're more resilient to topology changes such as the creation of new subnets.
5. **VPN gateways** and **ExpressRoute gateways** can be deployed in a **zone-redundant configuration**. These gateways require different gateway **stock keeping units (SKUs)** and use Standard public IP addresses instead of Basic public IP addresses.
6. **Azure ExpressRoute** lets you extend your on-premises networks into the Microsoft cloud over a private connection, with the help of a connectivity provider.
7. With **ExpressRoute**, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.
8. ExpressRoute uses the **BGP**. **BGP** is used to exchange routes between on-premises networks and resources running in Azure. This protocol enables **dynamic routing** between your on-premises network and services running in the Microsoft cloud.
9. Each connectivity provider uses **redundant devices** to ensure that connections established with Microsoft are highly available.

* **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**

1. **Co-location** refers to your datacenter, office, or other facility being physically co-located at a cloud exchange, such as an ISP.
2. **Point-to-point ethernet connection** refers to using a point-to-point connection to connect your facility to the Microsoft cloud.
3. With **any-to-any connectivity**, you can integrate your **wide area network (WAN)** with Azure by providing connections to your offices and datacenters.
4. With **ExpressRoute**, your data doesn't travel over the **public internet**, so it's not exposed to the potential risks associated with internet communications. **ExpressRoute is a private connection** from your on-premises infrastructure to your Azure infrastructure.
5. **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.
6. **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.
7. **Azure role-based access control (Azure RBAC)** is used to control who has access to specific actions for your organization.
8. **Azure DNS also supports private DNS domains**. This feature allows you to use your own custom domain names in your private virtual networks, rather than being stuck with the Azure-provided names.
9. Azure DNS also supports **alias record sets**.

# Describe Azure storage Service

# 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.

1. **Locally redundant storage (LRS)**
2. **Geo-redundant storage (GRS)**
3. **Read-access geo-redundant storage (RA-GRS)**
4. **Zone-redundant storage (ZRS)**
5. **Geo-zone-redundant storage (GZRS)**
6. **Read-access geo-zone-redundant storage (RA-GZRS)**

# Azure Storage always stores multiple copies of your data so that it's protected from planned and unplanned events such as transient hardware failures, network or power outages, and natural disasters. Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.

# Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region, locally redundant storage (LRS) and zone-redundant storage (ZRS).

# Locally redundant storage (LRS) replicates your data three times within a single data center in the primary region. LRS provides at least 11 nines of durability (99.999999999%) of objects over a given year.

# LRS is the lowest-cost redundancy option and offers the least durability compared to other options. LRS protects your data against server rack and drive failures. However, if a disaster such as fire or flooding occurs within the data center, all replicas of a storage account using LRS may be lost or unrecoverable. To mitigate this risk, Microsoft recommends using zone-redundant storage (ZRS), geo-redundant storage (GRS), or geo-zone-redundant storage (GZRS).

# zone-redundant storage (ZRS) replicates your Azure Storage data synchronously across three Azure availability zones in the primary region. ZRS offers durability for Azure Storage data objects of at least 12 nines (99.9999999999%) over a given year.

# With ZRS, your data is still accessible for both read and write operations even if a zone becomes unavailable.

# 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.

# When you create a storage account, you select the primary region for the account. The paired secondary region is based on Azure Region Pairs, and can't be changed.

# By default, data in the secondary region isn't available for read or write access unless there's a failover to the secondary region. If the primary region becomes unavailable, you can choose to fail over to the secondary region. After the failover has completed, the secondary region becomes the primary region, and you can again read and write data.

# Azure Storage offers two options for copying your data to a secondary region: geo-redundant storage (GRS) and geo-zone-redundant storage (GZRS). GRS is similar to running LRS in two regions, and GZRS is similar to running ZRS in the primary region and LRS in the secondary region.

# GRS (Geo Redundant Storage) 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. GRS offers durability for Azure Storage data objects of at least 16 nines (99.99999999999999%) over a given year.

# GZRS(Geo-Zone -Reduntant Storage) combines the high availability provided by redundancy across availability zones with protection from regional outages provided by geo-replication. Data in a GZRS storage account is copied across three Azure availability zones in the primary region (similar to ZRS) and is also replicated to a secondary geographic region, using LRS, for protection from regional disasters. Microsoft recommends using GZRS for applications requiring maximum consistency, durability, and availability, excellent performance, and resilience for disaster recovery.

# Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages.

