

**PLACEMENT EMPOWERMENT PROGRAM**

**Cloud Computing & DevOps Centre**

Creating a “Storage Account” in Azure and uploading files in it. Also configuring access permissions [Access levels, Network access restrictions, Access Keys, and SAS]

**Name:** Pranav Karunakaran

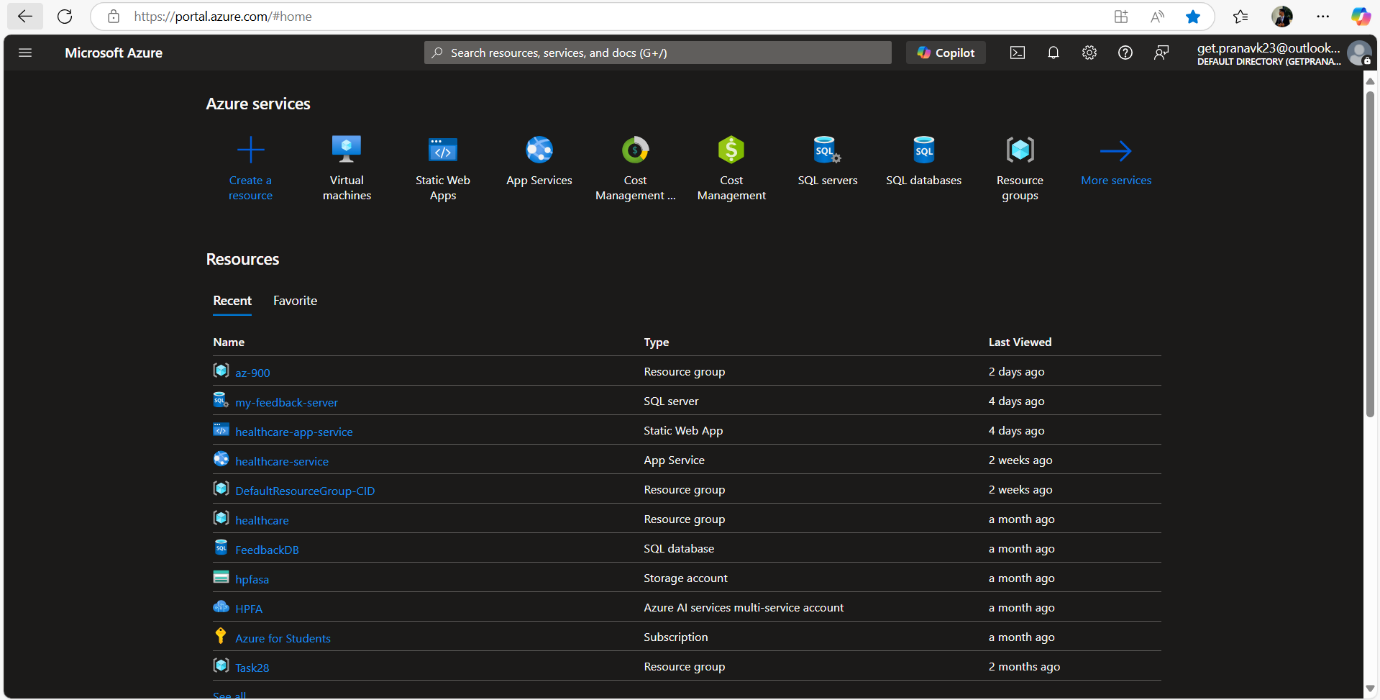
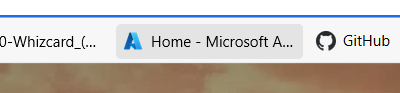
**Dept:** IT

