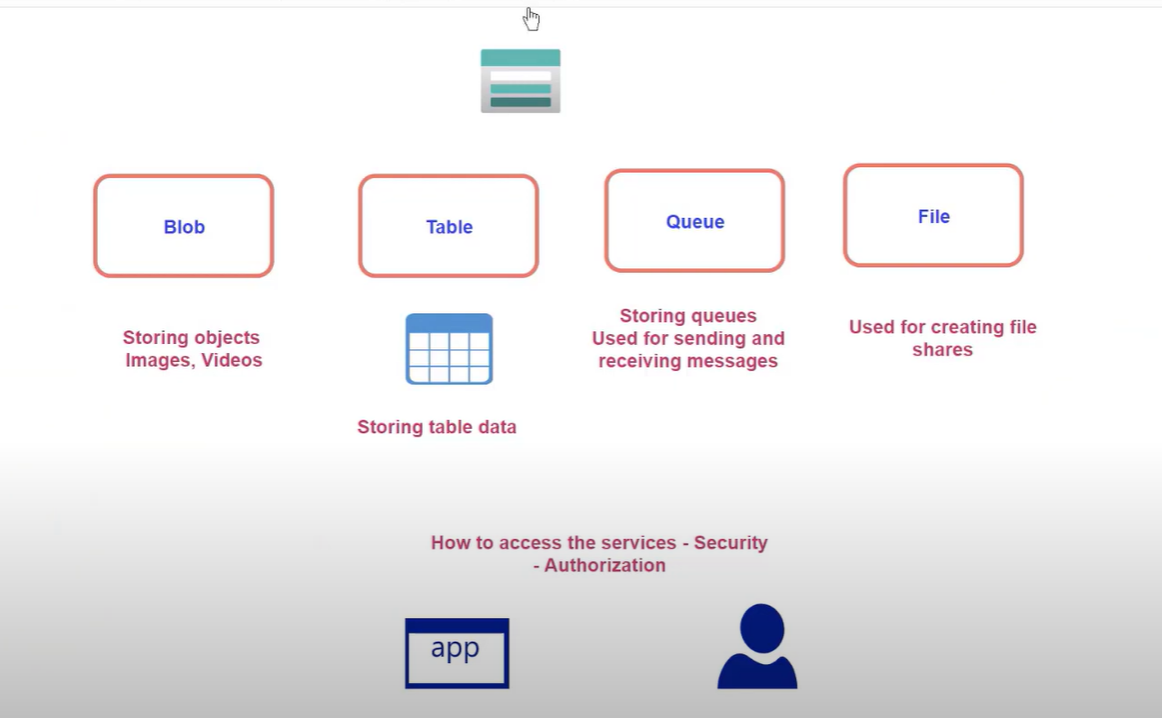
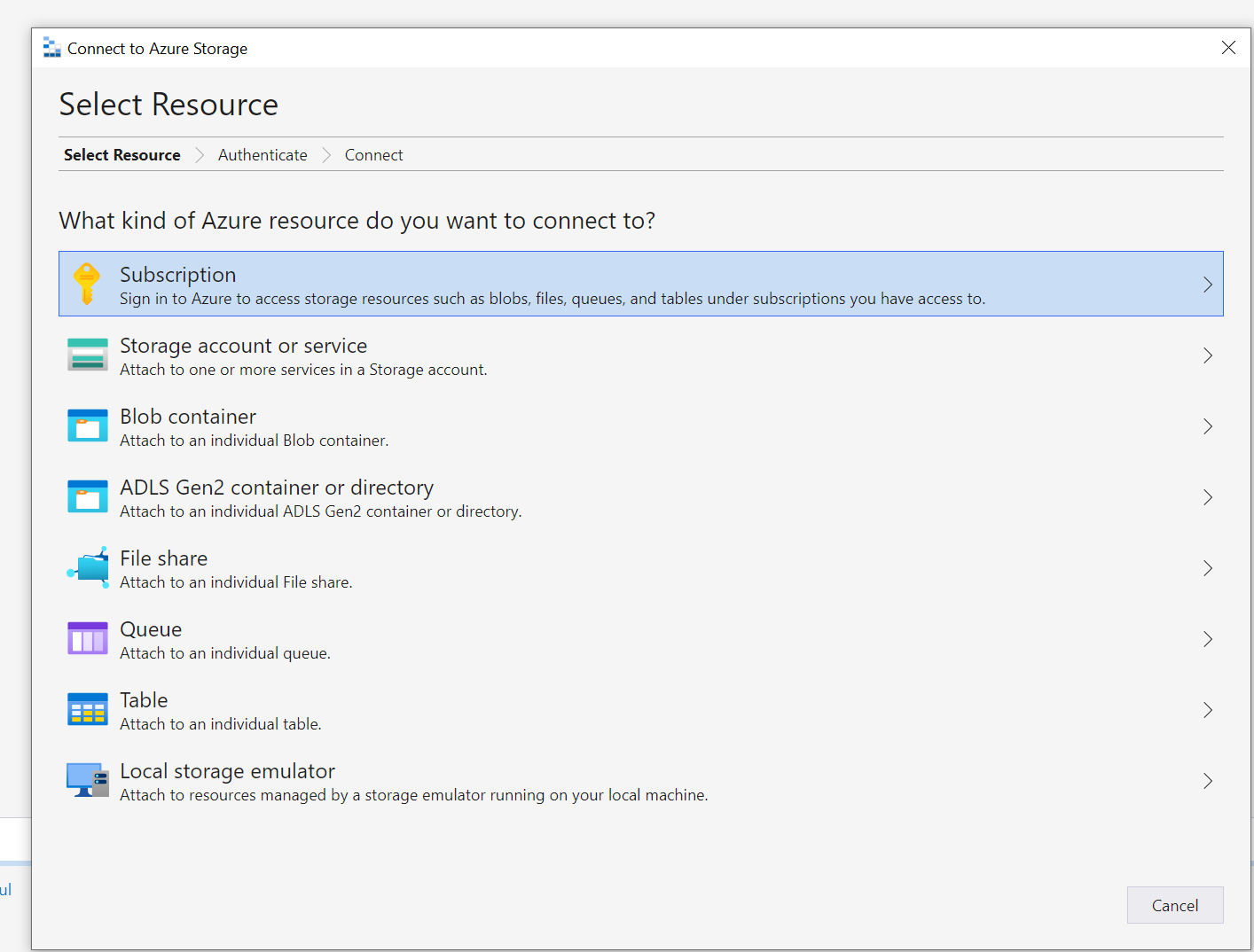
**Lesson08 Authorization Techniques**