# Remember that the data in your secondary region may not be up-to-date due to RPO.

1. **Azure Blobs**: A massively scalable object store for **text and binary data**. Also includes support for **big data analytics through Data Lake Storage Gen2**.
2. **Azure Files**: Managed file shares for cloud or on-premises deployments.
3. **Azure Queues**: A messaging store for reliable messaging between application components.
4. **Azure Disks**: Block-level storage volumes for Azure VMs.
5. **Azure Tables:** NoSQL table option for structured, non-relational data.

# Objects in blob storage can be accessed from anywhere in the world via HTTP or HTTPS. Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library. The storage client libraries are available for multiple languages, including .NET, Java, Node.js, Python, PHP, and Ruby.

**Azure Storage offers different access tiers for your blob storage**, helping you store object data in the most cost-effective manner. The available access tiers include:

1. **Hot access tier**: Optimized for storing data that is accessed frequently (for example, images for your website).
2. **Cool access tier**: Optimized for data that is infrequently accessed and stored for at least 30 days (for example, invoices for your customers).
3. **Cold access tier**: Optimized for storing data that is infrequently accessed and stored for at least 90 days.
4. **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).
5. **Hot and cool** access tiers can be set at the **account level**.
6. **The cold and archive** access tiers aren't available at the **account level**.
7. **Hot, cool, cold, and archive** tiers can be set at the **blob leve**l, during or after upload.
8. Data in the **cool and cold access** tiers **can tolerate slightly lower availability**, but still requires **high durability, retrieval latency, and throughput characteristics** similar to hot data.
9. For **cool and cold data**, a lower availability **service-level agreement (SLA)** and higher access costs compared to hot data are acceptable trade-offs for lower storage costs.
10. **Archive storage stores** data offline and offers the lowest storage costs, but also the highest costs to rehydrate and access data.

# Azure File storage 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 Queue storage is a service for storing large numbers of messages. Once stored, you can access the messages from anywhere in the world via authenticated calls using HTTP or HTTPS.

# A queue can contain as many messages as your storage account has room for (potentially millions). Each individual message can be up to 64 KB in size. Queues are commonly used to create a backlog of work to process asynchronously.

# Azure Disk storage, or Azure managed disks, are block-level storage volumes managed by Azure for use with Azure VMs.

# Azure Table storage stores large amounts of structured data. Azure tables are a NoSQL datastore that authenticated accepts calls from inside and outside the Azure cloud. This enables you to use Azure tables to build your hybrid or multi-cloud solution and have your data always available. Azure tables are ideal for storing structured, non-relational data.

**Azure Migrate is 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. It provides the following:

* **Unified migration platform**: A single portal to start, run, and track your migration to Azure.
* **Range of tools**: A range of tools for assessment and migration. Azure Migrate tools include Azure Migrate: Discovery and assessment and Azure Migrate: Server Migration. Azure Migrate also integrates with other Azure services and tools, and with independent software vendor (ISV) offerings.
* **Assessment and migration**: In the Azure Migrate hub, you can assess and migrate your on-premises infrastructure to Azure.

1. **Azure Data Box** is a physical migration service that helps transfer **large amounts of data in a quick, inexpensive, and reliable way.**Data Box storage device that has a maximum usable storage capacity **of 80 terabytes.**
2. Data Box is ideally suited to **transfer data sizes larger than 40 TBs** in scenarios with no to limited network connectivity.
3. **AzCopy** is a **command-line utility** that you can use to copy **blobs or files to or from your storage account**. With AzCopy, you can upload files, download files, copy files between storage accounts, and even synchronize files. AzCopy can even be configured to work with other cloud providers to help move files back and forth between clouds.
4. Synchronizing blobs or files with AzCopy is one-direction synchronization. When you synchronize, you designated the source and destination, and AzCopy will copy files or blobs in that direction. It doesn't synchronize bi-directionally based on timestamps or other metadata.
5. **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.
6. **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,& Security**