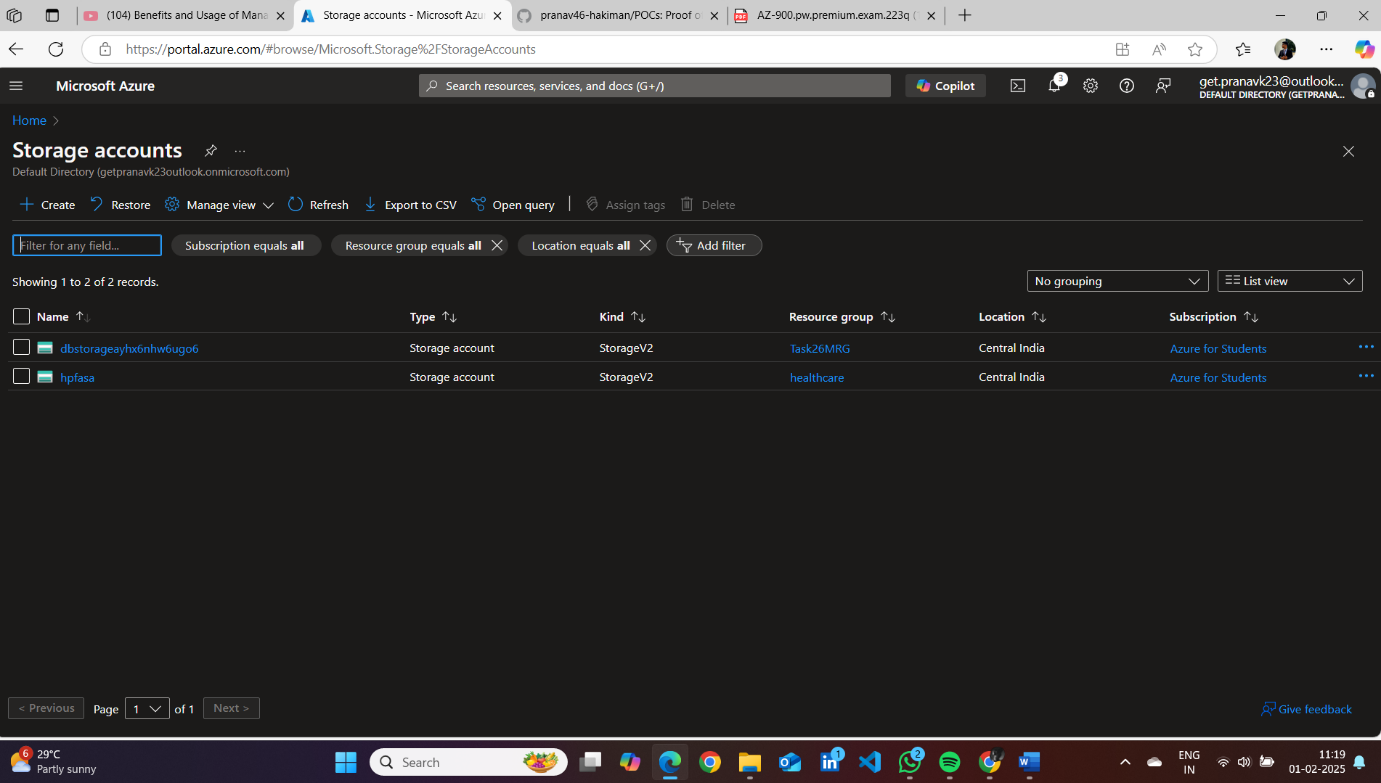
**INTRODUCTION**

* Creating a Storage Account in Azure involves setting up a secure and scalable storage solution for file management. Begin by navigating to the Azure Portal, selecting Storage Accounts, and clicking Create. Provide details like subscription, resource group, region, and redundancy options, then finalize by clicking Review + Create. Once the storage account is ready, create a Blob Container to organize your files and upload them directly through the portal or programmatically using the Azure SDK.
* To configure access permissions, consider multiple layers of security. Set Access Levels through role-based access control (RBAC) by assigning roles such as Storage Blob Data Owner or Data Reader under the Access Control (IAM) section. Manage Network Access Restrictions by enabling firewalls or virtual network rules to limit access. Access Keys provide full control and should be used cautiously with regular key rotation for enhanced security. For more granular and time-bound permissions, generate Shared Access Signatures (SAS) to grant temporary access without sharing sensitive keys. By combining these configurations, you ensure secure and efficient file management within Azure**.**

**Step-by-step process:**

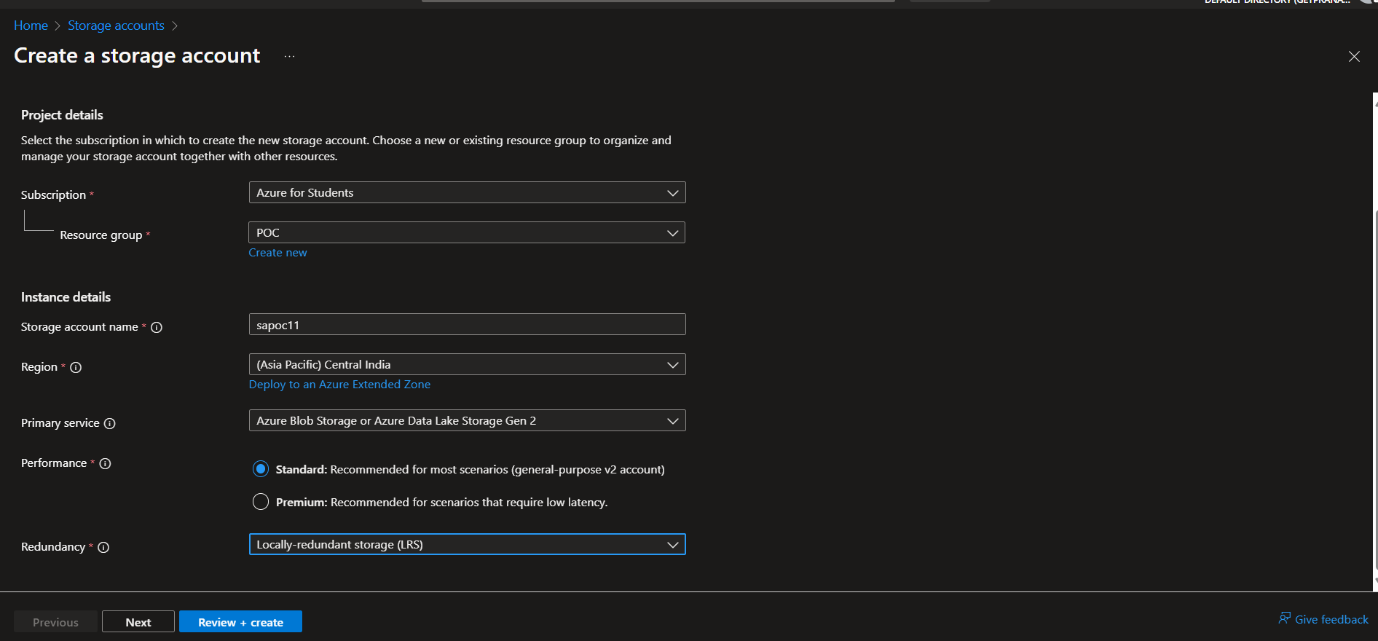
**Step 1:** Go to Azure portal.



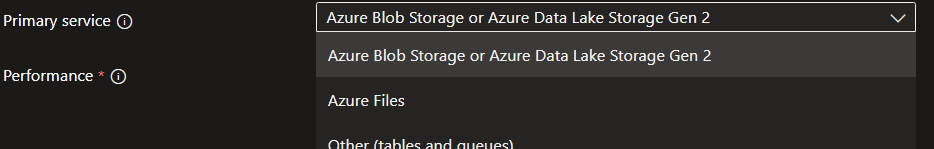
Step 2: Navigate to “Storage Accounts”. 