**Notes:-**

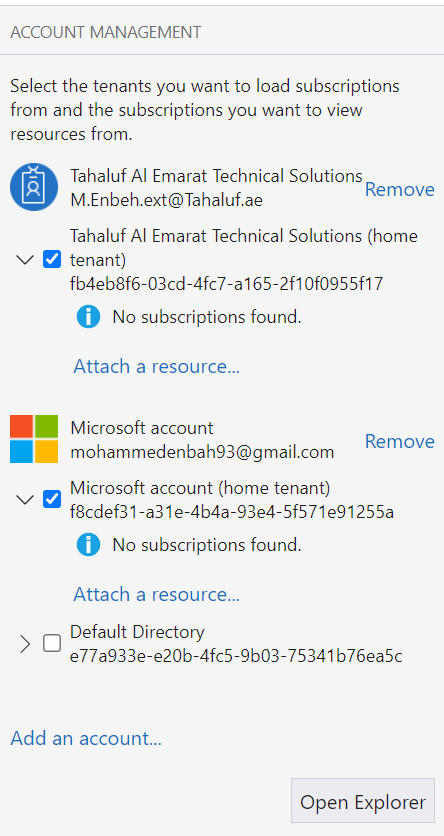
**1-there are different way to access azure container type > files** **A-Public Access, which means that you can access to any files on any container under that storage account**