1. **Microsoft Entra ID** is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop. Microsoft Entra ID can also help you maintain your **on-premises Active Directory deployment**.
2. **Microsoft Entra ID** is **Microsoft's cloud-based identity** and **access management service**. With Microsoft Entra ID, you control the identity accounts, but Microsoft ensures that the service is available globally.
3. **Single sign-on (SSO)** enables you to remember only one username and one password to access multiple applications.
4. You can manage your cloud and on-premises apps by using Microsoft Entra ID.
5. One method of connecting **Microsoft Entra ID** with your **on-premises AD** is using **Microsoft Entra Connect**.
6. **Microsoft Entra Connect** synchronizes user identities between on-premises Active Directory and Microsoft Entra ID. Microsoft Entra Connect synchronizes changes between both identity systems, so you can use features like **SSO, multifactor authentication, and self-service password reset** under both systems.
7. **Microsoft Entra Domain Services** is a service that provides managed domain services such as domain join, group policy, **lightweight directory access protocol (LDAP)**, and **Kerberos/NTLM authentication**.
8. **Microsoft Entra Domain Services** integrates with your existing **Microsoft Entra tenant**. This integration lets users sign into services and applications connected to the managed domain using their existing credentials.
9. **A managed domain** is configured to perform a **one-way synchronization** from **Microsoft Entra ID** to **Microsoft Entra Domain Services**.
10. **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.
11. **Single sign-on** is only as secure as the initial authenticator because the subsequent connections are all based on the security of the initial authenticator.
12. **Multifactor authentication** is the process of prompting a user for an extra form (or factor) of identification during the sign-in process. MFA helps protect against a password compromise in situations where the password was compromised but the second factor wasn't.
13. **Multifactor authentication** provides additional security for your identities by requiring two or more elements to fully authenticate.
14. **Microsoft Entra multifactor authentication** is a Microsoft service that provides **multifactor authentication** capabilities**. Microsoft Entra multifactor authentication** enables users to choose an additional form of authentication during sign-in, such as a **phone call or mobile app notification**.
15. **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.
16. **Passwordless authentication** needs to be set up on a device before it can work.

* **Microsoft global Azure** and **Azure Government** offer the following three passwordless authentication options that integrate with Microsoft Entra ID: **Windows Hello for Business**
* **Microsoft Authenticator app**
* **FIDO2 security keys**

1. **Windows Hello for Business** is ideal for information workers that have their own designated Windows PC. The biometric and PIN credentials are directly tied to the user's PC, which prevents access from anyone other than the owner.
2. **The Authenticator App** turns any **iOS or Android phone** into a strong, passwordless credential. Users can sign-in to any platform or browser by getting a notification to their phone, matching a number displayed on the screen to the one on their phone, and then using their biometric (touch or face) or PIN to confirm.
3. **The FIDO (Fast IDentity Online)** Alliance 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 (WebAuthn)** standard.
4. **FIDO2 security keys** are an **unphishable** standards-based passwordless authentication method that can come in any form factor. **Fast Identity Online (FIDO)** is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign-in to their resources without a username or password by using an external security key or a platform key built into a device.
5. **Microsoft Entra External ID** refers to all the ways you can securely interact with users outside of your organization.
6. **Business to business (B2B) collaboration** - Collaborate with external users by letting them use their preferred identity to sign-in to your Microsoft applications or other enterprise applications (SaaS apps, custom-developed apps, etc.). B2B collaboration users are represented in your directory, typically as guest users.
7. **B2B direct connect** - Establish a mutual, **two-way trust** with another Microsoft Entra organization for seamless collaboration. B2B direct connect currently supports Teams shared channels, enabling external users to access your resources from within their home instances of Teams. B2B direct connect users aren't represented in your directory, but they're visible from within the Teams shared channel and can be monitored in Teams admin center reports.
8. **Microsoft Azure Active Directory business to customer (B2C)** - Publish modern SaaS apps or custom-developed apps (excluding Microsoft apps) to consumers and customers, while using Azure AD B2C for identity and access management.
9. **Conditional Access** is a tool that Microsoft Entra ID 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.
10. **Role-based access control** is applied to a scope, which is a resource or set of resources that this access applies to.
11. **Azure RBAC** is enforced on any action that's initiated against an Azure resource that passes through Azure Resource Manager. **Resource Manager** is a management service that provides a way to organize and secure your cloud resources.
12. **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.
13. 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.
14. 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.

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

1. **The physical security layer** is the **first line of defense** to protect **computing hardware** in the datacenter.
2. **The identity and access layer** controls access to infrastructure and change control.
3. **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.
4. **The network layer** limits communication between resources through segmentation and access controls.
5. **The compute layer** secures access to virtual machines.
6. **The application layer** helps ensure that applications are secure and free of security vulnerabilities.
7. **The data layer** controls access to business and customer data that you need to protect.
8. **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.
9. **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.
10. Defender for Cloud can also protect resources in other clouds (such as AWS and GCP).

