

In this lab, you will learn how to provision a new Azure storage account using the Azure CLI.

Microsoft Azure is a cloud computing service offered and operated by Microsoft. Use this service to host your data and applications in the cloud.

An Azure storage account is an Azure cloud service that contains all of your Azure storage data objects: blobs, file shares, queues, tables, and disks. You can host files, including images, videos, music and binary, as well as noSQL data and messages in the cloud using this service.

An Azure storage account contains all of your Azure storage data objects including blobs, file shares, queues, tables, and VM disks.

Log into the Azure CLI and Azure Portal

Deploy an Azure storage account

Clean up the storage account

Microsoft Azure is a cloud computing service offered and operated by Microsoft that can be used to host your data and applications in the cloud.

Use the following credentials to login to the Azure CLI:

```
az login -u $username -p $password
```

So what's next? Let's create an Azure storage account. This service contains all your Azure storage data objects: blobs, file shares, queues, tables, and disks.

Step 2: Provision a New Azure Storage Account

The following command deploys an Azure storage account to your allocated Azure resource group:

```
az storage account create -n $storageAccountName --resource-group $resource --sku Standard_LRS
```

The command specifies the name for your storage account, \$storageAccountName, as well as the pricing SKU.

```
DBCr3CN3iHGKhaL0
$ az storage account create -n $storageAccountName --resource-group $resource --sku Standard_LRS
The public access to all blobs or containers in the storage account will be disallowed by default in the future, which means de
s still null but will be equivalent to false.
{
  "accessTier": "Hot",
  "allowBlobPublicAccess": true,
  "allowCrossTenantReplication": null,
  "allowSharedKeyAccess": null,
  "allowedCopyScope": null,
  "azureFilesIdentityBasedAuthentication": null,
  "blobPublicAccess": null
}
```

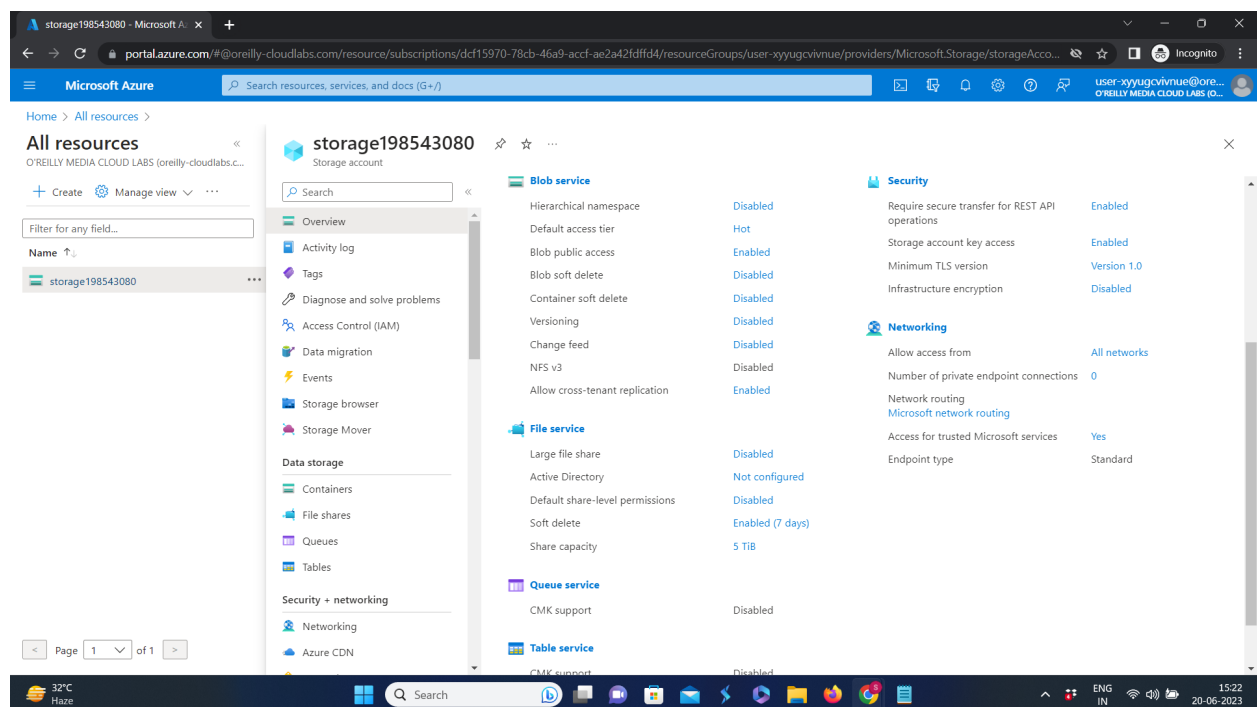
https://learn.microsoft.com/en-us/rest/api/storagerp/srp_sku_types

Step 3: List All Storage Accounts in your Resource Group

se the following command to confirm that the new storage account is created within your allocated resource group:

```
az storage account show -g $resource -n $storageAccountName
```

```
$ az storage account show -g $resource -n $storageAccountName
{
  "accessTier": "Hot",
  "allowBlobPublicAccess": true,
  "allowCrossTenantReplication": null,
  "allowSharedKeyAccess": null,
  "allowedCopyScope": null,
  "azureFilesIdentityBasedAuthentication": null,
  "blobRestoreStatus": null,
  "creationTime": "2023-06-20T09:46:16.792666+00:00",
  "customDomain": null,
  "defaultToOAuthAuthentication": null,
  "dnsEndpointType": null
```



Step 5: Delete the Storage Account

Use the following command to clean up the storage accounts from your allocated resource group:

az storage account delete -n \$storageAccountName -g \$resource

Use the following command to list all storage accounts in your allocated resource group:

az storage account list -g \$resource

```
password: Bb1P3CN3H0K4aB0
$ az storage account delete -n $storageAccountName -g $resource
Are you sure you want to perform this operation? (y/n): y
$ az storage account list -g $resource
[]
$
```