**B-Access Key**

**C-Shared Access Signature   
D-Active Directory**

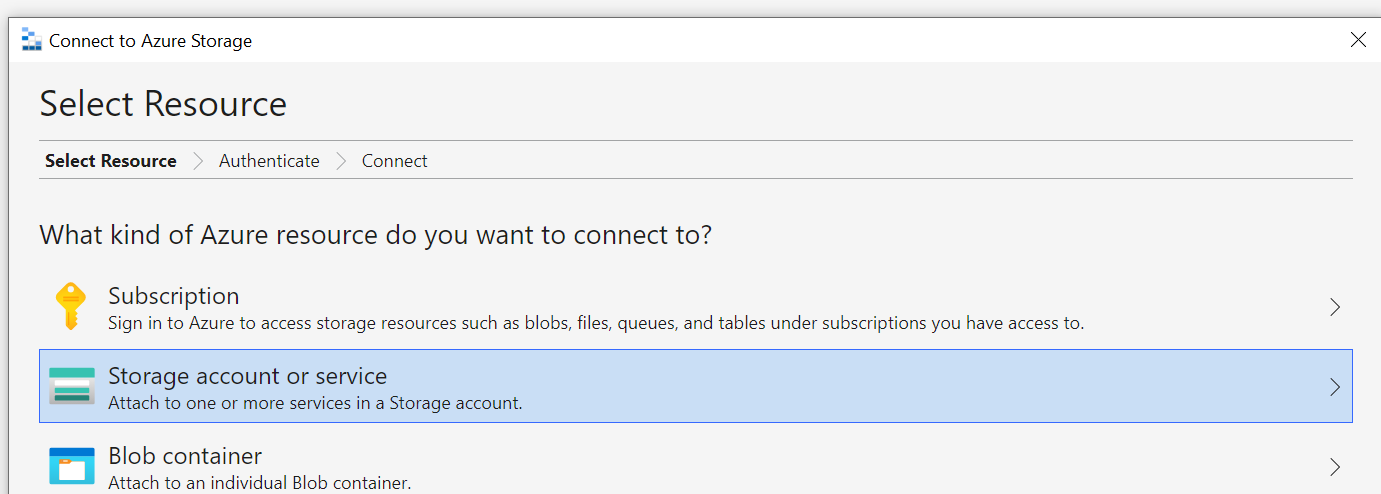
**A-Active Directory   
  
1-we will download and install Azure Storage Explorer and then click on Connect icon > choose Subscription**

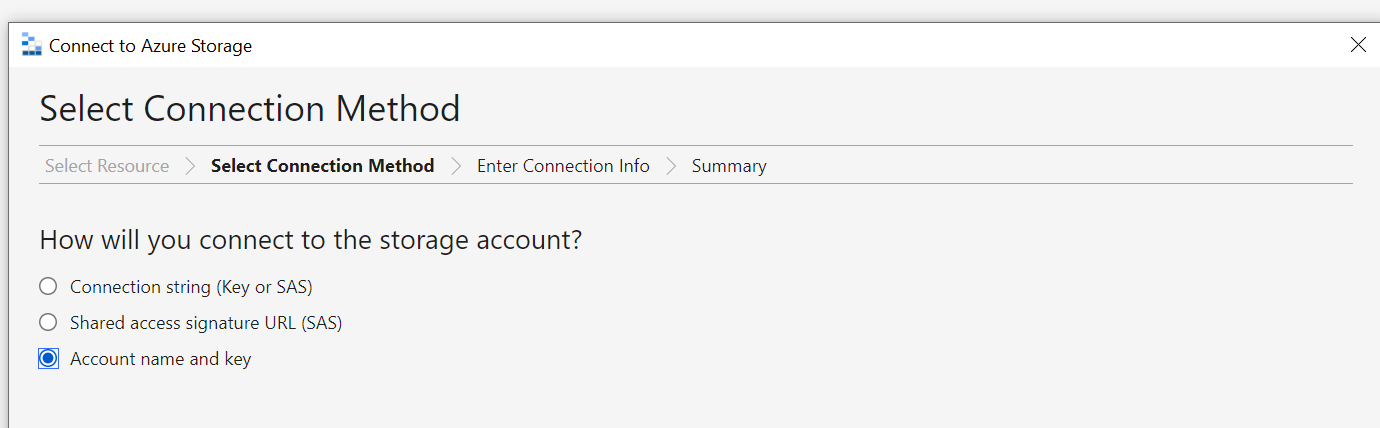
**2-then we type the username active directory we have it before and it will show**



