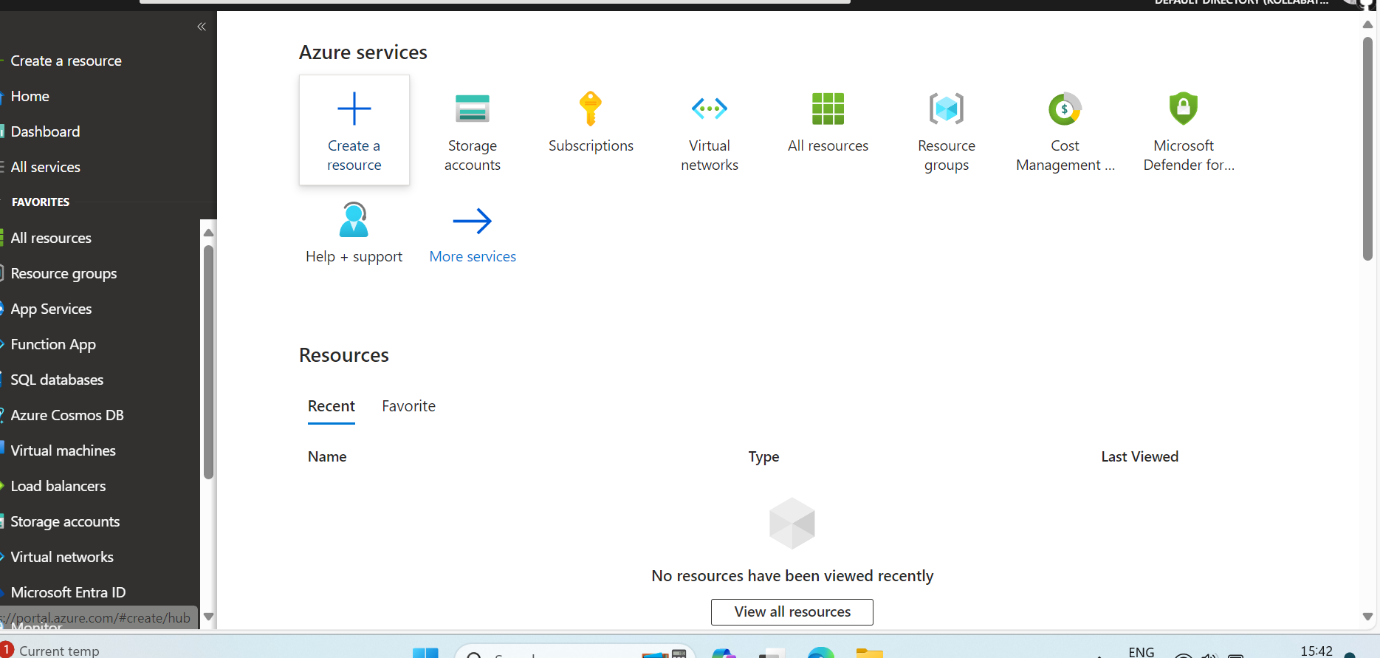
**Create a Storage account in any cloud Azure and try securing it:**

