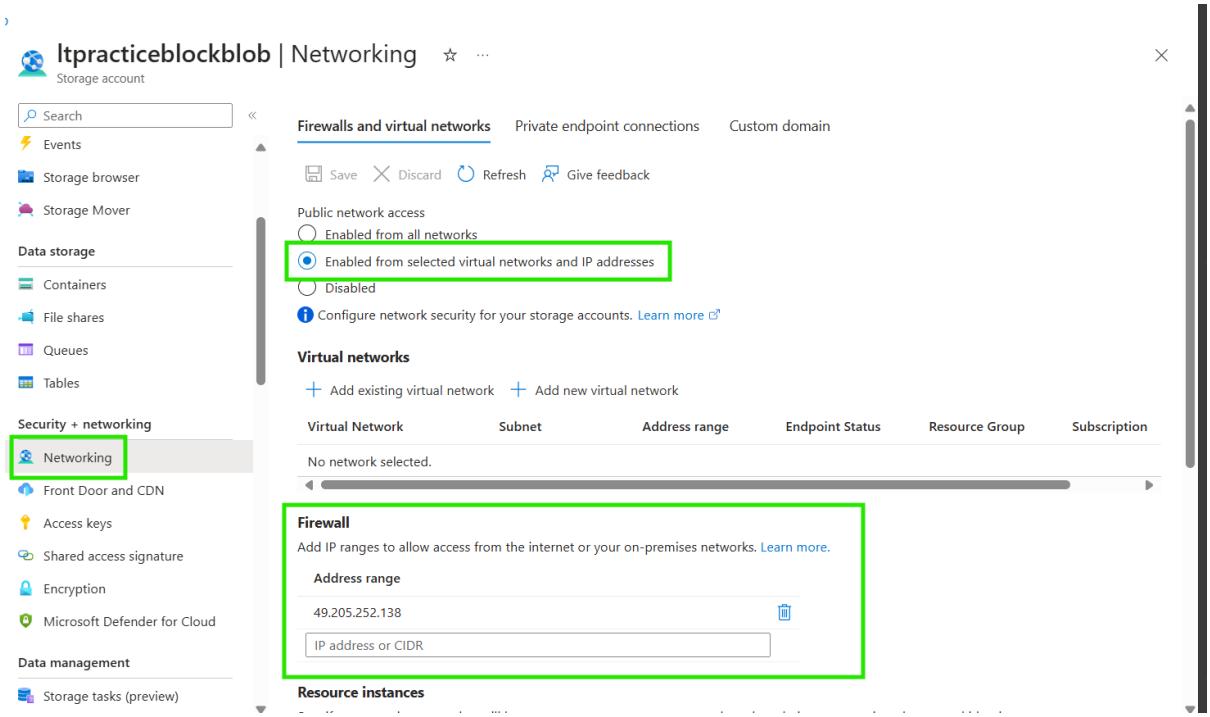
Azure Storage Account

- Tiers:
  - Standard:
    - offers lowest cost per gb and is backed by HDDs
  - Premium:
    - Offers low latency performance & is backed by SSD
- Storage Account Type
  - General purpose Storage:
    - This is of tier standard
    - Redundancy options:
      - LRS
      - ZRS
      - GRS
      - GZRS
  - Block Blob Storage
    - Redundancy options:
      - LRS
      - ZRS
  - File Storage
    - Redundancy options:
      - LRS
      - ZRS
  - Page Blob storage
    - Redundancy options:
      - LRS
      - ZRS