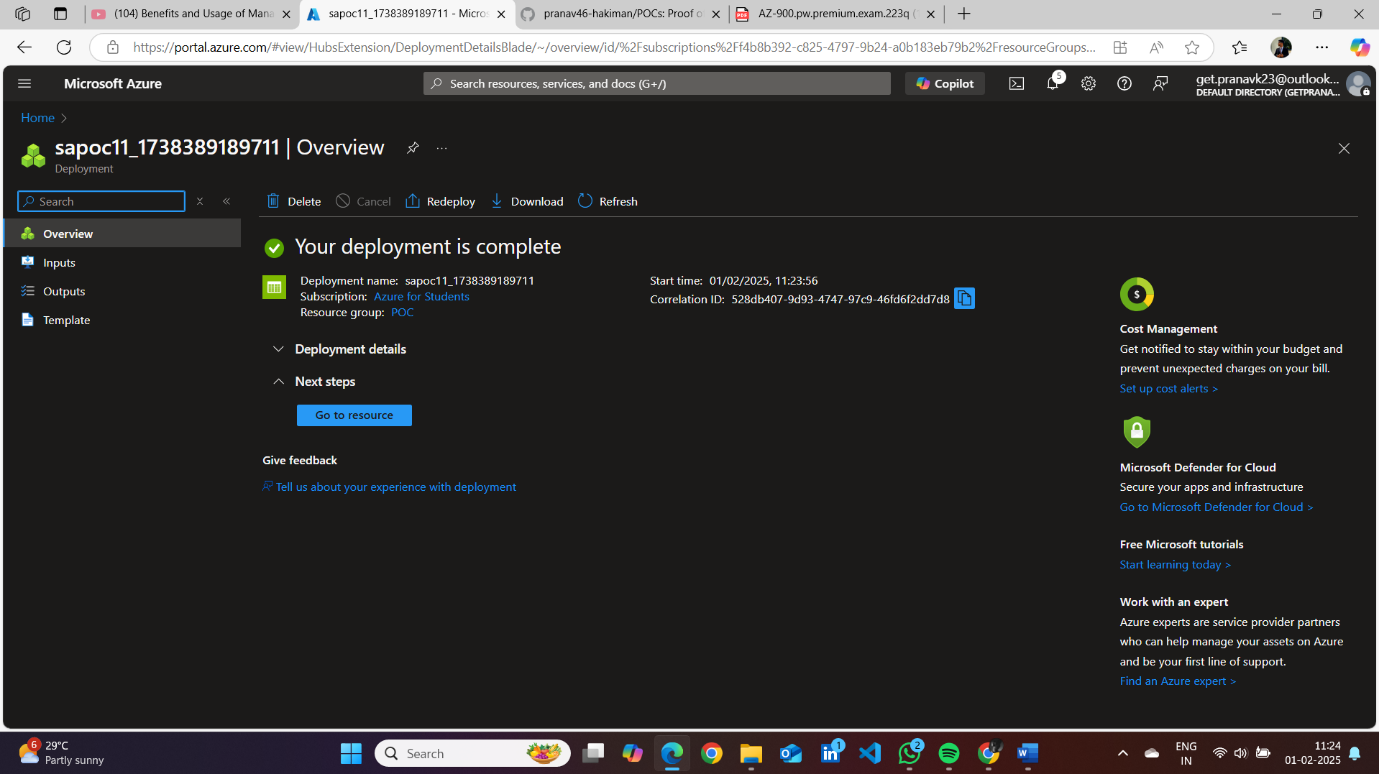
Step 3: Enter the following details: 

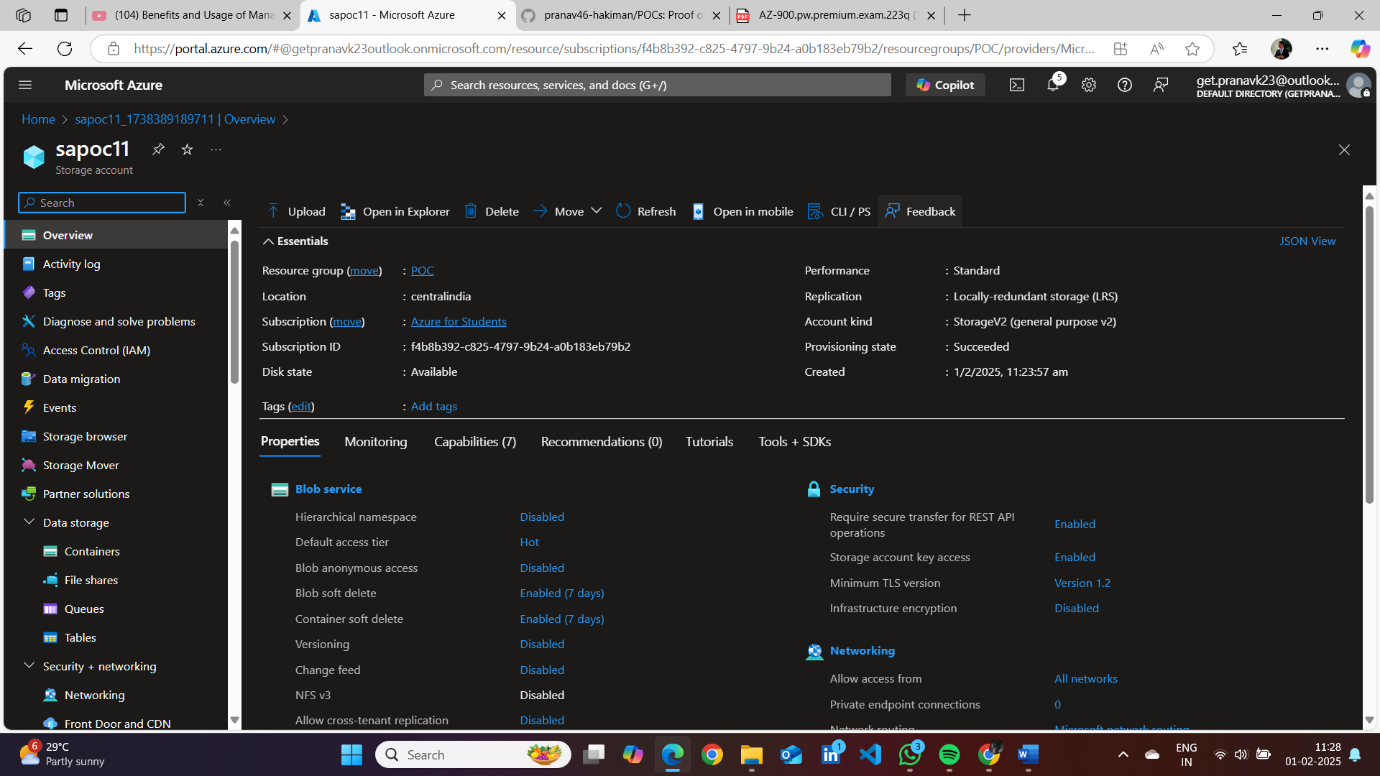
1. **Subscription**: Choose your subscription.
2. **Resource group**: Create a new one or select an existing resource group.
3. **Storage account name**: Enter a unique name.
4. **Region**: Select the nearest region.
5. **Performance**: Standard or Premium (choose based on requirements).
6. **Redundancy**: Select redundancy option (e.g., Locally-redundant storage).



