1.1. Describe Cloud Computing

Basic/Major cloud services

1. Compute power (how much processing a computer can do)
2. Storage

Shared responsibility model

Sets how to moderate the services among server and consumers
On-premises: consumer is responsible for everything
Laas: most responsibility on the consumer
Paas: middle ground
Saas: most responsibility on the cloud provider

Cloud Models

Private: full control of org, expensive, private
Public: vice versa
Hybrid: flexible
Multi Cloud: deal with two or more public cloud providers
Azure arc: set of technologies that help manage cloud environments.
Azure vmware solution: if migration from private to public happens

IT infrastructure models

1. Capital Expenditure (CapEx)
2. Operational Exp (OpEx)

CapEx: one time, up front expenditure
OpEx: over time (azure too is consumption based model)

1.2. Benefits of using cloud services

Availability and scalability (Higher consideration)

1. Uptime(availability) - SLAs
2. Ability to handle demands(scalability) - horizontal (plus minus the no of resources) and vertical scaling (plus minus the capababilities of resources)

Reliability and predictability

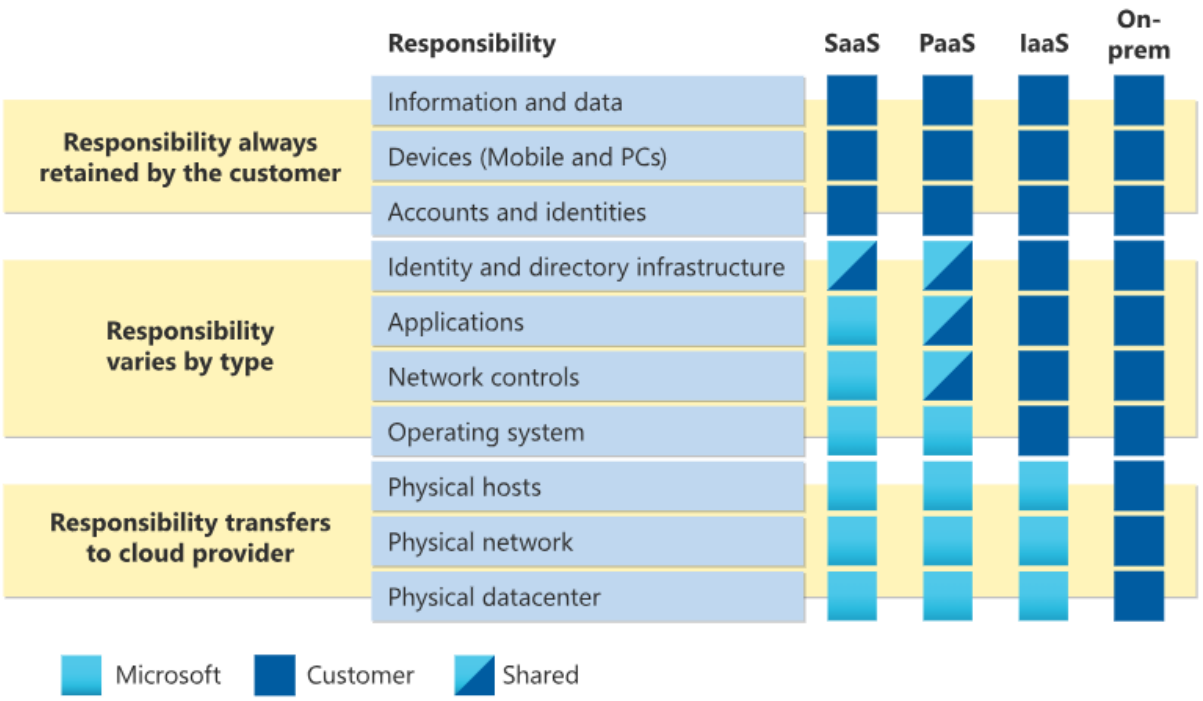
Reliability: ability to recover from failures
Predictability: performance(predicting resources for positive results like autoscaling, load balancing, high availability) & cost

Security, governance and management

IaaS: relatively maximum security
Management:

1. Of the cloud (scale more resources, preconfigured templates, auto replace failing resources, automatic alerts)
2. In the cloud (through web portal, apis, cli, powershell)

1.3. Cloud services types



IaaS: lift and shift migration, testing and development
PaaS: development framework, analytics and business intelligence
SaaS: email and messaging, business productivity applications, finance and expense tracking.