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

1. **Continuously assess** – Know your security posture. Identify and track vulnerabilities.
2. **Secure** – Harden resources and services with Azure Security Benchmark.
3. **Defend** – Detect and resolve threats to resources, workloads, and services.
4. When Defender for Cloud detects a threat in any area of your environment, it generates a security alert.
5. **Defender for cloud** provides advanced threat protection features for many of your deployed resources, including **virtual machines, SQL databases, containers, web applications, and your network**. Protections include securing the management ports of your VMs with just-in-time access, and adaptive application controls to create allowlists for what apps should and shouldn't run on your machines.

[**Describe cost management in Azure**](https://learn.microsoft.com/en-us/training/modules/describe-cost-management-azure/)

1. **Azure Marketplace** lets you purchase Azure-based solutions and services from third-party vendors. This could be a server with software preinstalled and configured, or managed network firewall appliances, or connectors to third-party backup services.
2. When you purchase products through **Azure Marketplace**, you may pay for not only the Azure services that you’re using, but also the services or expertise of the third-party vendor. **Billing structures are set by the vendor**.
3. **The pricing calculator** and the **total cost of ownership (TCO) calculator** are two calculators that help you understand potential Azure expenses. Both calculators are accessible from the internet, and both calculators allow you to build out a configuration.
4. **The pricing calculator** is designed to give you an estimated cost for provisioning resources in Azure. You can get an estimate for individual resources, build out a solution, or use an example scenario to see an estimate of the Azure spend. The pricing calculator’s focus is on the cost of provisioned resources in Azure.
5. **The Pricing calculator** is for information purposes only. The prices are only an estimate. Nothing is provisioned when you add resources to the pricing calculator, and **you won't be charged** for any services you select.
6. **The TCO calculator** is designed to help you compare the costs for **running an on-premises infrastructure** compared to an **Azure Cloud infrastructure**. With the TCO calculator, you enter your current infrastructure configuration, including servers, databases, storage, and outbound network traffic. The TCO calculator then compares the anticipated costs for your current environment with an Azure environment supporting the same infrastructure requirements.

**To migrate to Azure, you might:**

1. **Use Azure Virtual Machines instances**, similar to the virtual machines used in your datacenter.
2. **Use Azure Application Gateway** for load balancing.
3. **Use Azure SQL Database** to hold inventory and pricing information.
4. The virtual machines and the database run all the time (**730 hours per month**).
5. The network processes about **1 TB of data per month.**
6. The database doesn't need to be configured for **high-performance workloads** and requires no more than **32 GB** of storage.
7. **Cost Management** provides the ability to quickly check Azure resource costs, create alerts based on resource spend, and create budgets that can be used to automate management of resources.
8. **Cost analysis** is a subset of **Cost Management** that provides a quick visual for your Azure costs. Using cost analysis, you can quickly view the total cost in a variety of different ways, including by billing cycle, region, resource, and so on.
9. **Cost alerts** provide a single location to quickly check on all of the different alert types that may show up in the Cost Management service.

**The three types of alerts that may show up are:**

1. **Budget alerts**
2. **Credit alerts**
3. **Department spending quota alerts.**
4. **Budget alerts** notify you when spending, based on usage or cost, reaches or exceeds the amount defined in the alert condition of the budget. Budget alerts support both **cost-based** and **usage-based** budgets. Budget alerts are generated automatically whenever the budget alert conditions are met.
5. **Credit alerts** notify you when your Azure credit monetary commitments are consumed. **Monetary commitments** are for organizations with Enterprise Agreements (EAs). Credit alerts are generated automatically at 90% and at 100% of your Azure credit balance. Whenever an alert is generated, it's reflected in cost alerts, and in the email sent to the account owners.
6. **Department spending quota alerts** notify you when department spending reaches a **fixed threshold of the quota**. Spending quotas are configured in the EA portal. Whenever a threshold is met, it generates an email to department owners, and appears in cost alerts.
7. **A budget** is where you set a spending limit for Azure. You can set budgets based on a subscription, resource group, service type, or other criteria. **When you set a budget, you will also set a budget alert**. When the budget hits the budget alert level, it will trigger a budget alert that shows up in the cost alerts area.
8. A **more advanced use of budgets** enables **budget conditions to trigger automation** that suspends or otherwise modifies resources once the trigger condition has occurred.
9. **Tags allow you to associate metadata with a resource to help keep track of resource management, costs and optimization, security, and so on.**
10. **Microsoft Purview** is a family of data governance, risk, and compliance solutions that helps you get a **single, unified** view into your data. Microsoft Purview brings insights about your on-premises, multicloud, and **software-as-a-service** data together.
11. **Microsoft 365** features as a core component of the **Microsoft Purview** risk and compliance solutions. **Microsoft Teams, OneDrive, and Exchange** are just some of the **Microsoft 365** services that Microsoft Purview uses to help manage and monitor your data.
12. **Azure Policy** enables you to define both **individual policies** and **groups of related policies**, known as **initiatives**. Azure Policy evaluates your resources and highlights resources that aren't compliant with the policies you've created. Azure Policy can also prevent **noncompliant resources from being created**.
13. **Azure Policies** are inherited, so if you set a policy at a high level, it will automatically be applied to all of the groupings that fall within the parent.