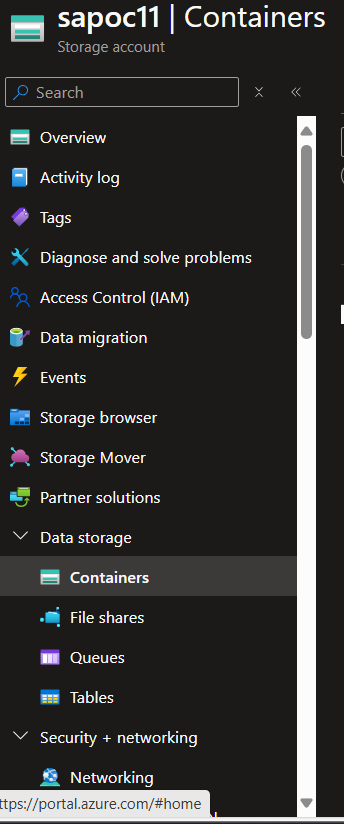
**Note: You can choose the service you want while creating the storage account in azure.**

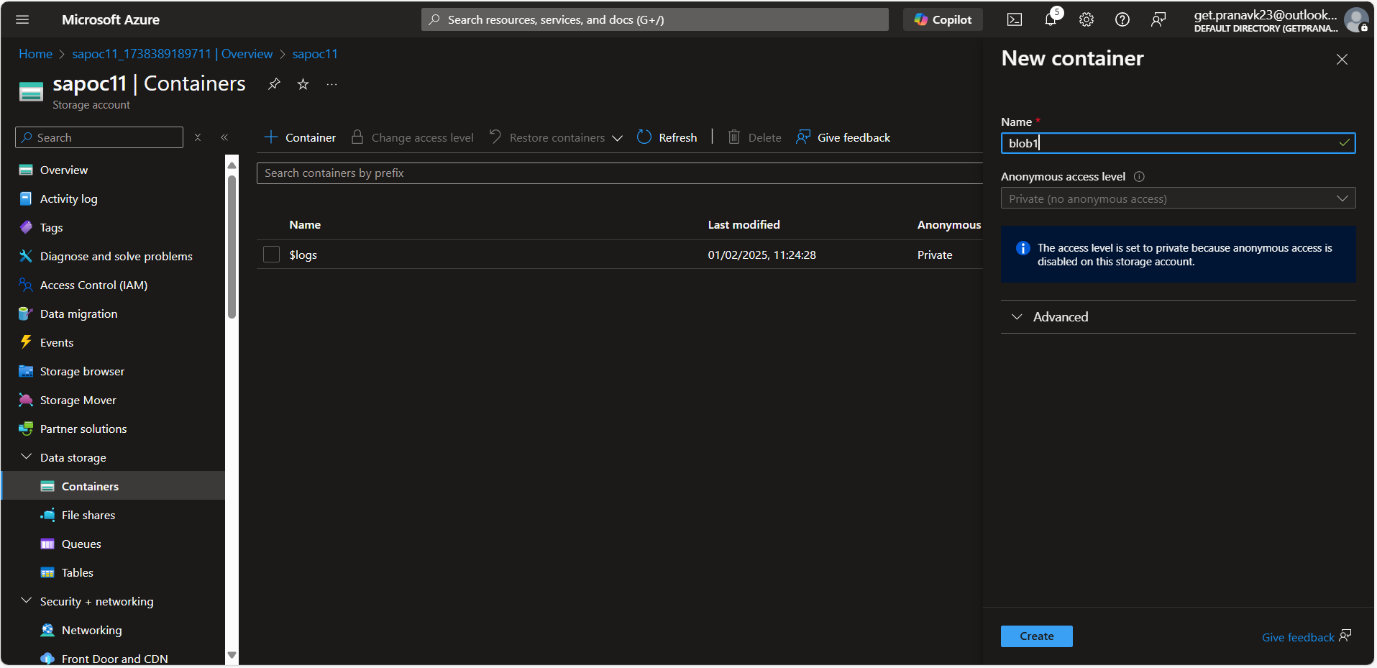


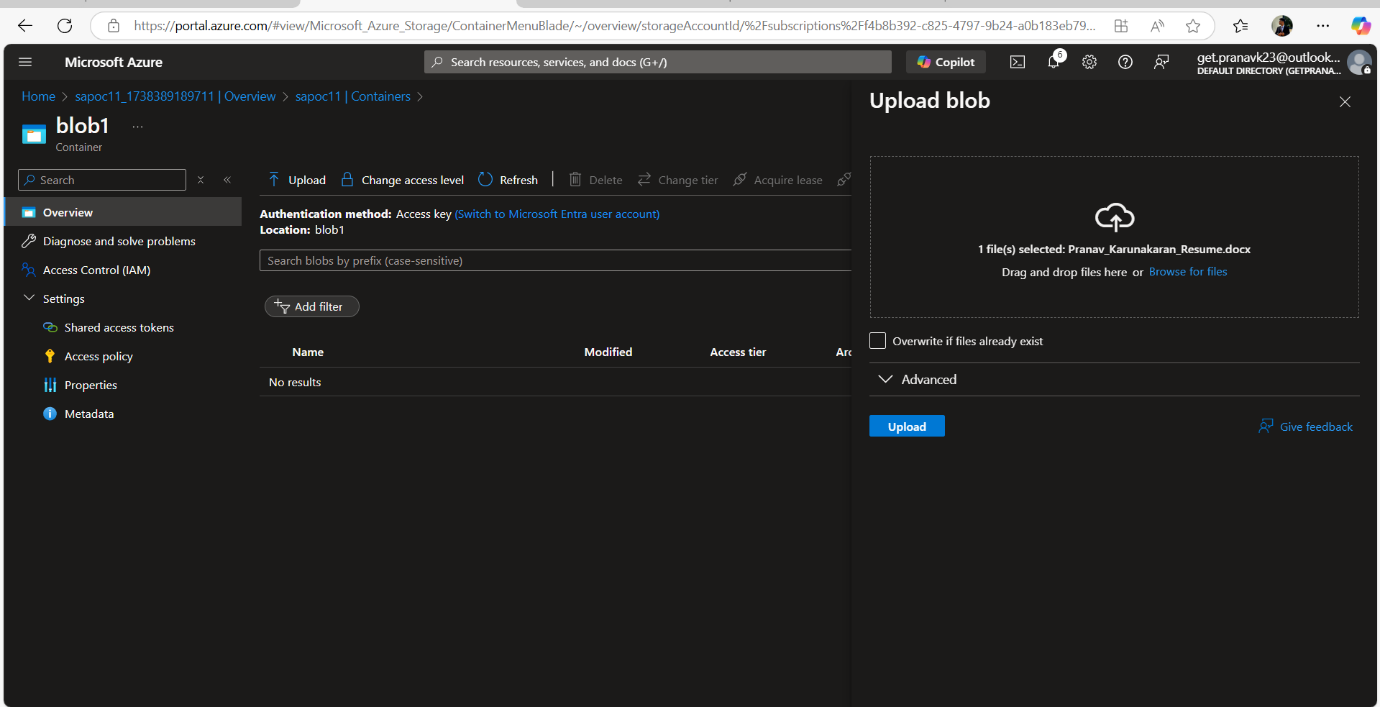
**Step 4**: Once deployment is done go to the Resource Group to view your Storage account. 