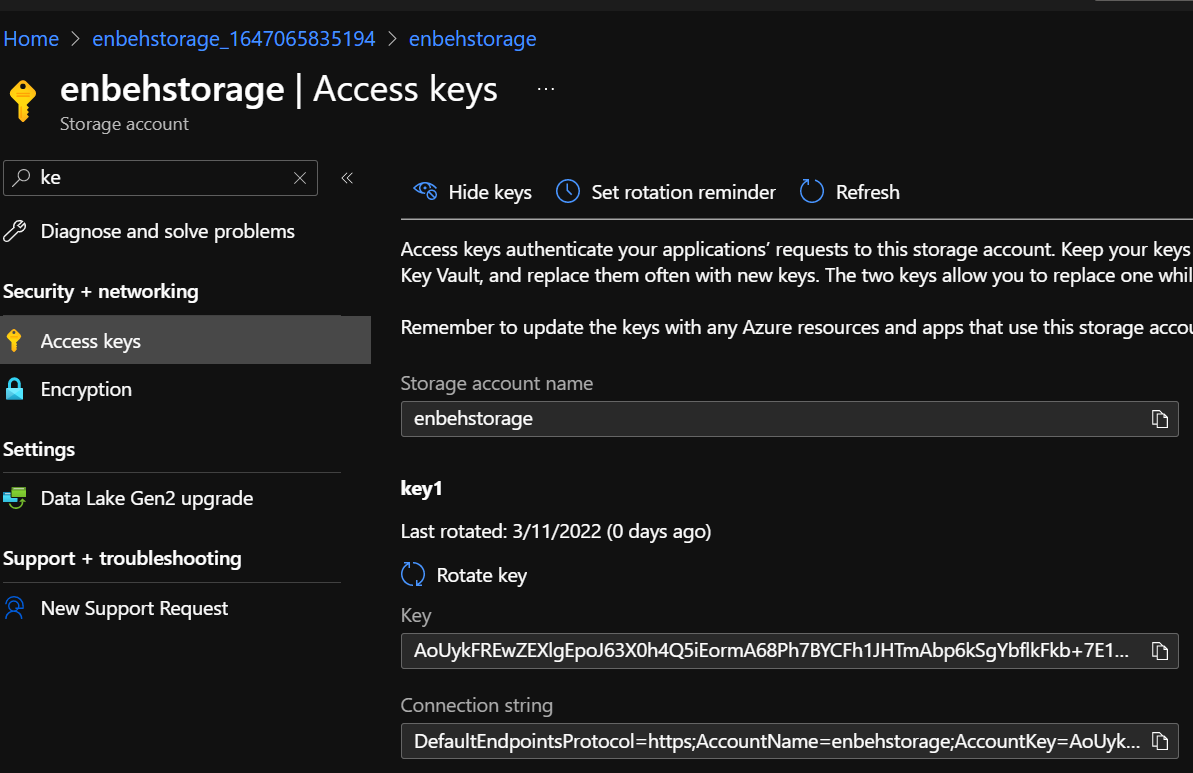
**B-Access Key**

**(It will provide full access permission unlike active directory based on the role of that login user)**

**1-click on Connect Icon on Azure Storage Explorer**



**2-under the azure storage account > Access Keys > we copy the name and key as below**

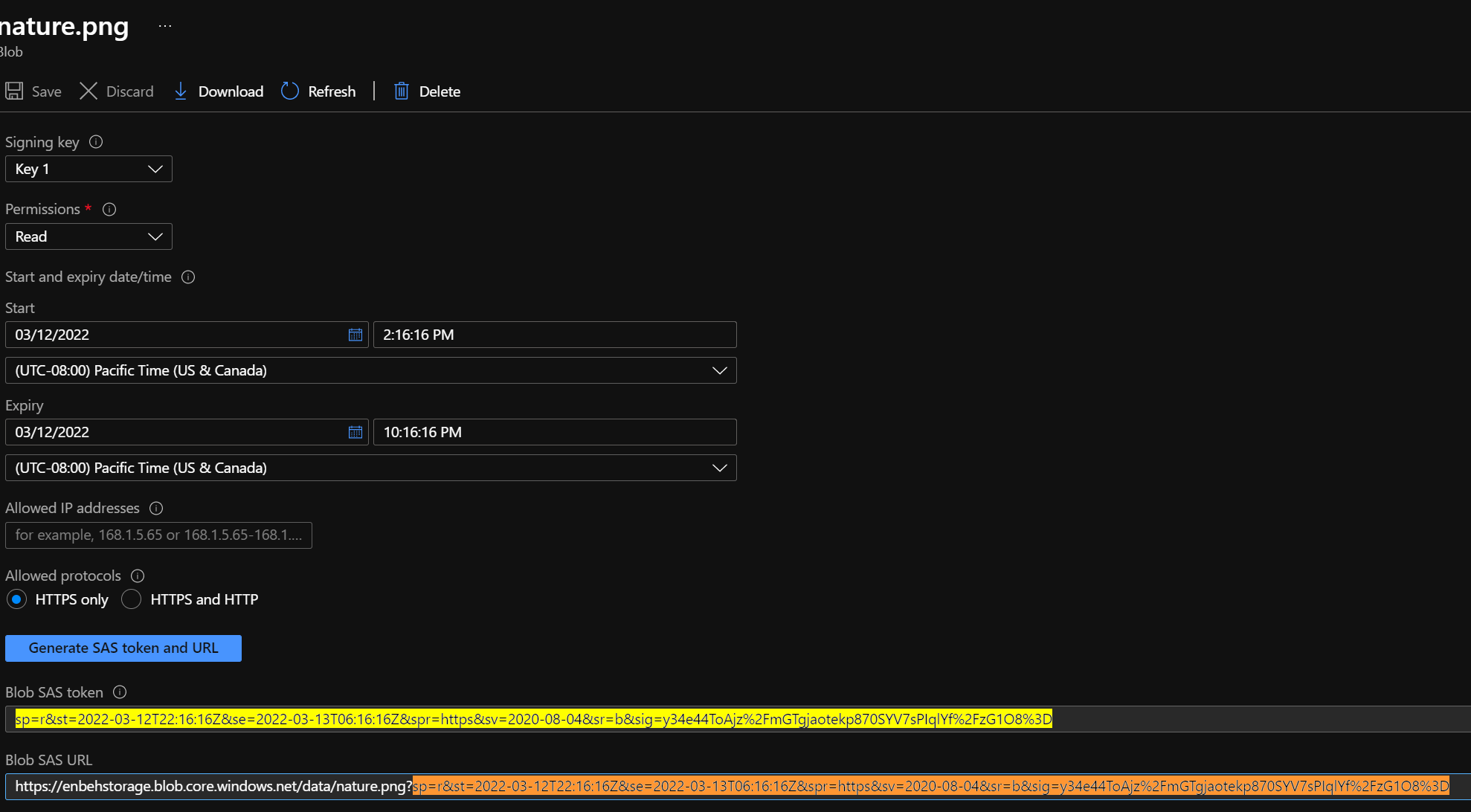


