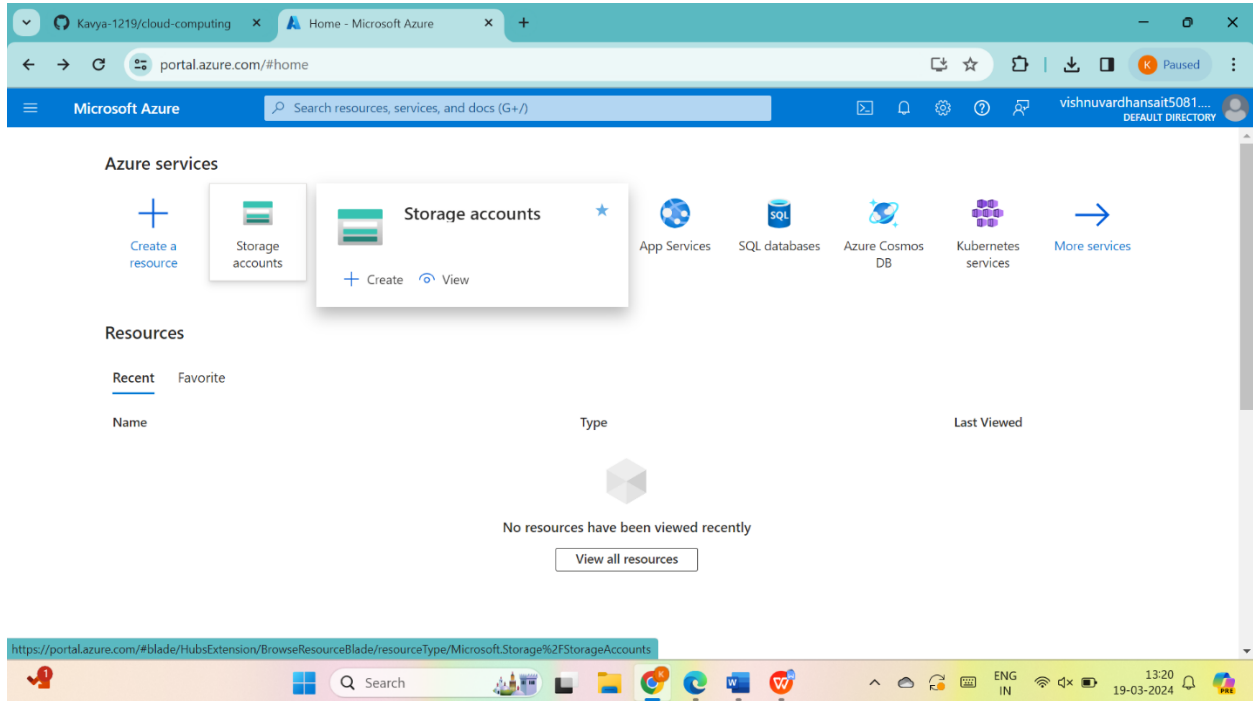


EXPERIMENT:22:

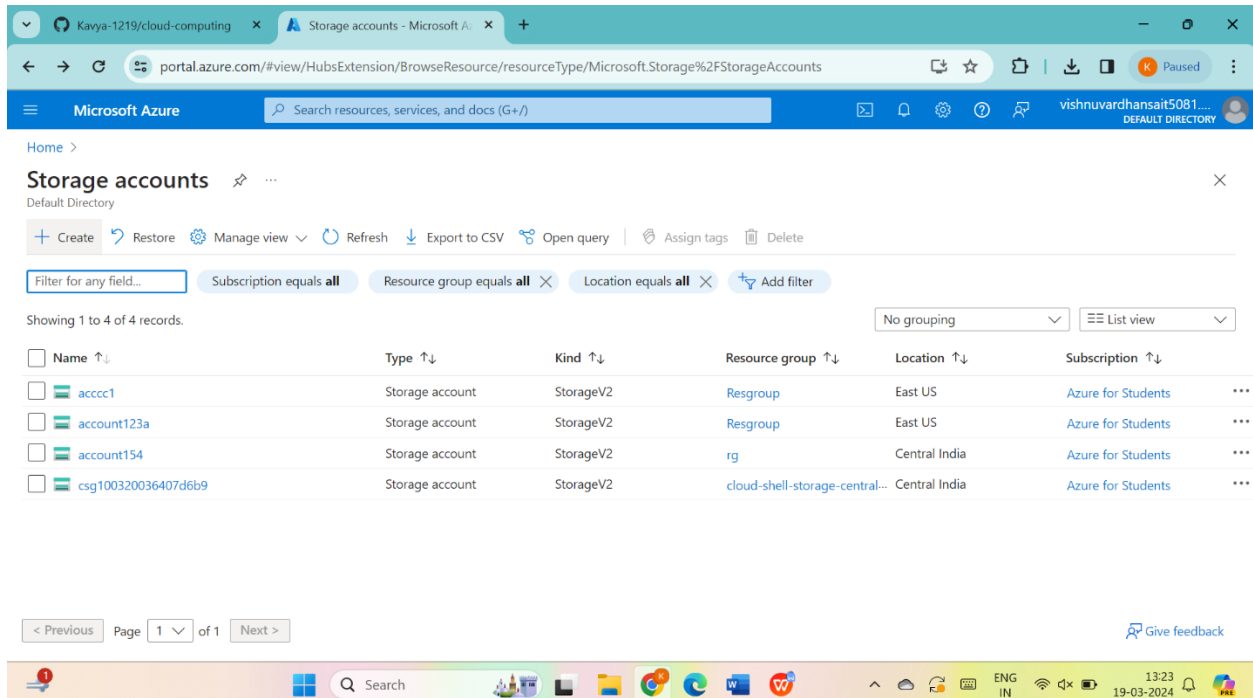
Aim: To Create a Storage service using any Public Cloud Service Provider (Azure/GCP/AWS) and check the public accessibility of the stored file to demonstrate Storage as a Service.

Implementation:

STEP:1:: open azure and create account Go to resource groups



THEN GO THE CREATE THEN



Assign name to storage account and give next

The screenshot shows the 'Create a storage account' page in the Microsoft Azure portal. The browser address bar shows 'portal.azure.com/#create/Microsoft.StorageAccount-ARM'. The page title is 'Create a storage account'. The 'Subscription' is 'Azure for Students' and the 'Resource group' is 'cloud-shell-storage-centralindia'. Under 'Instance details', the 'Storage account name' is 'exp2', the 'Region' is '(Asia Pacific) Central India', the 'Performance' is 'Standard: Recommended for most scenarios (general-purpose v2 account)', and the 'Redundancy' is 'Geo-redundant storage (GRS)'. At the bottom, there are buttons for 'Previous', 'Next', and 'Review + create'. A 'Give feedback' link is also present.

Subscription * Azure for Students

Resource group * cloud-shell-storage-centralindia
[Create new](#)

Instance details

Storage account name * exp2

Region * (Asia Pacific) Central India
[Deploy to an edge zone](#)

Performance * ☒ Standard: Recommended for most scenarios (general-purpose v2 account)
☐ Premium: Recommended for scenarios that require low latency.

Redundancy * Geo-redundant storage (GRS)

[Previous](#) [Next](#) [Review + create](#) [Give feedback](#)

give next for advanced

The screenshot shows the 'Create a storage account' page in the Microsoft Azure portal, with the 'Advanced' tab selected. The 'Security' section is visible, with the following settings: 'Require secure transfer for REST API operations' is checked, 'Allow enabling anonymous access on individual containers' is unchecked, 'Enable storage account key access' is checked, 'Default to Microsoft Entra authorization in the Azure portal' is unchecked, 'Minimum TLS version' is 'Version 1.2', and 'Permitted scope for copy operations' is 'From any storage account'. At the bottom, there are buttons for 'Previous', 'Next', and 'Review + create'. A 'Give feedback' link is also present.