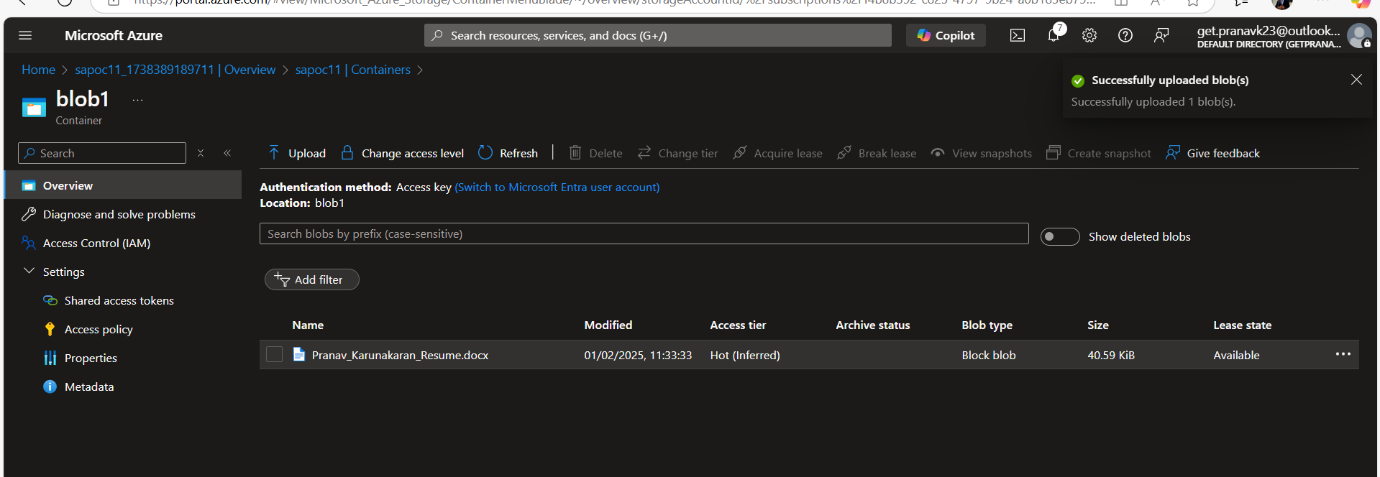


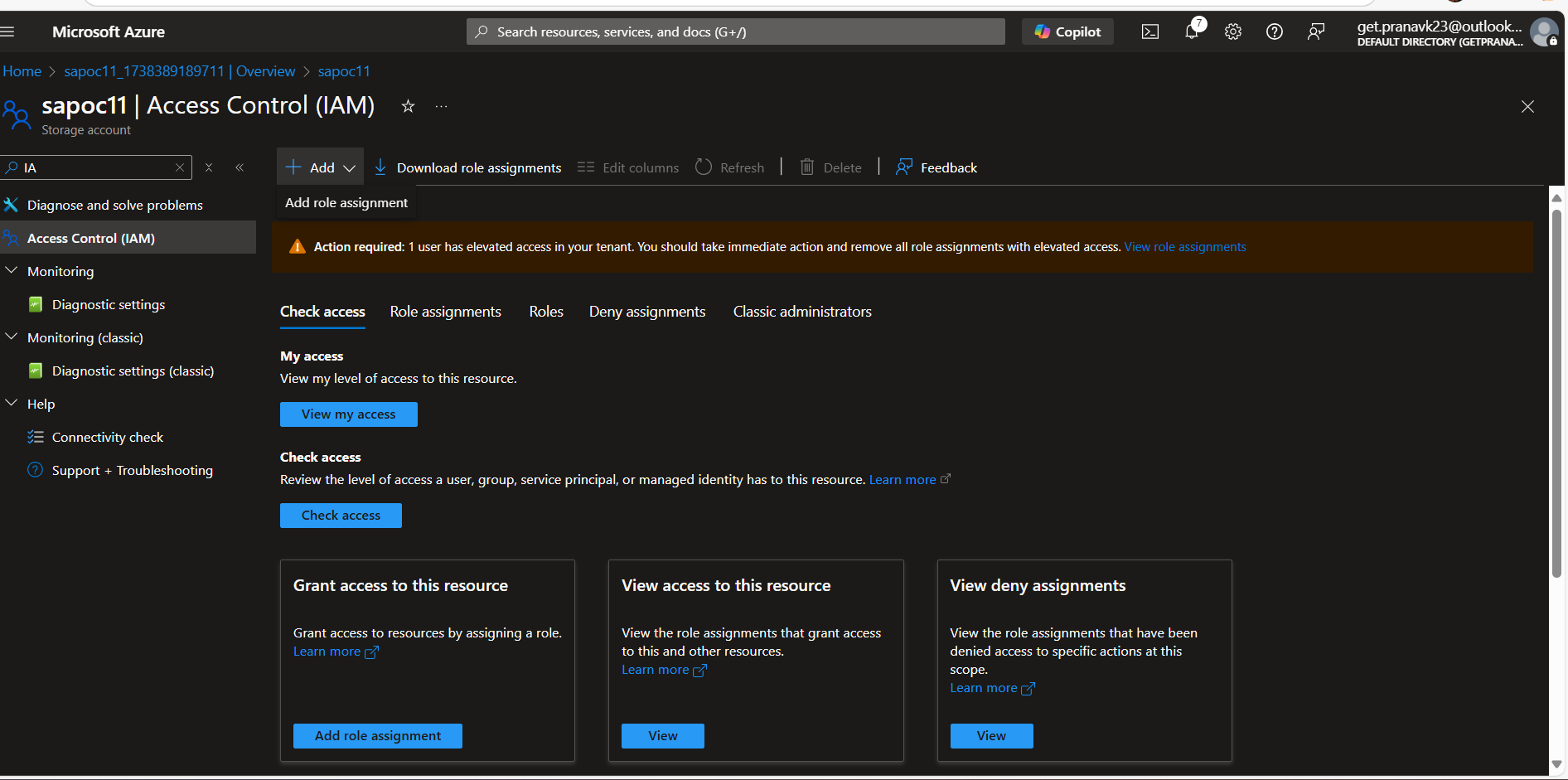
**Step 5**: Got to “Conatiners” which is located in data storage in your Storage account.