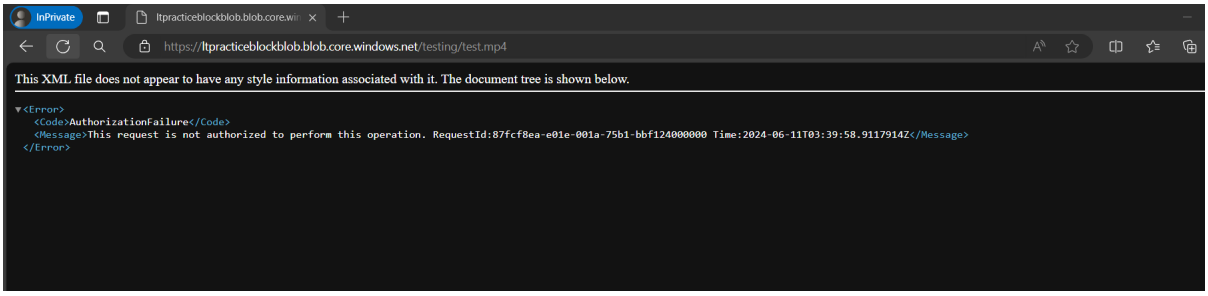
Storage Account Endpoints

- The name for storage account has to be unique across all accounts in Azure.
- sample blob endpoint `https://ltpracticeblockblob.blob.core.windows.net/testing/test.mp4`
- Securing the endpoints:

- We can make only selected virtual networks and ip address access the endpoints



- For all other than selected ip addresses and virtual networks when we access data we get authorization failure