**Under this initiative, the following policy definitions are included:**

1. **Monitor unencrypted SQL Database in Security Center** This policy monitors for unencrypted SQL databases and servers.
2. **Monitor OS vulnerabilities in Security Center** This policy monitors servers that don't satisfy the configured OS vulnerability baseline.
3. **Monitor missing Endpoint Protection in Security Center** This policy monitors for servers that don't have an installed endpoint protection agent.
4. **A resource lock** prevents resources from being accidentally deleted or changed.
5. **Resource locks are inherited**, meaning that if you place a resource lock on a resource group, all of the resources within the resource group will also have the resource lock applied.
6. There are **two types** of resource locks, **one that prevents users from deleting** and **one that prevents users from changing or deleting** a resource.
7. You can manage resource locks from **the Azure portal, PowerShell, the Azure CLI, or from an Azure Resource Manager template**.
8. **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.**

**The Service Trust Portal features and content are accessible from the main menu. The categories on the main menu are:**

1. **Service Trust Portal** provides a quick access hyperlink to return to the Service Trust Portal home page.
2. **My Library** lets you save (or pin) documents to quickly access them on your My Library page. You can also set up to receive notifications when documents in your My Library are updated.
3. **All Documents** is a single landing place for documents on the service trust portal. From **All Documents**, you can pin documents to have them show up in your **My Library**.
4. Service Trust Portal reports and documents are available to download for at least 12 months after publishing or until a new version of document becomes available.
5. **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.
6. **The Azure portal** updates continuously and requires no downtime for maintenance activities.
7. **Azure Cloud Shell** is a browser-based shell tool that allows you **to create, configure, and manage Azure resources** using a shell. Azure Cloud Shell support both **Azure PowerShell** and the **Azure Command Line Interface (CLI),** which is a **Bash shell.**
8. It is a **browser-based shell** experience, with no local installation or configuration required.
9. **Azure PowerShell** is a shell with which developers, DevOps, and IT professionals can run commands called **command-lets (cmdlets**). These commands call the Azure REST API to perform management tasks in Azure. **Cmdlets can be run independently** to handle one-off changes, or they may be combined to help orchestrate complex actions.
10. **The Azure CLI** is functionally equivalent to **Azure PowerShell**, with the primary difference being the syntax of commands. While **Azure PowerShell** uses **PowerShell commands**, the **Azure CLI** uses **Bash commands**.
11. In utilizing **Azure Resource Manager (ARM),** **Arc** lets you extend your Azure compliance and monitoring to your **hybrid and multi-cloud configurations**. **Azure Arc** simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.
12. **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. Anytime you do anything with your Azure resources, ARM is involved.
13. **Infrastructure as code** is a concept where you manage your infrastructure as lines of code.
14. By using **ARM templates**, you can **describe the resources** you want to use in a declarative JSON format. With an ARM template, the deployment code is verified before any code is run. This ensures that the resources will be created and connected correctly.
15. **Bicep** is a language that uses declarative syntax to **deploy Azure resources**. A Bicep file defines the infrastructure and configuration.
16. While similar to an **ARM template,** which is written in **JSON**, Bicep files tend to use a simpler, more concise style.
17. **Azure Advisor** evaluates your **Azure resources** and makes recommendations to help improve reliability, security, and performance, achieve operational excellence, and reduce costs. **Azure Advisor** is designed to help you save time on cloud optimization. The recommendation service includes suggested actions you can take right away, postpone, or dismiss.
18. **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.
19. **On the left** is a list of the sources of logging and metric data that can be collected at every layer in your application architecture, from application to operating system and network.
20. **In the center**, the logging and metric data are stored in central repositories.
21. **On the right**, the data is used in several ways. You can view real-time and historical performance across each layer of your architecture or aggregated and detailed information. The data is displayed at different levels for different audiences. You can view high-level reports on the Azure Monitor Dashboard or create custom views by using Power BI and Kusto queries.
22. **Azure Log Analytics** is the tool in the Azure portal where you’ll write and run log queries on the data gathered by Azure Monitor.
23. **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.