Azure Storage Accounts

- Provide storage facility on the cloud

Blob → Store objects, images and videos.

Table → Store table data

Queue → Store data in queue form: used for sending and receiving messages.

File → Used for creating file shares.

⇒ Types of storage account

1⇒ Standard General purpose V2

This is standard storage for file, queue, table and blob.

2⇒ Premium block blobs :- Specific for blocks and append blobs.

This is used when you want fast access to your blobs, high transaction rates.

3⇒ Premium Page blobs: Supported for page blobs.

This is used when you want fast blob access, high transaction to your VM disk storage

Teacher's Signature .....

Enroll
Page No:
Date: / /

4 → Premium file share.

This is supported for file shares. This is when you want fast access to your files, high transaction rates.

⇒ Creating an Azure storage account

Storage Account → Create → Select properties

Subscription
Resource Group
Disk Name
Performance

Performance ⇒ Standard: General purpose V2
Premium: Used for low latency.

- Block Blob
- Page Blob
- File share.

Teacher's Signature .....

⇒ Blob Storage :- it is optimized for storing large amount of unstructured data.
You store blob objects in container.
You will get a unique URL to access storage services.

1⇒ Block blob :- Made up of blocks of data that can be managed individually.

2⇒ Append blob :- These are block blobs that are optimized for append operation - Good for logging.

3⇒ Page blob :- This is used for virtual hard drive files for Azure Virtual Machines.

⇒ Uploading a Blob

Go to your instance of Storage account → Containers
Go to Containers ← Create Containers
→ Upload (Using Azure portal)

⇒ Sharing blob data with other

Go to file under Storage Account → Container
← Select File ← Select Container
- Under Overview, you can find the URL OR
- You can generate SAS and share it with others.

Teacher's Signature .....

Enroll
Page No:
Date: / /

* While uploading a blob file, using advance configuration, you can:
  - Change Authentication type
  - Change Blob type
  - Change block size
  - Change Access Tier
  - Create a folder
  - Create key-value pair for files
  - Change Retention policy.

* When you will share the URL of blob stored data, if someone tries to access it anonymously (not provided access), he will get Resource not found.

⇒ Methods to authorize someone of storage data shared using URL

1⇒ Providing access to anyone having URL, allowing anonymous access as well.
Select the object from Storage Account
Change access level to public
- Blob :- Read access for blob only
- Container :- Read access for container & blob.

2⇒ Access keys :- Sharing at storage account level

Go to Storage Account → Access keys → Here
you can share Access key or Connection strings to provide access

Teacher's Signature .....

Why 2 Access key :- If any of your key got compromised you can switch your application to 2nd key early and regenerate compromised key. This way your application won't get compromised.

3⇒ Shared Access Signature :- Sharing at blob level.

Go to Storage Account → Data Storage level → Object/table → Generate SAS

You can also control permission on file using SAS method.

* If you want to provide access for short time, you can best use SAS method.
You can also filter allowed IP using SAS.

* Shared Access Signature can also be configured at account level ⇒ Storage Account → Shared Access Signature

Storage Account

To store Files — As backend of VM

By default, V.M runs on managed ~~virtual Machine~~ storage.

Search Storage → Add

* Its Good practice to put your storage location according to your user or application location

* GPV2 is most used storage type.

Replication ↴

LRS:- 3 Copy of data in same datacenter but different harddisk

GRS:- 6 Copy of data in 2 different datacenter.

RA-GRS:- Read access to different datacenter & Write access to different datacenter.

- Subscription & Resource Group
- Name (Basis of URL)
- Location (Different location have different Cost)
- Performance
- Account type
- Replication
- Access tier
- Networking Connectivity
- Advance

Create

Teacher's Signature .....

Enroll
Page No:
Date: / /

* By default, when you create a storage account that is accessible from anywhere, using some credentials, To secure this either put your storage behind public endpoint (Selected Network) or private endpoint. They you can access this storage account only from same virtual network where your storage exist.