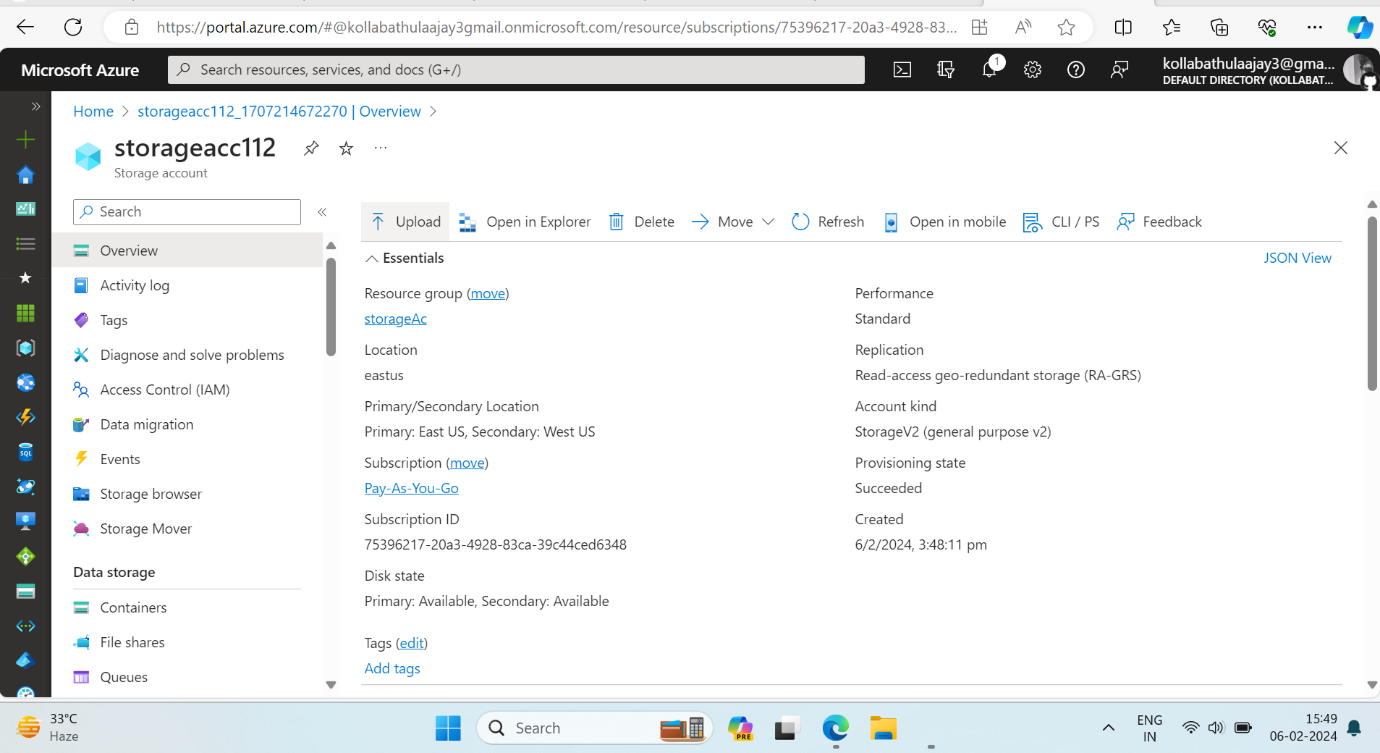
**1.Created a new Storage Account:**

Search for "Storage account" and select it



Click on "Create" to begin to a new storage account

Resource group-storageAC, Storage account name-storageacc112, Location-east us, Performance-standard, Account kind-storageV2(general purpose V2), Replication-Read-Access geo-redundant storage(RA-GRS), and Access tier.