Basics **Advanced** Networking Data protection Encryption Tags Review + create

Security
Configure security settings that impact your storage account.

Require secure transfer for REST API operations ☒

Allow enabling anonymous access on individual containers ☐

Enable storage account key access ☒

Default to Microsoft Entra authorization in the Azure portal ☐

Minimum TLS version * Version 1.2

Permitted scope for copy operations * From any storage account

[Previous](#) [Next](#) [Review + create](#) [Give feedback](#)

give next for networking

The screenshot shows the 'Create a storage account' page in the Microsoft Azure portal, specifically the 'Networking' tab. The page is titled 'Create a storage account' and has a breadcrumb trail 'Home > Storage accounts >'. The 'Networking' tab is selected, and the 'Network connectivity' section is visible. It explains that you can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint. Under 'Network access', there are three radio button options: 'Enable public access from all networks' (selected), 'Enable public access from selected virtual networks and IP addresses', and 'Disable public access and use private access'. A note indicates that enabling public access from all networks might make the resource available publicly and recommends using a more restricted access type. Below this, the 'Network routing' section is visible, and at the bottom, there are 'Previous', 'Next', and 'Review + create' buttons, along with a 'Give feedback' link.

Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Storage accounts >

Create a storage account

Basics Advanced **Networking** Data protection Encryption Tags Review + create

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access *

☒ Enable public access from all networks

☐ Enable public access from selected virtual networks and IP addresses

☐ Disable public access and use private access

i Enabling public access from all networks might make this resource available publicly. Unless public access is required, we recommend using a more restricted access type. [Learn more](#)

Network routing

Previous Next **Review + create**

[Give feedback](#)

give next for data protection

The screenshot shows the 'Create a storage account' page in the Microsoft Azure portal, specifically the 'Data protection' tab. The page is titled 'Create a storage account' and has a breadcrumb trail 'Home > Storage accounts >'. The 'Data protection' tab is selected, and the 'Recovery' section is visible. It explains that you can protect your data from accidental or erroneous deletion or modification. Under 'Recovery', there are three checkboxes: 'Enable point-in-time restore for containers' (unchecked), 'Enable soft delete for blobs' (checked), and 'Enable soft delete for containers' (checked). The 'Enable soft delete for blobs' option has a note that soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. Below this, there is a 'Days to retain deleted blobs' field with a value of 7. The 'Enable soft delete for containers' option has a note that soft delete enables you to recover containers that were previously marked for deletion. At the bottom, there are 'Previous', 'Next', and 'Review + create' buttons, along with a 'Give feedback' link.

Microsoft Azure

Search resources, services, and docs (G+/I)

Home > Storage accounts >

Create a storage account

Basics Advanced Networking **Data protection** Encryption Tags Review + create

Recovery

Protect your data from accidental or erroneous deletion or modification.

☐ Enable point-in-time restore for containers

Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. [Learn more](#)

☒ Enable soft delete for blobs

Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. [Learn more](#)

Days to retain deleted blobs ⓘ

☒ Enable soft delete for containers

Soft delete enables you to recover containers that were previously marked for deletion. [Learn more](#)

Previous Next **Review + create**

[Give feedback](#)

give next for encryption

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal. The 'Encryption' tab is selected, showing options for encryption type and infrastructure encryption.

Encryption type *

- ☒ Microsoft-managed keys (MMK)
- ☐ Customer-managed keys (CMK)

Enable support for customer-managed keys

- ☒ Blobs and files only
- ☐ All service types (blobs, files, tables, and queues)

⚠ This option cannot be changed after this storage account is created.

Enable infrastructure encryption ☐

Navigation buttons: Previous, Next, Review + create. A 'Give feedback' link is also present.

give next for tags

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal. The 'Tags' tab is selected, showing a table for adding tags.