⊛ Blob soft delete :- Blob soft delete can be enable, if you want some retention period for your deleted data. (Chargable)

⊛ Before deleting storage account, disable the blob soft delete.

⇒ Storage Account → Properties

In properties of any storage account, you will find primary and secondary endpoints.

To access storage account you can use these endpoints, if primary endpoint is down, you can use secondary endpoints.

⇒ Storage Account → Access keys.

Access keys will be used to access your storage account from URL.

You can also regenerate your access key if you think your key got compromised.

⊛ Switch over to 2nd key before invalidating first.

:- Sharing Access to storage account.

It's not prescribed to share key with anyone, even if you want to share access to storage, better share it with tokens.

Teacher's Signature .....

⇒ Shared Access Signature

Storage Account → Shared access signature

Shared access signature is a token signed by one of your keys to share access to your storage account.

Benefits :-
- You aren't directly sharing your keys; keys are safe.
- You can control / restrict complete access & provide a part of it
- You can decide what you want to share and for how long period.
- You can filter IP address as well.
- You can generate SAS for file level as well.

* 4 types of data :-

i) Blob ⇒ Container Storage
ii) File Share
iii) Tables
iv) Queue

i) Container Storage :-

Storage Account → Storage → Containers → Add

or Interacting

⇒ Uploading Your data to Storage Account

a) To do it programmatically ⇒ Rest API

b) To do it manually

i) Download and install Azure Storage Explorer according to your O.S, and You can use it to interact with your Azure storage.

ii) Using Azure Portal :-

Storage Account → Storage Explorer

⇒ Changing configuration of pre-existing storage account

Storage Account → Select Storage → Configuration

Make Required Change → Save

Teacher's Signature .....

⇒ RBAC Authentication for storage

Storage Account → Select Storage → Access Control (IAM) → Add → Role Assignment

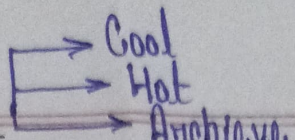
RBAC is very useful when you want any user to have limited access according to his role

(*) AzCopy :- Microsoft Software to copy files from 1 storage to, other or within different directory of any storage

Why to use:- When you want to copy some data from Storage Account 1 to Storage Account 2; You will have to download to your system then upload to other Storage Account, which will incur huge charge.
So, its better to do Server Side Copy using AzCopy.

Command Syntax:- AzCopy /Source: SourcePath /Dest: Destination path /Pattern: Pattern/Name of File Name
/SourceKey: Key for Source Storage
/DestKey: Key for Destination Storage.

(*) For production ⇒ Better to use premium.



⇒ Access Tier

How much you will be charged for storage & how much you will be charged for accessing data.

Cool ⇒ Cost for storage is low but cost of accessing is high. * Min Charging period = 30 days

Hot ⇒ Cost of storage ↑, Cost of accessing ↓

Changing Access Tier of pre-existed storage

Storage ⟶ Select Storage ⟶ Configuration.

(*) To change any configuration of existing resource, you can switch to configuration tab of that resource.
You can also change tiers for file level as well.

Archieve ⇒ Used to store data backups.
- Storage cost is very low, but retrival time is high
- If you want your data to retrieve fast, use high priority rehydrate. (For small object)
- Min charging period ⇒ 180 days.

(*)(*) There are two types of cost associated with storage:
1) Storage Charge
2) Read-Write operation (Access) Charge.

Teacher's Signature .....

⇒ Litecycle Management for Blob Storage

When you want files to automatically moved to low tier after a specific time period, to save overall cost.

Eg:- After 30 days of last modification ⇒ Move data to Cool storage
After 180 days of last modification ⇒ Move data to Archieve Storage
After 365 days ⇒ Delete Storage data

Storage Account → Select Storage → Litecycle Management
↓
Create Rule.