Storage

Wednesday, November 24, 2021

12:01 AM

* Storage account:

Type of storage account u create services can be used:

Blob

Tables

Queue

Files

* Blob:

Files are referred/ stored as objects

* Different authorization tech:

Shared access signature

Access keys

AAD

* Storage explorer:

Free tool to explore SA, cosmos DB

* SA --> Settings --> Access Keys

This storage account can be added to storage explorer using these keys

* SAS can be generated at SA/blob level to provide unique signature which allows access. It uses underlying keys, time can be defined for its validity. SAS which is generated at blob level can be viewed from browser. But the one which is generated at storage account cannot be viewed browser but can be added to storage explorer.
* Stored access policy can be used along with SAS which gives more control on the access via SAS. Can include time, permission. This is only for container (Blob service)
* While generating SAS to container it can be linked to existing policy
* Authorize using AD:
  + Create a user from AAD tab
  + SA --> IAM --> + Add
* Auth using AD is most secured way. There might be scenario where AD approach can't be implemented due to security policies, then use SAS access keys better be last option

LRS: 3 copies in diff storage device

ZRS: for data center failures. Copies are made in diff data centers/ zones

GRS: Data is replicated to diff region as LRS in primary, secondary region. Can access to secondary region only when primary region is down

RAGRS: can access secondary region at the same time

Geo- Zone - Redundant: primary is using ZRS. Secondary is using LRS

Read Access Geo Zone redundant:

Access Tiers: Hot(default), Cool(cost is less), Archive(cost is even less)

Hot - for frequently

Cool - for infrequently used data and is at least stored for 30 days

Archive - for data that is rarely used and stored for at least 180 days.

Hot and cool are enabled at storage account level. Archive is enabled at blob level

Can be changed from SA --> config

Setting a blob to archive makes it inaccessible, it had to be rehydrated to hot or cool which takes several hours based on priority std/high

LRS - ZRS --> Manual migration/ Live migration

If there are any archive blobs it has to be changed in order to change replication type

Prem performances:

Uses SSD

Life cycle management rules: based on specific condition blob's access tier can be changed/deleted

Object replication: rules define, asynchr copy

Blob:

Files are stored as object within the service. Every file or object that is stored gets unique URL to access individually. These cannot be mapped as drive

If files need to be shared across machines **file share** need to be used.

File Share:

Gives the link used to connect from windows, linux, mac

File share Backup:

Can be done by:

Snapshot - snapshot for file share can be taken and restored at any point in time. This is manual way.

Recovery services - create a recovery services vault in same region and link storage account. While deleting recovery services vault unregister the storage account

Backup --> Add Azure storage and schedule

Backup Items --> u can see the jobs (Bckup now and restore file share to same/ alternate location)

Service Endpoints:

Service Endpoints can be created for SQL data bases, Azure storage accounts to access within Vnet

Establishes a public secure connection

Azure private endpoint:

It is a network interface that is provisioned in the vnet and enables secure private connections to services

Azure File Sync:

Azure file share is used to access files over servers/VMs on SMB.

File sync is used to keep data in sync fast and efficient to the machines so that people accessing the data from the machine will not even know that it from Azure

Deploy a VM and install file sync agent

Deploy File sync in same region as storage account and add sync group -->SA. This sync group gonna a create a cloud end point which is storage account where the data is stored and accessed from.

DATA TRANSFER

WAImportExport

AzCOpy

AzureDataBox

AzureDAtaFActory

Stored access policy

Service end points, azure private end points