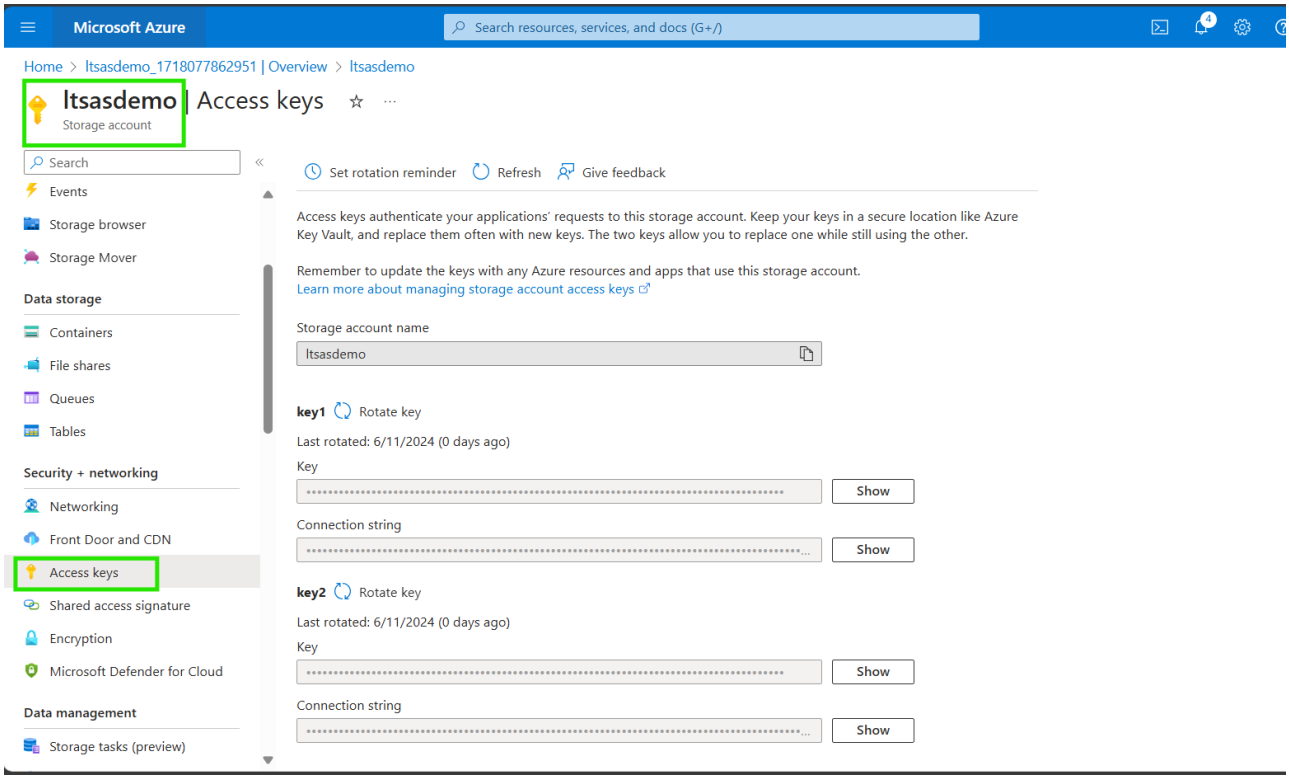


Azure Storage Security

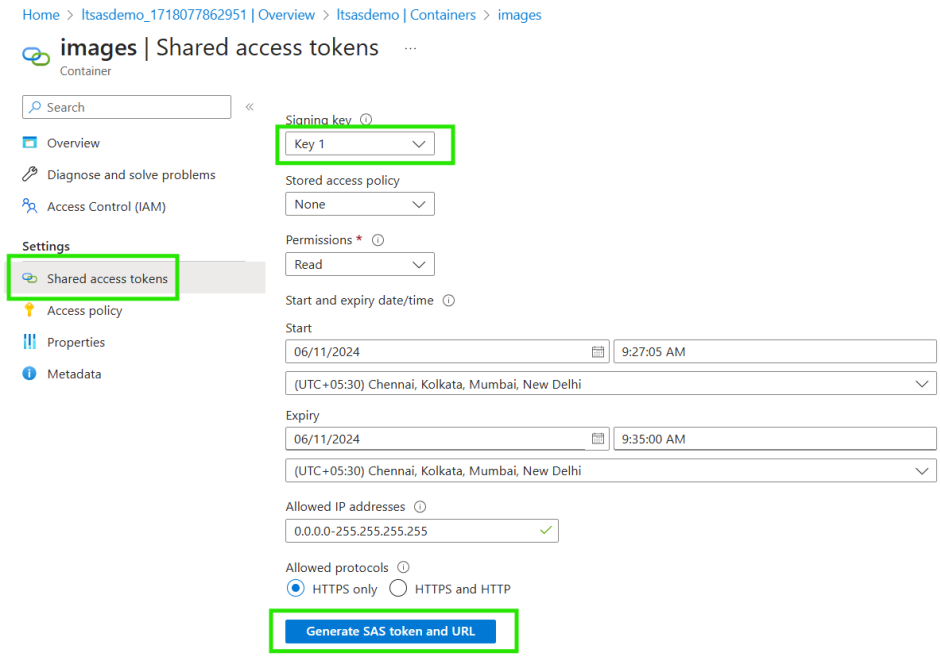
- Security is a major concern for organizations storing data in public cloud.
- Azure provides a set of comprehensive security capabilities to address the concerns of orgaizations.
  - Encryption: Azure encrypts all data written in azure storage account automaticatically using storage encryption serivce.
  - Authentication: Azure storage supports Azure AD based authentication for Azure blobs. Using RBAC we can control the access of storage account
  - Data in transit: (HTTPS)
  - Azure Disk encryption
  - Shared Access signatures: We can control fine-grained access to data objects using SAS keys