Core architectural components

1. Physical infrastructure
2. Management infrastructure

Physical infrastructure
Data Centers and they are grouped into regions or availability zone

Region
Geographical area that contains at least one but potentially multiple data centres.

Availability zones
Physically separate data centres within the azure region.
Azure services that support availability zones fall into three categories:

1. Zonal services
2. Zone redundant services
3. Non-regional service

Regular Regions + Sovereign Regions (instance of azure that are isolated from the main instance of azure)

Sequence from inc to dec
Geography

Region pair
Azure region
Availability zone

Management infrastructure
Includes resources, groups, subscriptions, and accounts

Resource group
Collection of resources in one group
Resources can be moved from one to another. But at a time it can be at one place. All operations performed on a single resource will be applied to other resources as well in a resource group.

Azure subscription
Azure account
- Test subscription
- Dev subscription
- Production subscription

In multi-subscription account, subscription boundaries are:
Billing boundary
Access control boundary

2.0. Azure architecture and services

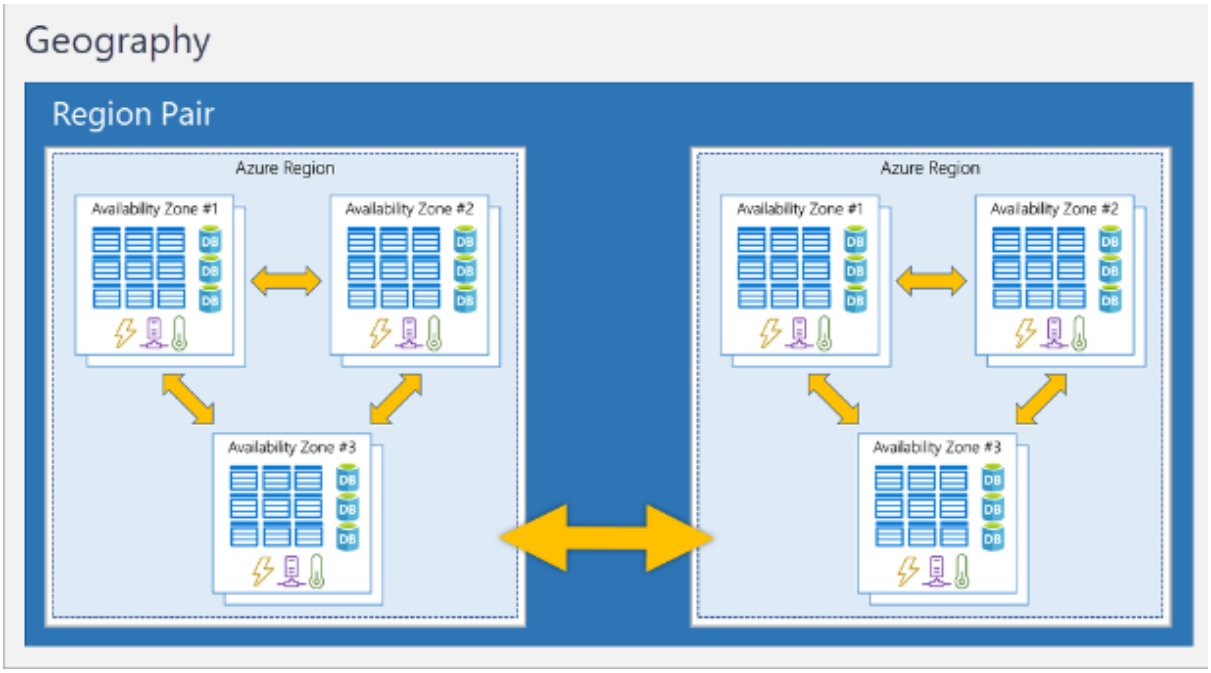
2.1. Describe core architectural components of Azure

