

# AZURE CLOUD COMPUTING

## MINOR PROJECT-1

**Name:** Madhushree N

**Mentor / Trainer:** Arib

**Batch:** December

**Project Description:**

Create an azure storage account using the azure portal and create a BLOB storage(Hot tier) inside a container.

Upload one image as well as a short video and set different access permissions (private and public). ENABLE ACCESS TRACKING and add a rule in the lifecycle management policies telling that

i. if the page blob which we created is not accessed for 10 days then change its access tier to cool.

ii. If the blob is not modified for 45 days, delete the blob.

Requires screen recording to be enabled for task submission and write a 1 page report mentioning the steps to do this task.

**LINK TO THE MINOR PROJECT VIDEO FILE:**

[https://drive.google.com/file/d/173yC\\_5KGYCOpy3aGBeVCHReijRwgdqr\\_/view?usp=sharing](https://drive.google.com/file/d/173yC_5KGYCOpy3aGBeVCHReijRwgdqr_/view?usp=sharing)

## **INTRODUCTION:**

**Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose.**

Azure Storage lifecycle management offers a rule-based policy that you can use to transition blob data to the appropriate access tiers or to expire data at the end of the data lifecycle. A lifecycle policy acts on a base blob, and optionally on the blob's versions or snapshots. For more information about lifecycle management policies, see [Optimize costs by automatically managing the data lifecycle](#).

A lifecycle management policy is comprised of one or more rules that define a set of actions to take based on a condition being met. For a base blob, you can choose to check one of two conditions:

- The number of days since the blob was last modified.
- The number of days since the blob was last accessed. To use this condition in an action, you must first optionally enable access time tracking.

**When the selected condition is true, then the management policy performs the specified action. For example, if you have defined an action to move a blob from the hot tier to the cool tier if it has not been modified for 30 days, then the lifecycle management policy will move the blob 30 days after the last write operation to that blob.**

For a blob snapshot or version, the condition that is checked is the number of days since the snapshot or version was created.

## Steps of creating a blob storage account using Azure Storage Accounts (without any rules under Lifecycle Management) :

- Open Azure portal.
- Select Storage Accounts under Azure services.
- Click on Create.
- Enter the project details.
- Enter the subscription type in which the storage account is created. In my case Azure for students is used.
- Select the resource group for creation of storage account. A new resource group can be created by selecting create new.
- Under instance details fill in the name of the storage account that is required to be created.
- Rest all is given by default. The storage account by default gets created in the hot tier itself.
- Under networking three options are provided namely **public endpoint (all networks)**, **public endpoint (selected networks)**, **private endpoint**. Anyone out of the three can be selected. **I have selected public endpoint (all networks) for my storage account.**
- Click on review and create. The required storage account gets created once the validation is passed.

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal, specifically the 'Basics' tab. The interface includes a top navigation bar with the Microsoft Azure logo, a search bar, and user information. The main content area has a breadcrumb trail 'Home > Storage accounts >' and a title 'Create a storage account'. Below the title are tabs for 'Basics', 'Advanced', 'Networking', 'Data protection', 'Encryption', 'Tags', and 'Review + create'. A note states: 'If you need to create a legacy storage account type, please click [here](#).' The form fields are as follows: 'Storage account name' with the value 'minorprojectdc'; 'Region' with a dropdown menu showing '(US) East US'; 'Performance' with two radio button options, 'Standard: Recommended for most scenarios (general-purpose v2 account)' being selected, and 'Premium: Recommended for scenarios that require low latency.'; 'Redundancy' with a dropdown menu showing 'Geo-redundant storage (GRS)'; and a checked checkbox for 'Make read access to data available in the event of regional unavailability.' At the bottom, there are three buttons: 'Review + create' (highlighted in blue), '< Previous', and 'Next : Advanced >'.

Microsoft Azure Search resources, services, and docs (G+)

Home > Storage accounts >

### Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review + create

If you need to create a legacy storage account type, please click [here](#).

Storage account name

Region

Performance ☒ Standard: Recommended for most scenarios (general-purpose v2 account)  
☐ Premium: Recommended for scenarios that require low latency.

Redundancy

☒ Make read access to data available in the event of regional unavailability.

[Review + create](#) [< Previous](#) [Next : Advanced >](#)

The screenshot shows the 'Create a storage account' page in the Microsoft Azure portal. The 'Networking' tab is selected. Under 'Network connectivity', there is a message: 'You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.' Below this, the 'Connectivity method' section has three radio button options: 'Public endpoint (all networks)' (selected), 'Public endpoint (selected networks)', and 'Private endpoint'. A blue information icon is followed by the text: 'All networks will be able to access this storage account. We recommend using Private endpoint for accessing this resource privately from your network. [Learn more](#)'. At the bottom, there are three buttons: 'Review + create' (blue), '< Previous', and 'Next : Data protection >'.

This screenshot shows the 'Create a storage account' page in the Microsoft Azure portal, specifically the 'Networking' tab. It includes the same information as the previous screenshot. Below the connectivity options, the 'Network routing' section is visible. It contains the text: 'Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.' The 'Routing preference' section has two radio button options: 'Microsoft network routing' (selected) and 'Internet routing'. At the bottom, the same three buttons are present: 'Review + create' (blue), '< Previous', and 'Next : Data protection >'.

### Optionally enabling access tracking:

- Navigate to the data management in the resource of the storage account created. Under it select the Lifecycle management.
- Go to the list view. Enable the access tracking by checking the checkbox. Then navigate to ADD to add rules and filters.
- Select Limit blobs with filters in the details, which creates an extra option of the Filter set.
- Add the number of days and the rules to be initiated in the Base Blobs.
- In the filter set give a valid blob prefix and click on add.
- The lifecycle management policy will be updated.

Microsoft Azure Search resources, services, and docs (G+)

Home > projectminor >

## Update a rule

Details **Base blobs** Filter set

Lifecycle management uses your rules to automatically move blobs to cooler tiers or to delete them. If you create multiple rules, the associated actions must be implemented in tier order (from hot to cool storage, then archive, then deletion).

If Base blobs haven't been modified in 10 days

Then Move to cool storage

If Base blobs haven't been modified in 45 days

Then Delete the blob

+ Add conditions

Update Previous Next

Microsoft Azure Search resources, services, and docs (G+)

Home > projectminor >

## projectminor | Lifecycle management

Storage account

Search (Ctrl+/) + Add a rule ✓ Enable ☐ Disable Refresh Delete

Lifecycle management offers a rich, rule-based policy for general purpose v2 and blob storage accounts. Use the policy to transition your data to the appropriate access tiers or expire at the end of the data's lifecycle. A new or updated policy may take up to 48 hours to complete. [Learn more](#)

List View Code View

Enable access tracking ☒

| Name              | Status  | Blob type |
|-------------------|---------|-----------|
| move-to-cool-tier | Enabled | Block     |

Overview  
Activity log  
Tags  
Diagnose and solve problems  
Access Control (IAM)  
Data migration  
Events  
Storage browser (preview)

Data storage  
Containers  
File shares  
Queues  
Tables

### Code View:

```
{  
  "rules": [  
    {  
      "enabled": true,  
      "name": "move-to-cool-tier",  
      "type": "Lifecycle",  
      "definition": {  
        "actions": {
```

```
"baseBlob": {
  "tierToCool": {
    "daysAfterModificationGreaterThan": 10
  },
  "delete": {
    "daysAfterModificationGreaterThan": 45
  }
},
"filters": {
  "blobTypes": [
    "blockBlob"
  ],
  "prefixMatch": [
    "mycontainer/project"
  ]
}
}
```