Shared access signature

- Every storage account has two keys called the access keys

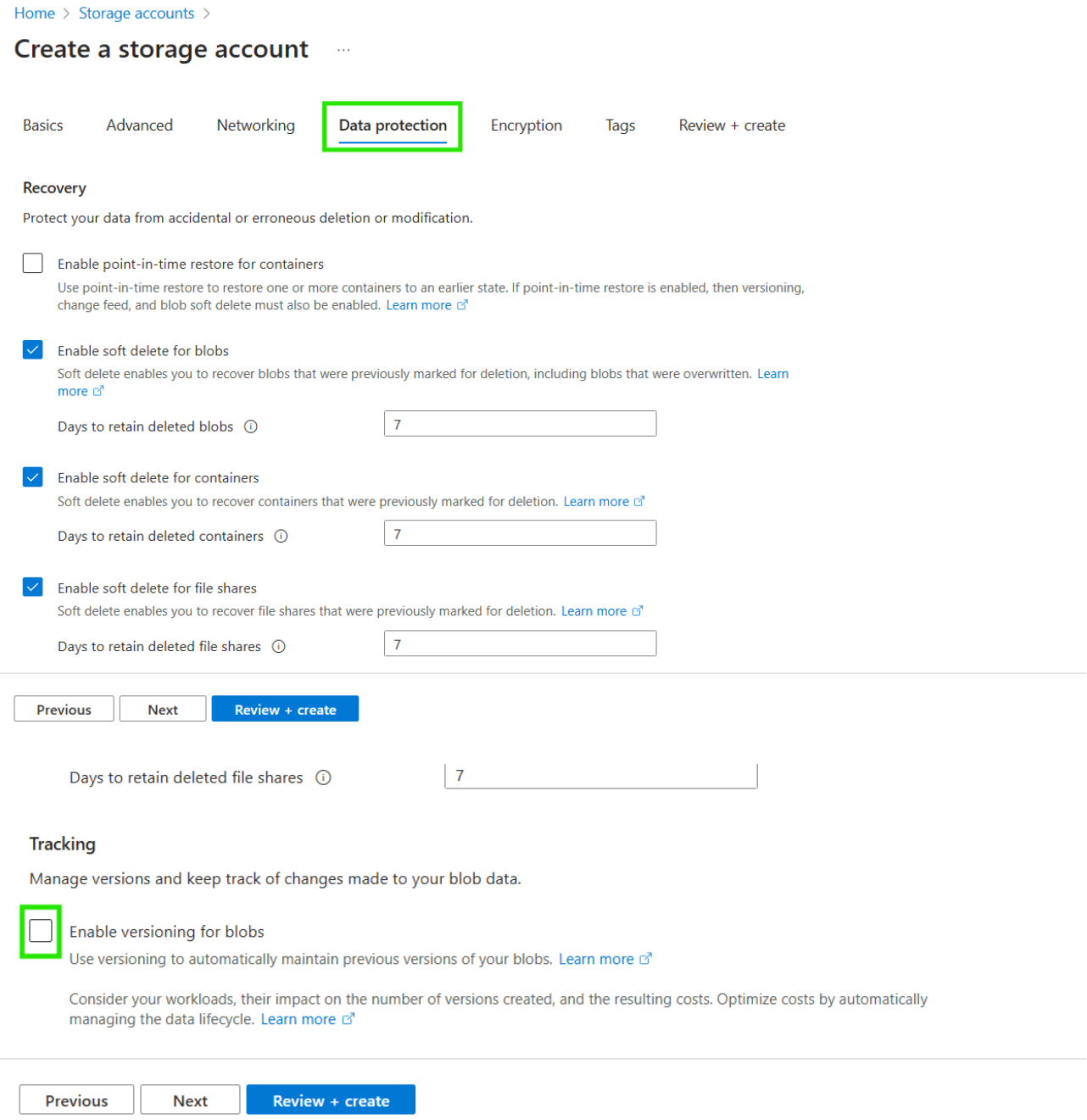


- We can share these access keys with users and they can use this is Autorization header of API calls to get authenticated.
- This is not considered to be a good apporach as the user gets full access as long as keys are not rotated
- SAS is a UR that is composed of various parameters by which you can restrict access to Azure storage
- SAS gives us the ability to grant granular access to the objects. Using SAS
    - Control access at the service level
    - Set the time frame during which SAS is valid
    - Set permisions like read, write, delete etc
    - Set IP rangres from which SAS Keys are accepted
    - Set the protocol to HTTP or HTTPS
- Create a SAS for read access