**C-Shared Access Signature – SASS  
it’s generate either on blob file or on the storage account level**

**A-Blob level**

**(This SASS token has time limit on the blob file provided)**

**(There is blob sass URL that contains the SASS token)**

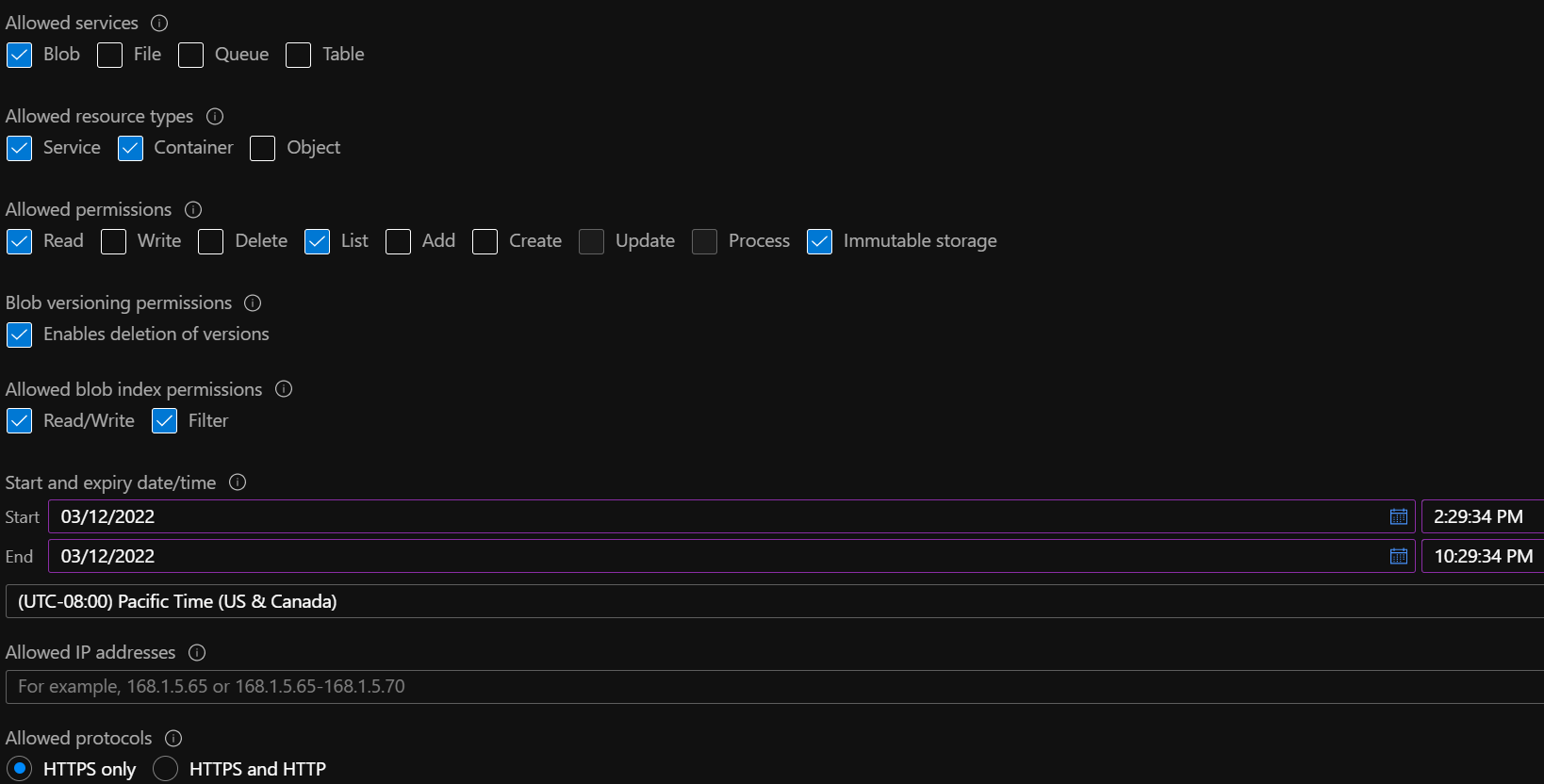


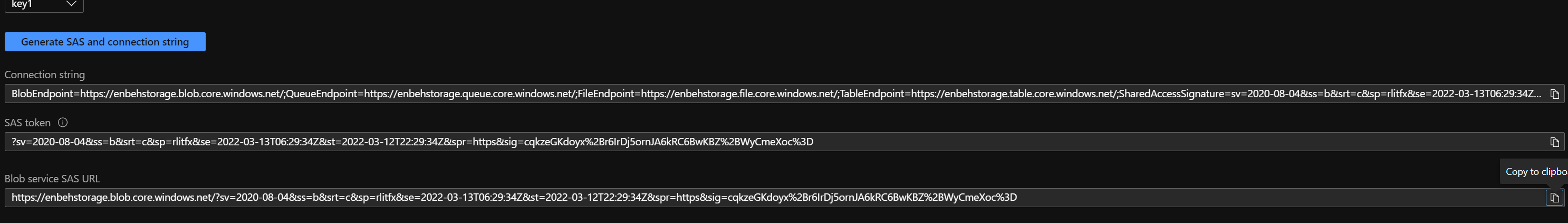
**B-Storage Account level**

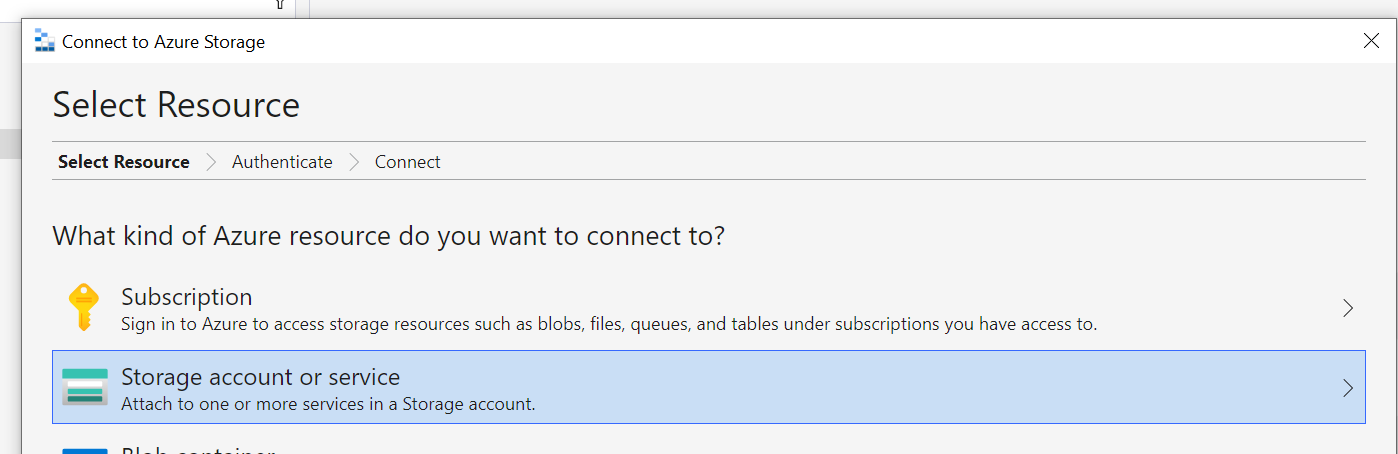