Azure account
- Subscription
- —- Resource groups
- –------ Resources

Physical infrastructure
It starts with datacenters. Data Centers are grouped into regions or availability zones

Regions

Availability zones
Availability zones are physically separate data centres within an Azure region. Availability zones are primarily for VMs, managed disks, load balancers, and SQL databases.
Azure services that support availability zones fall into three categories:
Zonal service, Zone-redundant services, Non-regional services



A resource is the basic building block of Azure. Virtual Machines (VMs), virtual networks, databases, cognitive services, etc. are all considered resources within Azure.

Resource groups
They provide a convenient way to group resources together.

Azure subscriptions
There are two types of subscription boundaries that you can use:

1. Billing boundary
2. Access control boundary

Azure management groups
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.
Resources are gathered into resource groups, and resource groups are gathered into subscriptions. And Azure management group is something above subscriptions.

By moving multiple subscriptions under a management group, you can create one Azure role-based access control (Azure RBAC)

Hierarchy from top to bottom

1. Directory
2. Management groups
3. Subscriptions
4. Resource groups
5. Resources

2.2. Describe Azure compute and networking services

- VMs provide infrastructure as a service (IaaS)
- VMs are an ideal choice when you need:
    - Total control over the operating system (OS).
    - The ability to run custom software.
    - To use custom hosting configurations.

Another type of virtual machine is the **Azure Virtual Desktop**. Azure Virtual Desktop is a desktop and application virtualization service that runs on the cloud.

Containers
VM is limited to a single operating system per virtual machine. To run multiple instances of an application on a single host machine, containers are an excellent choice. One of the most popular container engines is *Docker*, which is supported by Azure.

Difference between VM and container:
VM virtualizes the hardware and performs well when we need complete control while containers virtualize the operating system and perform well when we need portability performance.

Azure Container Instances
Azure Container Instances are a *platform as a service (PaaS)* offering. Azure Container Instances offer the fastest and simplest way to run a container in Azure; without having to manage any VM or adopt any additional services.

Describe Azure Functions
Azure Functions is a serverless compute option that doesn't require maintaining VM or containers. Elsewise in order for your app to function, these resources have to be running.

Serverless computing in Azure
Serverless computing means the responsibility of managing servers is already handled for us. Benefits includes
No infrastructure management
Scalability
Only pay for what you use

Azure Functions are a key component of serverless computing. 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.

Application hosting options
Azure App Service
App Service enables you to build and host web apps without managing infrastructure. Azure App Service is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends. It supports languages including .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. It also supports both Windows and Linux environments.

Types of app services
With App Service, you can host most common app service styles like:
- Web apps
- API apps
- WebJobs
- Mobile apps

Azure virtual private network
Only deploy one VPN gateway in each virtual network.
- Policy based VPN
- Route based VPN
  Point to site connection
  Connections btw virtual networks
  Multisite connections
  Coexistence with an azure expressroute gateway

High availability scenarios
- Active/standby
- Active/active

- ExpressRoute failover
- Zone redundant gateways

Storage account
A storage account provides a unique namespace for your Azure Storage data that's accessible from anywhere in the world over HTTP or HTTPS.

redundancy options
Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.

- Locally redundant storage (LRS)
- Geo-redundant storage (GRS)
- Read-access geo-redundant storage (RA-GRS)
- Zone-redundant storage (ZRS)
- Geo-zone-redundant storage (GZRS)
- Read-access geo-zone-redundant storage (RA-GZRS)

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.