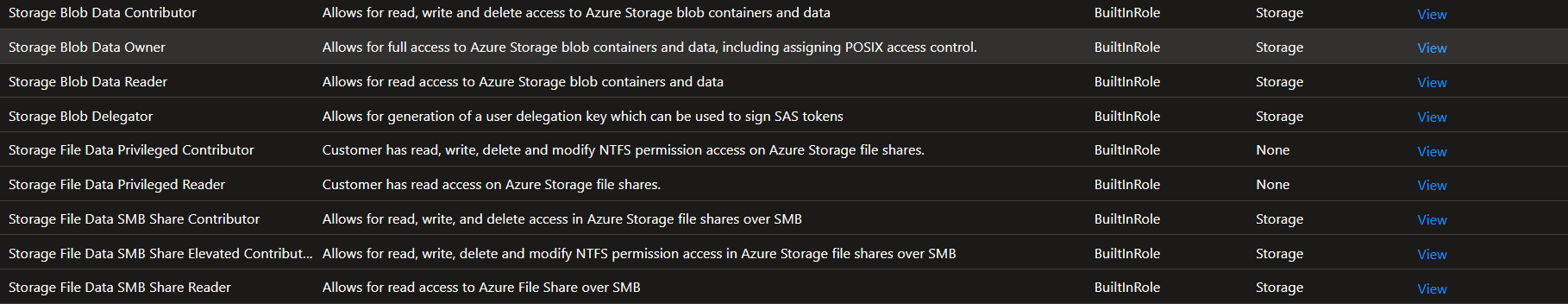
**Then create a Blob Container:** 

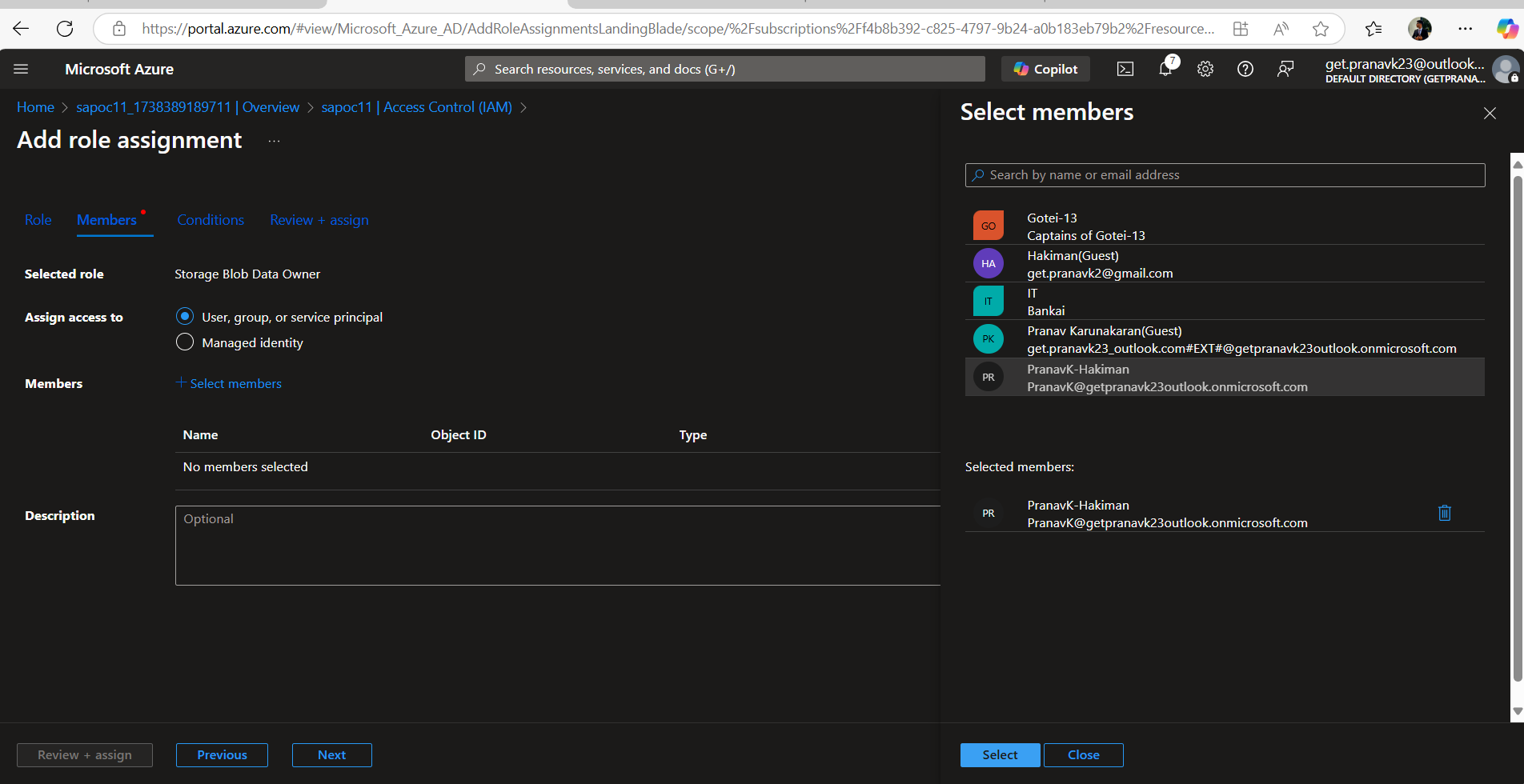


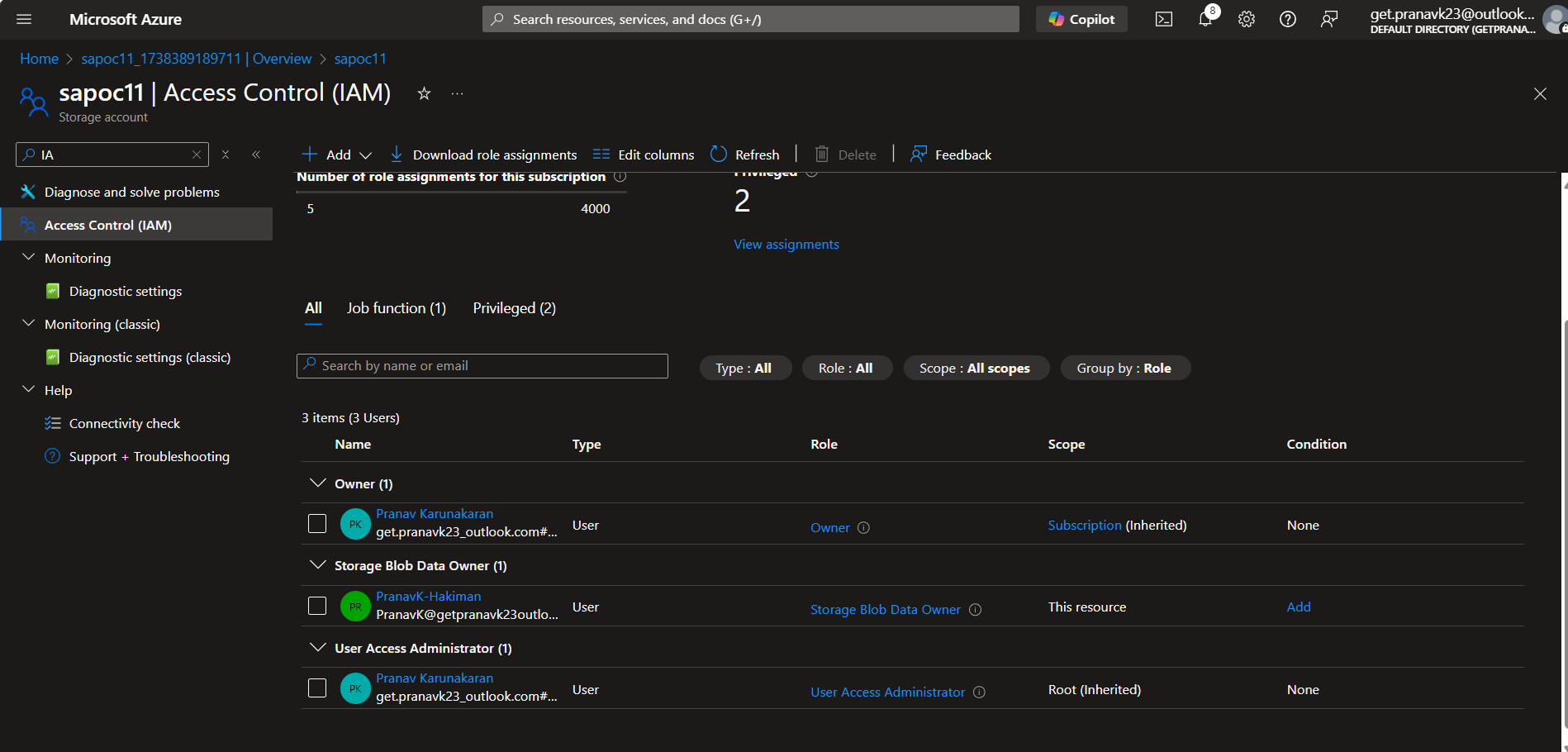
**Step 6:** Now open the “Container” you created and there will be an option to “+upload”, click