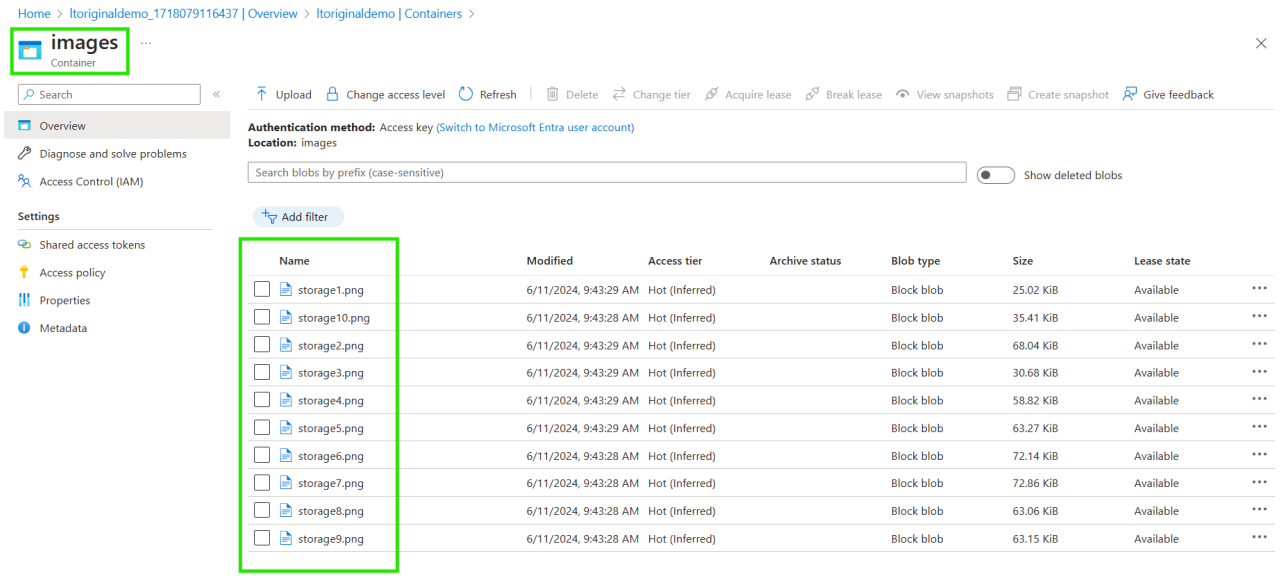


Data Protection in Azure storage Accounts

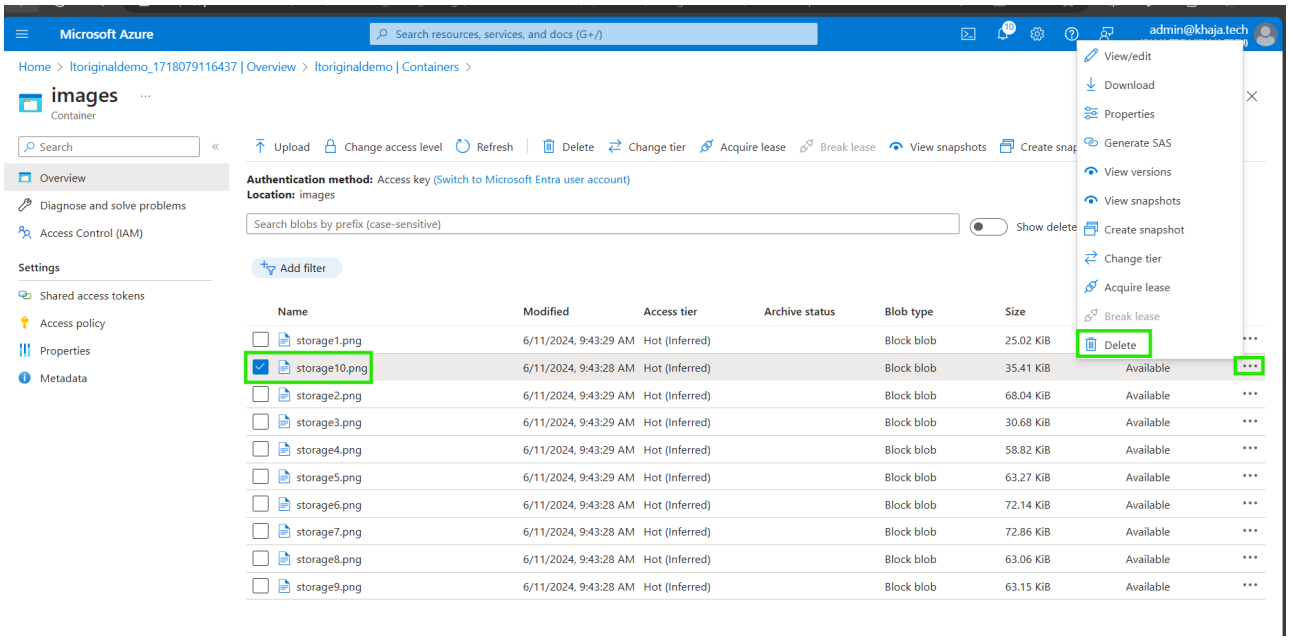
- Lets create a new resource group `original`
- Lets create a storage account with randomname and focus on Data protection tab