Name	Value	Resource
BBB	10	All resources selected
		All resources selected

Navigation buttons: Previous, Next, Review + create. A 'Give feedback' link is also present.

give next for review + create and go to create

The screenshot shows the 'Create a storage account' page in the Azure portal. The 'Review + create' tab is selected. The page displays the configuration details for the storage account 'exp22' in the 'cloud-shell-storage-centralindia' resource group. The configuration includes: Subscription: Azure for Students, Resource group: cloud-shell-storage-centralindia, Location: Central India, Storage account name: exp22, Performance: Standard, and Replication: Read-access geo-redundant storage (RA-GRS). The 'Advanced' section shows 'Enable hierarchical namespace' is disabled. At the bottom, there are 'Previous', 'Next', and 'Create' buttons. The 'Create' button is highlighted in blue. The Windows taskbar at the bottom shows the time as 13:27 on 19-03-2024.

Now the deployment is completed

The screenshot shows the 'exp22_1710835050310 | Overview' page in the Azure portal. The page displays the deployment details for the storage account. A green checkmark icon indicates that the deployment is complete. The deployment name is 'exp22_1710835050310', the subscription is 'Azure for Students', and the resource group is 'cloud-shell-storage-centr...'. The deployment details section shows the start time as 3/19/2024, 1:27:43 PM and the correlation ID as f82ebc52-6ff9-4eda-ad2f-eae6c81d3320. A 'Go to resource' button is visible. A notification banner at the top right states 'Deployment succeeded' and 'Deployment 'exp22_1710835050310' to resource group 'cloud-shell-storage-centralindia' was successful.' The Windows taskbar at the bottom shows the time as 13:28 on 19-03-2024.

Go to storage browser >file shares and add file

The screenshot shows the Microsoft Azure portal interface for the 'exp22' storage account. The left sidebar contains navigation links for Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser (selected), Storage Mover, Data storage, Containers, File shares, and Queues. The main content area displays the 'exp22' storage account overview, including a search bar, a list of resources (Favorites, Recently viewed, Blob containers, File shares, kugfbb, Queues, Tables), and a table of file shares. The 'File shares' section shows a table with one item: 'kugfbb', which is Transaction optimized, created on 19/03/2024 at 13:31:37, and has a quota of 5 TiB.

Name	Tier	Modified	Quota
kugfbb	Transaction optimized	19/03/2024, 13:31:37	5 TiB

Upload any file into it

The screenshot shows the Microsoft Azure portal interface for the 'exp22' storage account, with the 'Upload files' dialog box open. The dialog box has a title bar 'Upload files' and a close button. It contains a large dashed box with a cloud upload icon and the text 'Drag and drop files here or Browse for files'. Below this, there is a checkbox for 'Overwrite if files already exist' and an 'Upload' button. The 'Current uploads' section shows a progress bar for 'exp 2 cloud.docx' with a green checkmark and the text '1.98 MiB / 1.98 MiB'. The background shows the same storage account overview as the previous screenshot.

RESULT : THUS ,THE PROGRAM HAS BEEN EXCEUTED SUCCESSFULLY.

The screenshot shows the Microsoft Azure portal interface for a storage account named 'exp22'. The left sidebar contains navigation options: Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser (selected), Storage Mover, Data storage, Containers, File shares, and Queues. The main content area shows the 'exp22' Storage browser. It includes a search bar, a list of file shares (kugfbb), and a table of files. The table has columns for Name, Type, and Size. The file 'exp 2 cloud.docx' is listed with a size of 1.98 MiB.

exp22 | Storage browser

Storage account

Search

exp22

File shares > kugfbb

Authentication method: Access key (Switch to Microsoft Entra user account)

Search files by prefix

Showing all 1 items

Name	Type	Size
exp 2 cloud.docx	File	1.98 MiB