on that for uploading files. And then click on upload. 



Step 7: Configuring access permissions. For that you need to go to “Storage Account > IAM > Roles

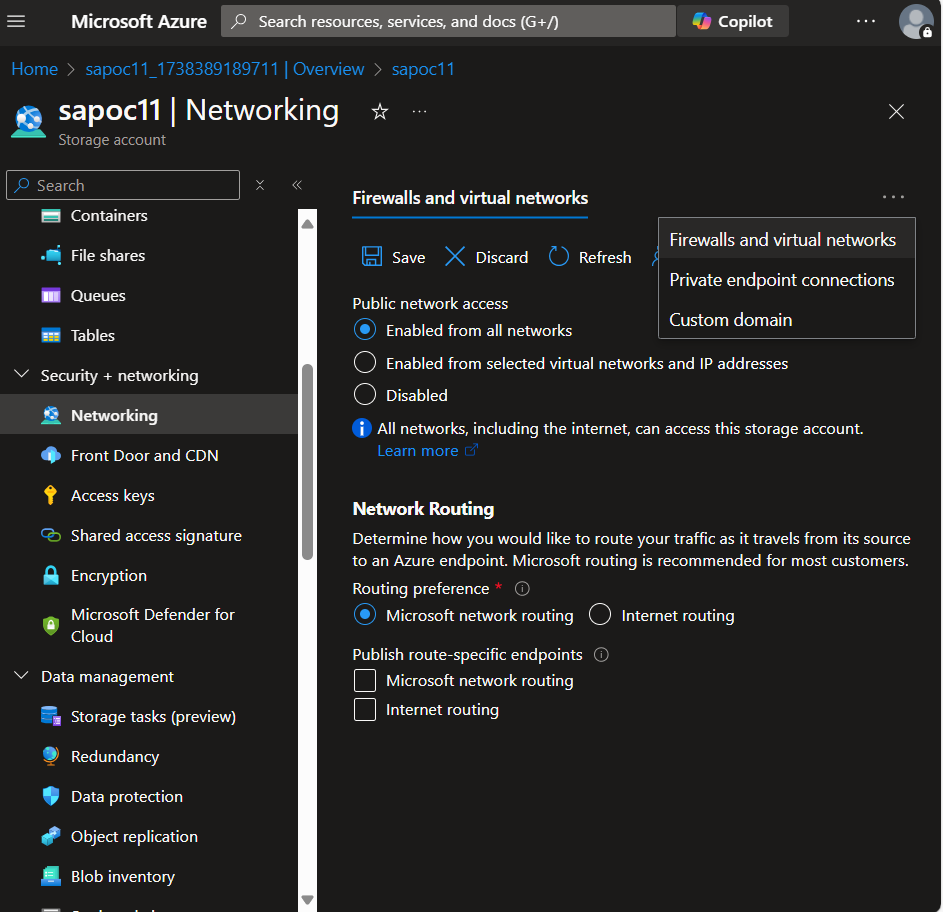
ROLES: 



Step 8: Once done click on “Review+Assign”. 