**(We can access either on keys (full access)**

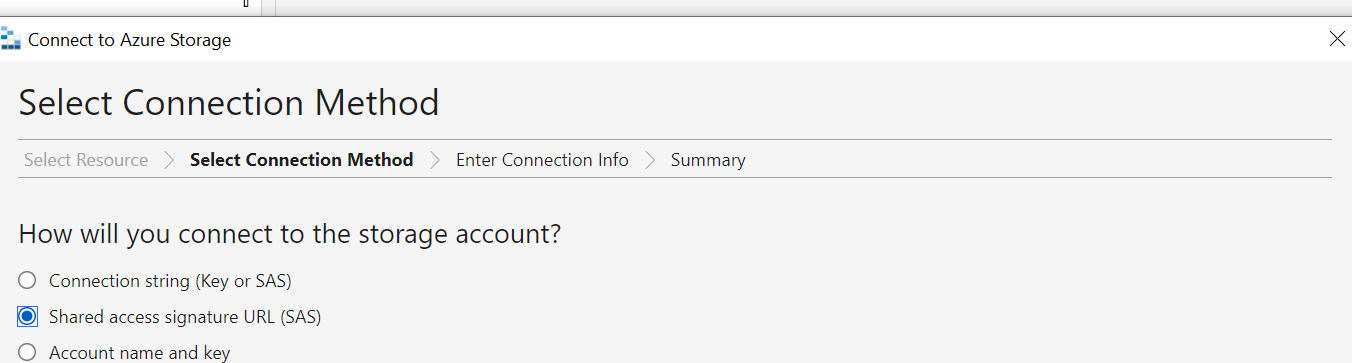
**Or SASS (specific access as configured manually with period time)**

**(Use SASS if you want to restrict access to storage account via SASS URL)**

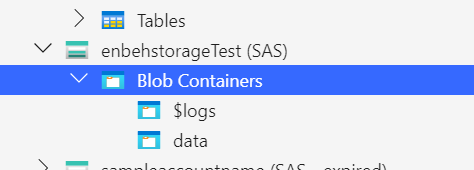


**(As you see you can choose what you want to access and select the authorization you want to operator to that service / container / object)**

**With blob SASS URL , I can access to storage account to allowed service > blob as below   
  
storage explorer > connect**



**(You will see that it will show only blob container not the other types)**



**(If you try to delete the file it will show insufficient privileges)**

**If you want to make less restrict roles based on parent role that attach with storage account > use access policy**

