AZ 104 – Training

**STORAGE ACCOUNT**

Data Lake Storage Gen2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workloads and enables file-level access control lists (ACLs). Learn more

* Blob Storage
  + Network File Storage (NFS) to mount drives to VMs
  + Access Tier: Hot and Cold
* Azure Files
  + File shares
* Tables and Queues
  + ???
* Container
  + ???

* Storage Access Key and Access Key
  + ???

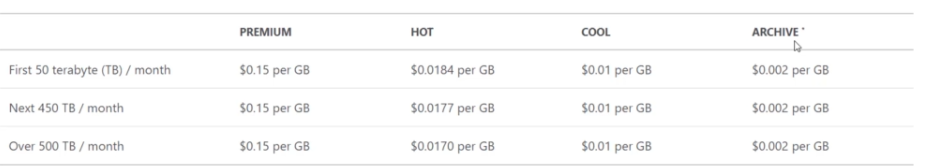
* Storage Explorer

* Log Analytics

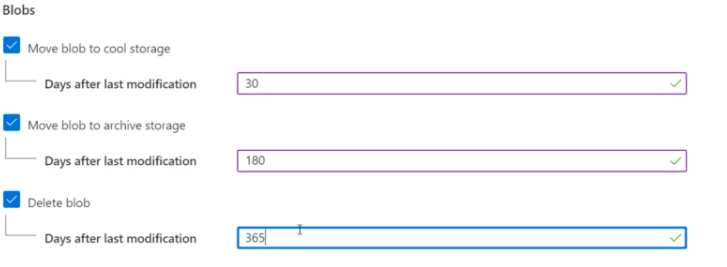
**COPY FILES WITH AzCopy**

* You can run it like ".\AzCopy "Source URL" "Destination URL"
* Can copy between azure subscription and storage accounts

**ACCESS TIERS (Storage accounts)**

* You will be charge by access and storage.
* Premium Tier, it has to be selected at the moment of the storage account creation.
  + It has better performance, it is ten times faster that standard for retrieving data.
* Hot Tier (Default option)
  + You will be charge the standard for access and storage.
* Cool Tier
  + You will be charge half for storage BUT double for access, read, write, view.
* Archive Tier
  + 99 More cheaper to store files that Hot tier, but more expensive to read, write and view, usually for backups
  + It can take several hours to retrieve the data depending on the priority of the rehydration.
* You can change your access tier, at your storage account level or even file level.
* 

**LIFECYCLE MANAGEMENT (Storage accounts)**

* Example: You want files to be in hot storage for the first 30 days and then you move them to cool storage
* Policies/Rules to move storage between access tiers, defining the time and access tiers.
* 

**AZURE AD ACCESS CONTROL FOR STORAGE (Storage accounts)**

* Grant permissions to storage resource to active domain users.
* Storage Account > Access Control (IAM) > Check access >
* Storage Account Contributor to read and write but not to delete

**OBJECT REPLICATION (Storage accounts)**

* Copying data to a different storage account and even to a different region.
* Destination container is read only, this is done by Azure itself.
* You can also create filters.
* Blobchangefeed it indicates the changes done in the storage account

**IMPORT AND EXPORT DATA TO AZURE (Storage accounts)**

**Moving Large Files**

* Import/Export
* Export
  + You can export all or just some selected containers and blobs
  + The ship actual HDD to YOU!!
* Import
  + They will send us an empty HDD to upload the DATA!!!
  + Journals…
* Sending the HDD is called Azure Data Box
* Data Box is 100 TB
* Data Box Disk is 8 TB
* Data Box Heavy is 1 PB!!

**Blob Storage**

* Storage Account > Performance > Premium
  + Block blobs: best for high transactions rates or low storage latency
  + Files Shares: best for enterprise or high-performance applications that need to scale
  + Page blobs: best for random and write operations
* Only the standard storage account has Geo redundant storage.
* LRS Locally redundant storage, basic protection against server rack and drive failures.
* ZRS Zone redundant storage, protection against datacenter-level failures
* GRS Geo redundant storage, failover capabilities in a secondary region.

**CDN – Content delivery network**

* tbd

**CONFIGURE AZURE FILES**

**Create Azure file share**

* You can select a quota limit of usage
* You can mount it to a PC

**Azure File Sync**

* Synchronize files from local servers into cloud, like a replication service for share files
* You need to download an Azure File Sync Agent
* It is also an object in azure, it is a storage sync service.
* Sync group to select what files are going to be sync between your services.

**Troubleshoot Azure File Sync**

* Need to investigate MS KB.

**IMPLEMENT BACKUP AND RECOVERY**

**Azure Backup**

* Location is important because it must be in the same region as our backup resources.
* It has to applications, Backups and Site Recovery.
* It also works with On-Premises resources using a backup service software.
* Backup for VMs, Azure File Share or SQL server VM.
* You create backup policies, with name with a schedule.

**File Recovery from a VM Backup**

* Go to VM > Backup > File Recovery
  + You can download an executable script that will mount the disks from an specific recovery point.
  + Once you have the file you will unmount.

**On-Premises Backup**

* You will need the recovery services agent installed in your on-prem machine.

**Backup Reports**

* Tbd

**Soft Delete for VM Backups**

* 14 days to delete backup data
* Can be un-deleted
* 15th day – auto delete

**Azure Site Recovery / ASR to Site-to-Site**

* It will make a copy and will have it ready to deploy to another region (They are sitting and synchronized in case something happens to start the failover)