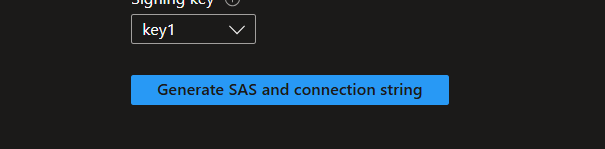
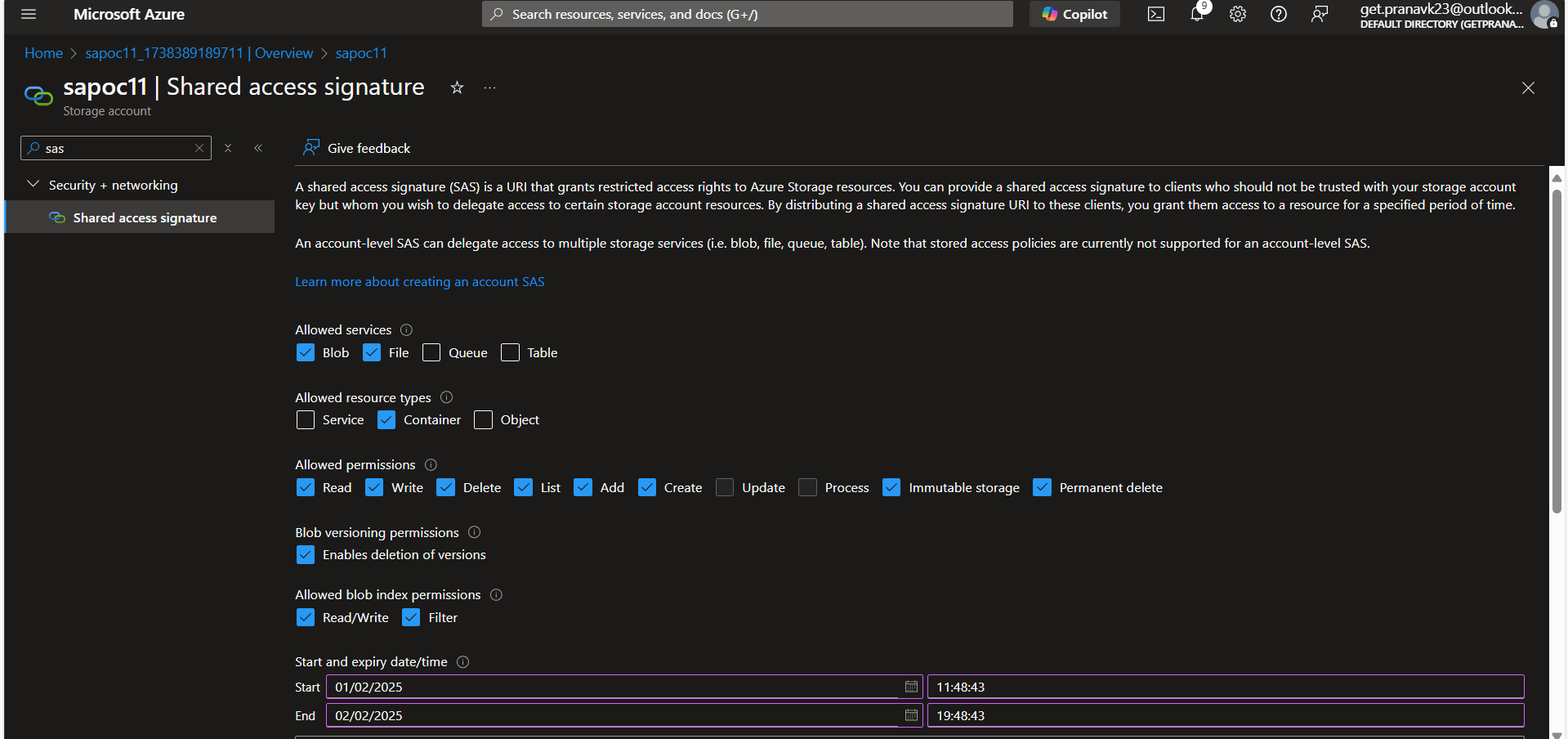
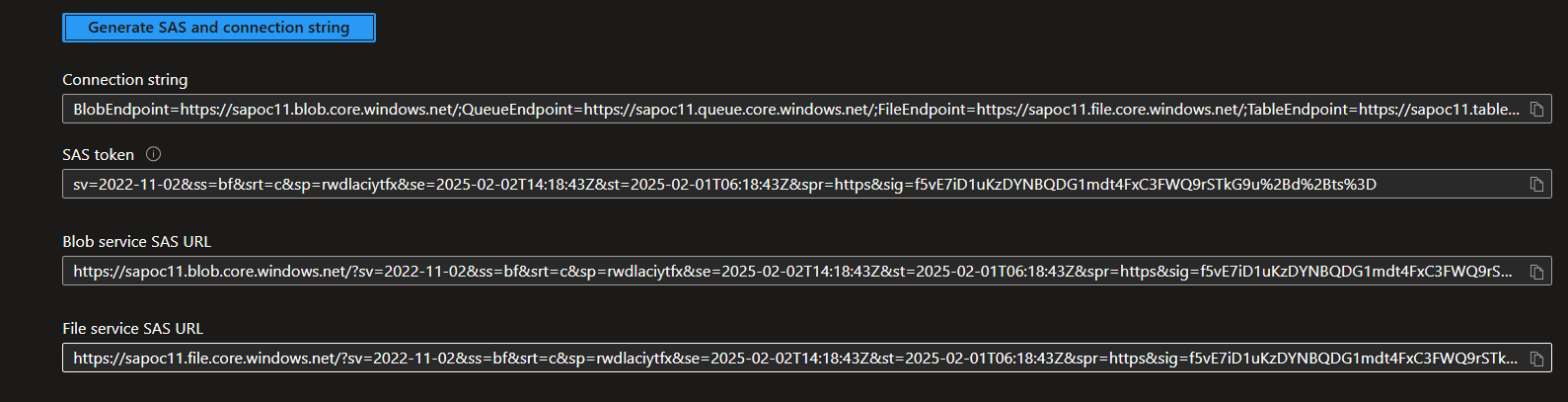
**Step 9**: Configuring Network access restricitions.

Go to Networking > Allow public (or) private access.

* **Enable public access.**
* **Set firewalls and virtual networks.** And then click on save.

**Step 10:** SAS: Shared access Signatures.

Storage Account > SAS

**Step 11:** Access Keys.

Security > Networking > Access keys