Redundancy in the primary region

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

Locally redundant storage (LRS)

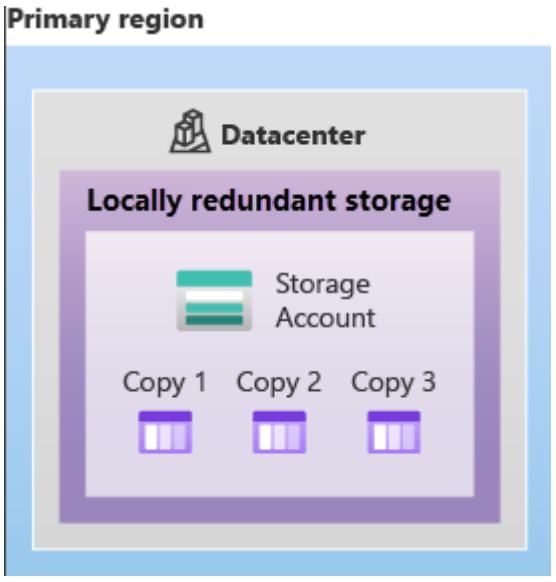
- LRS is the lowest-cost redundancy option.
- For locally redundant storage

- 9 nines
- Offers the least durability compared to other options.
- LRS protects your data against server rack and drive failures.
- 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).

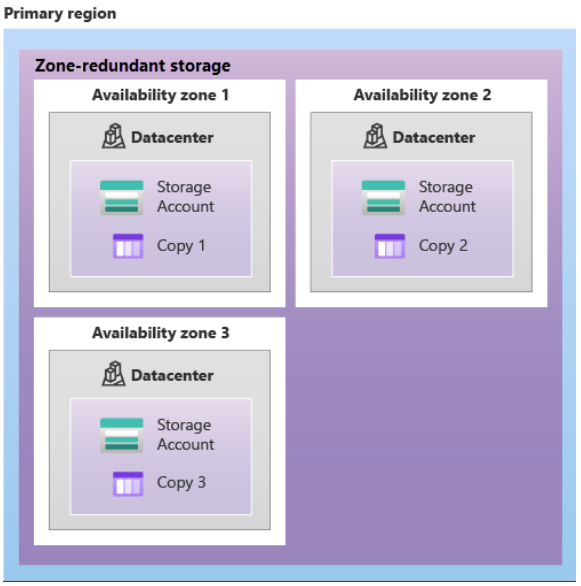
For better understanding:

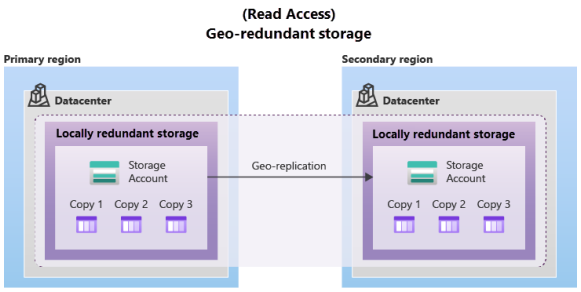
- https://learn.microsoft.com/en-us/training/modules/describe-azure-storage-services/3-redundancy

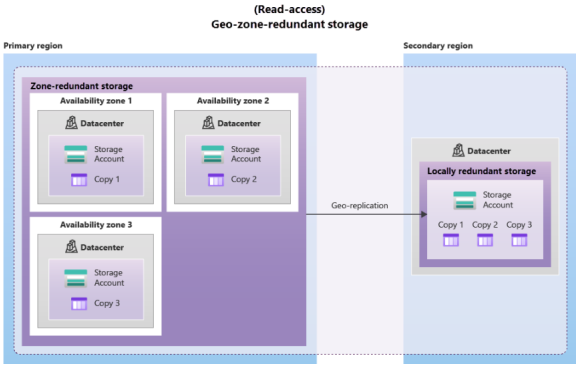
LRS - PRIMARY REGION



ZRS - PRIMARY REGION







Passwordless authentication?

- Windows Hello for Business
- Microsoft Authenticator app
- FIDO2 security keys

Fast Identity Online (FIDO) is an open standard for passwordless authentication.

Conditional Access is a tool that Azure Active Directory uses to allow (or deny) access to resources based on identity signals.

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.