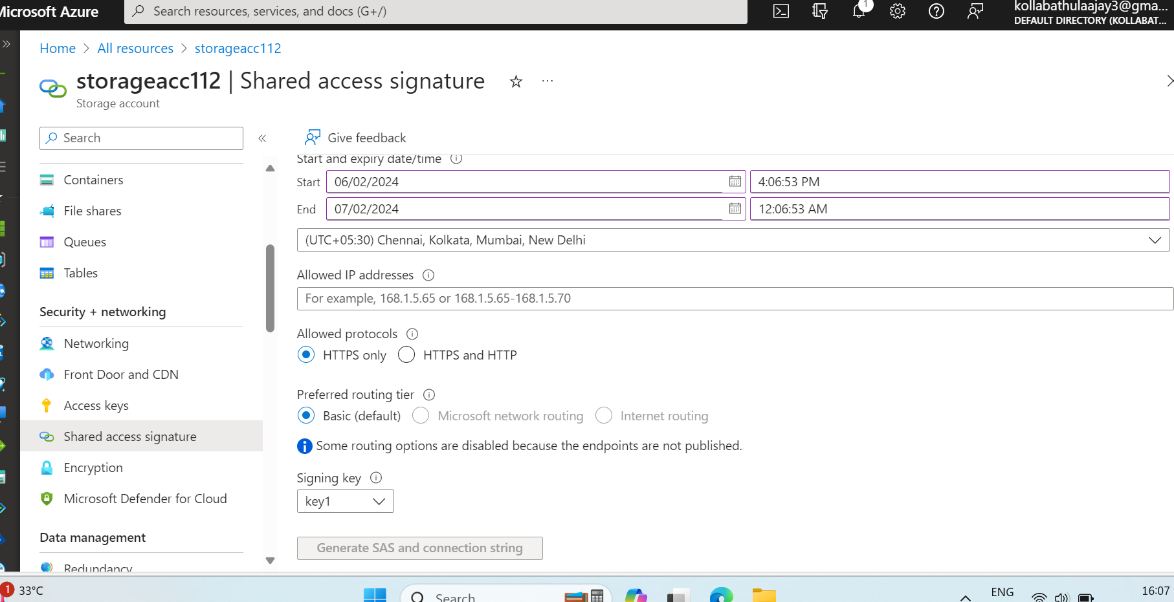


­­Click on "Review + create" and "Create" to create the storage account

**Securing the Azure Storage Account:**

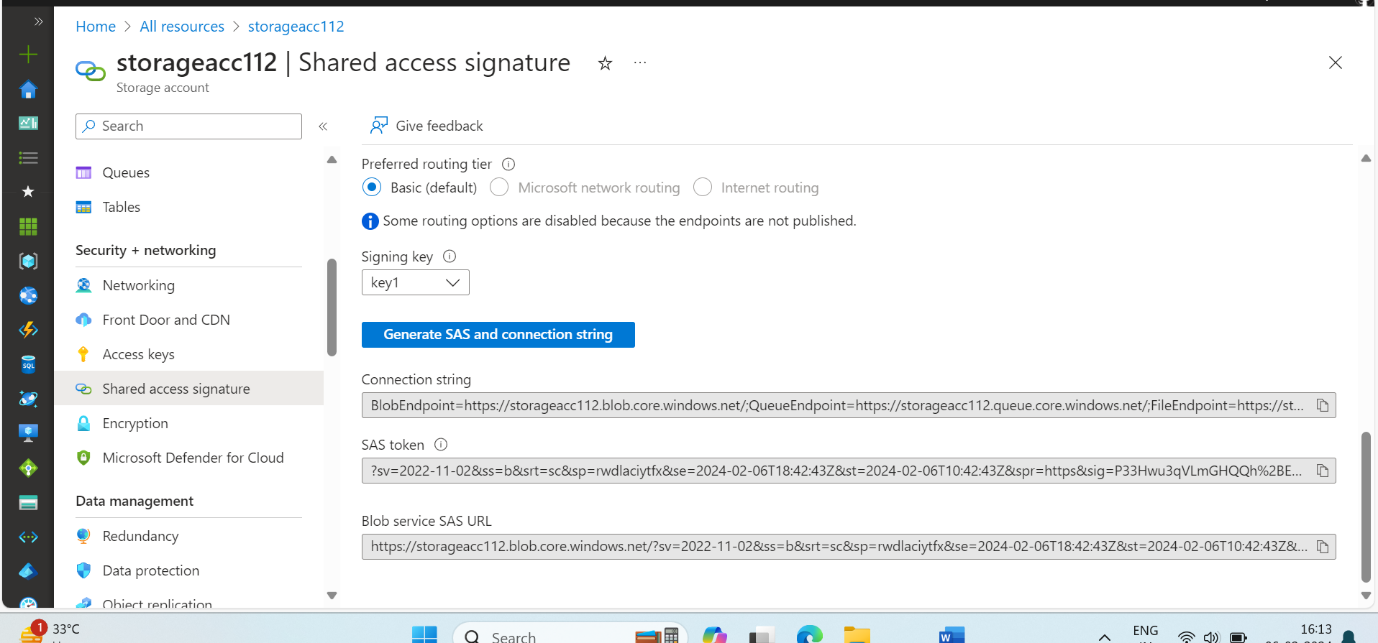
Ensure that only secure connections are allowed by enabling HTTPS for your storage account. By default, Azure Storage requires secure transfer (HTTPS) for all storage Account

**Shared Access Signatures (SAS):**

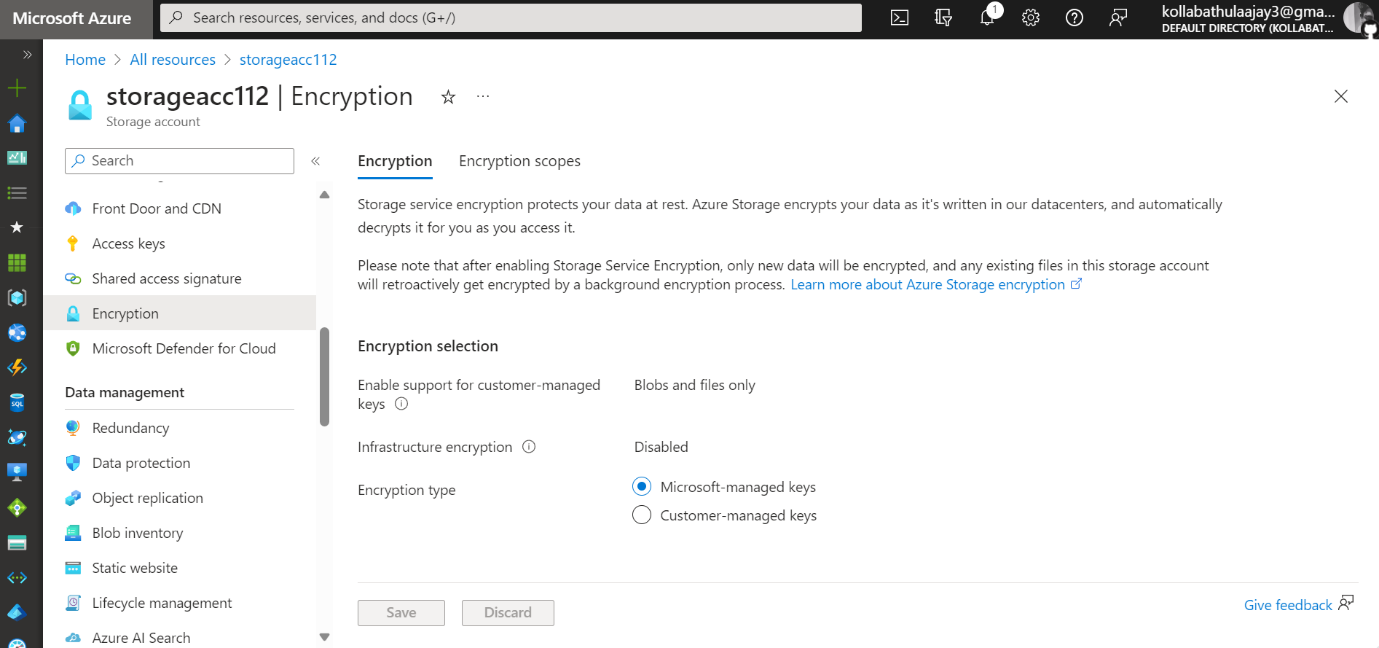
It uses to Share Access Signatures (SAS) to grant limited access to resources in your storage account without sharing your account keys. 