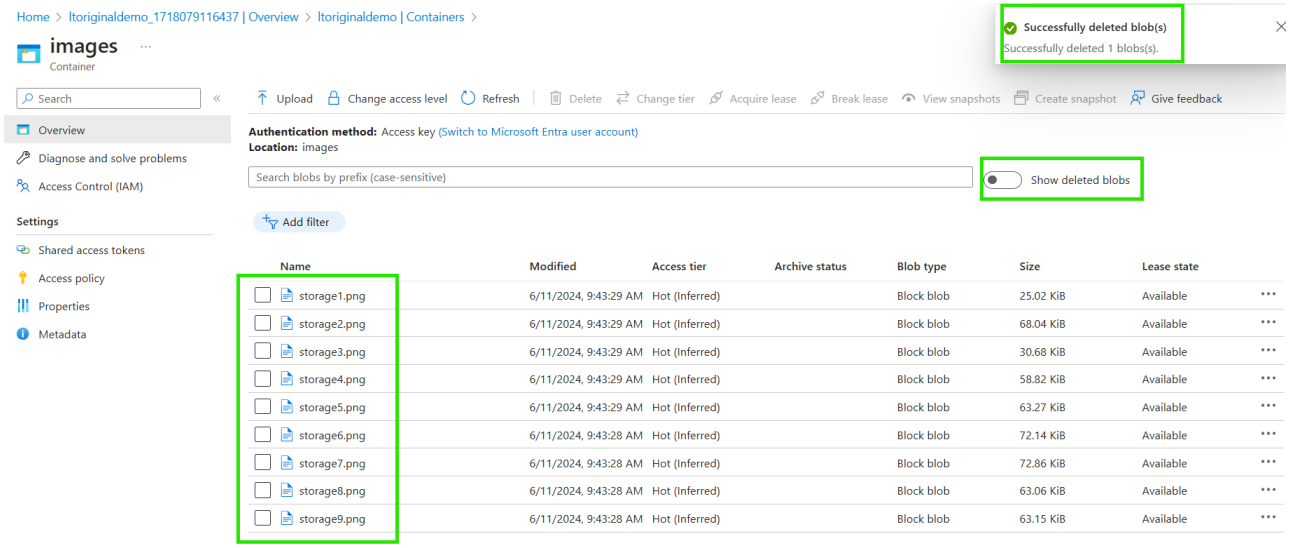
- Now create a container and upload some items into it

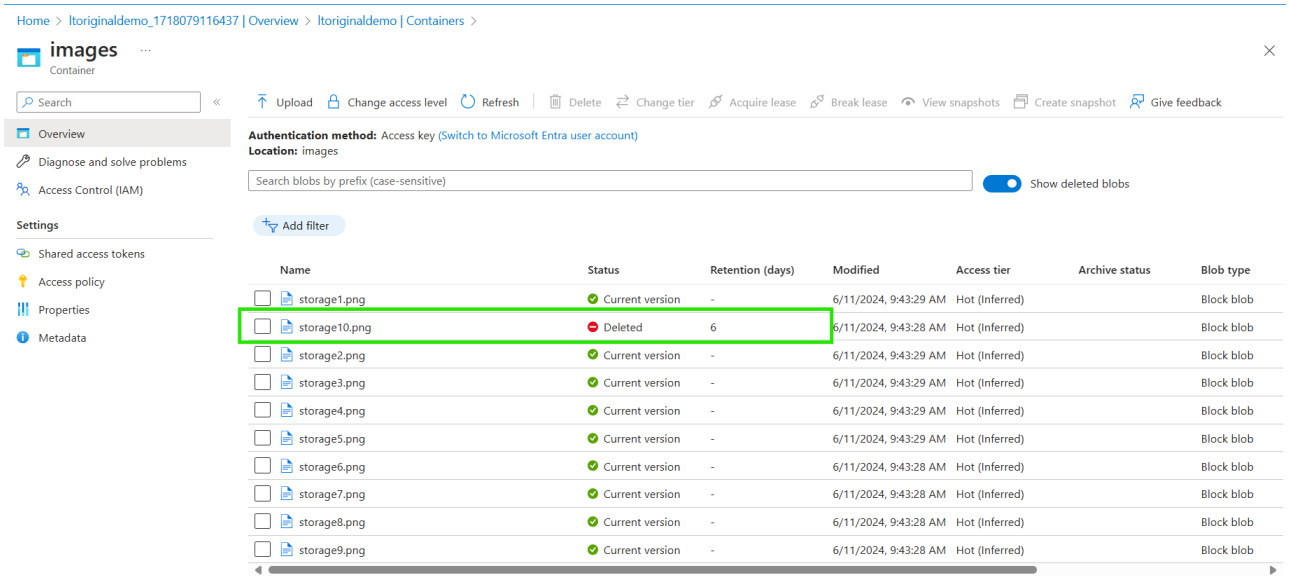


- Since soft delete is enabled for 7 days, lets delete storage10.png

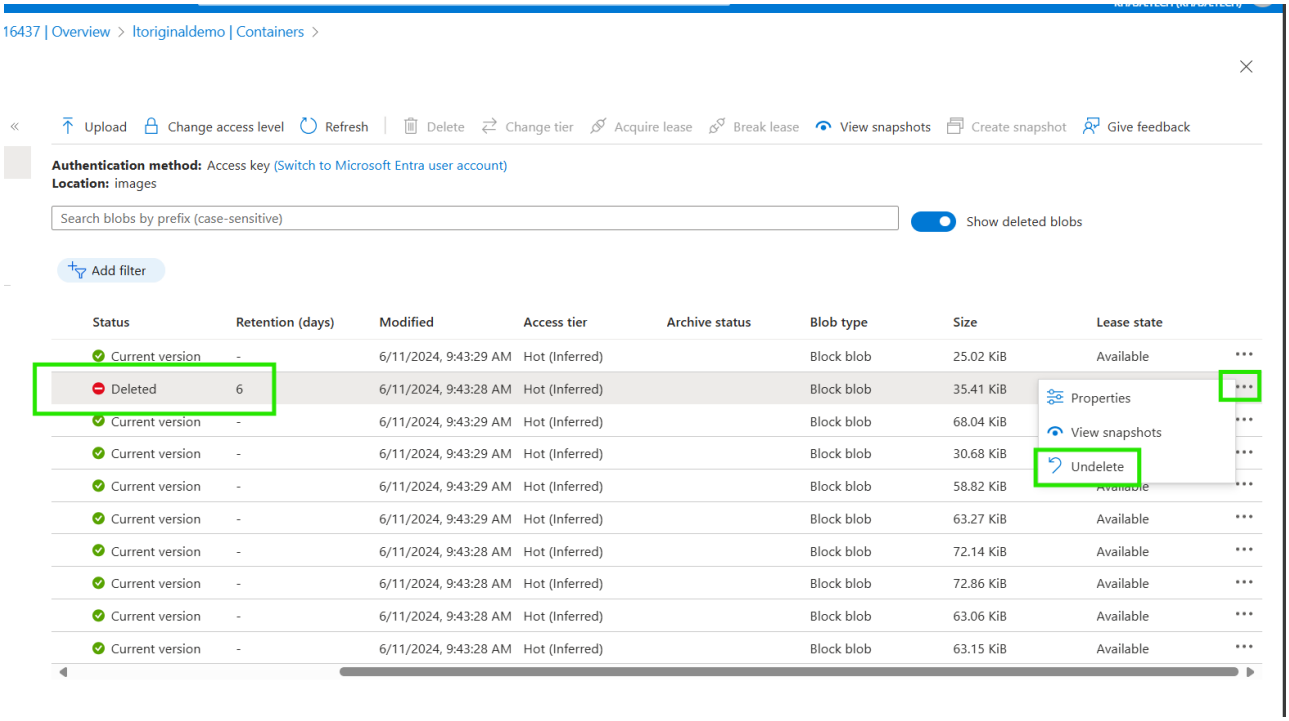


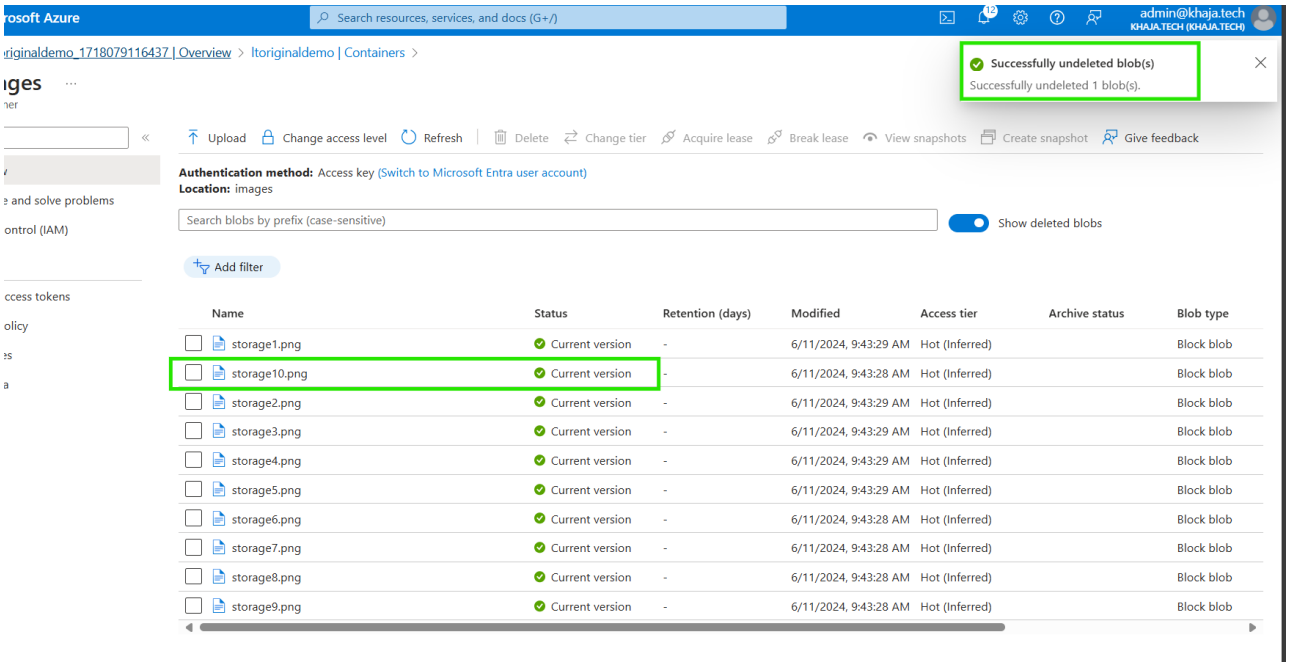
- Now lets view the items and select show deleted blobs





- To undelete the storage10.png





- We can undelete containers within 7 days
- We can undelete storage account within 14 days as long as you have not create a new storage account with a same name and resource group.