With specific permissions and constraints for the SAS tokens based on your requirement

Generate SAS and connecting to string

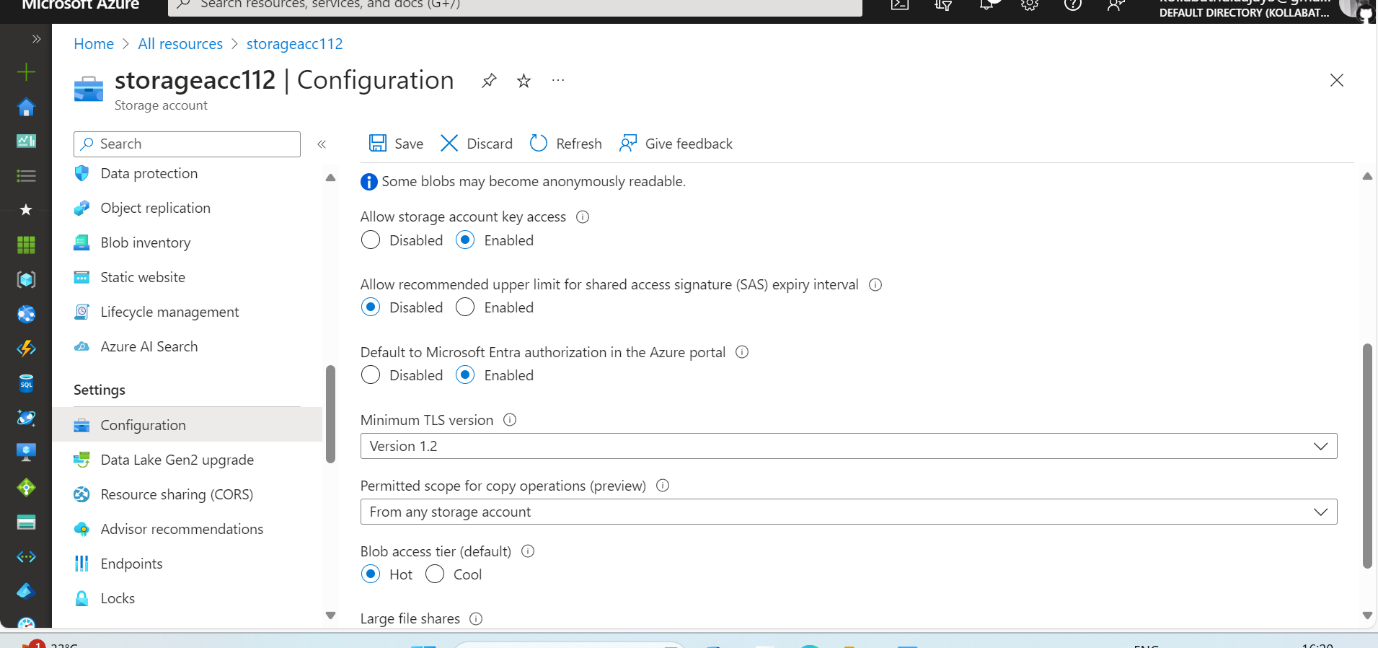


**Encryption**

****Azure Storage automatically encrypts your data at rest.

You can also enable client-side encryption to encrypt data before uploading it to Azure Storage.

**Configuration**

****

Enabled some permissions ,accounts keys