Name: Harsh Chheda

Roll Number: 31031521005 / 22-15405

Class: Msc. Computer Science

Subject: Cloud Computing

Year: 2022-23

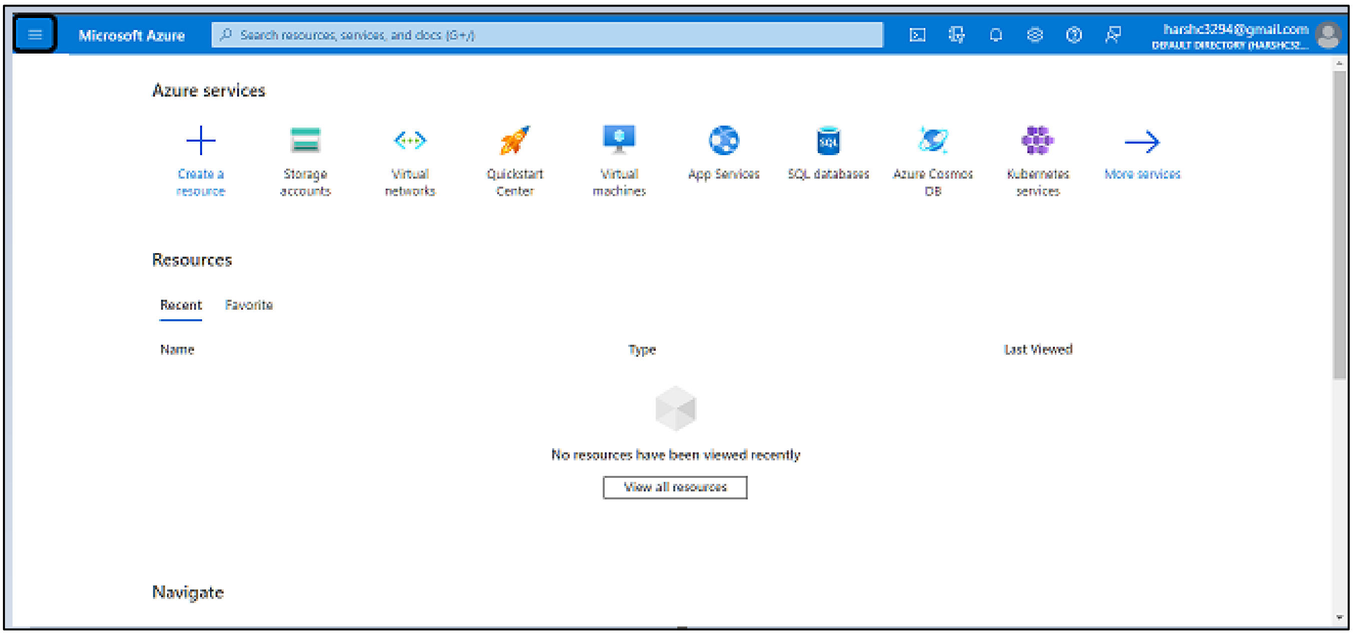
Practical 3

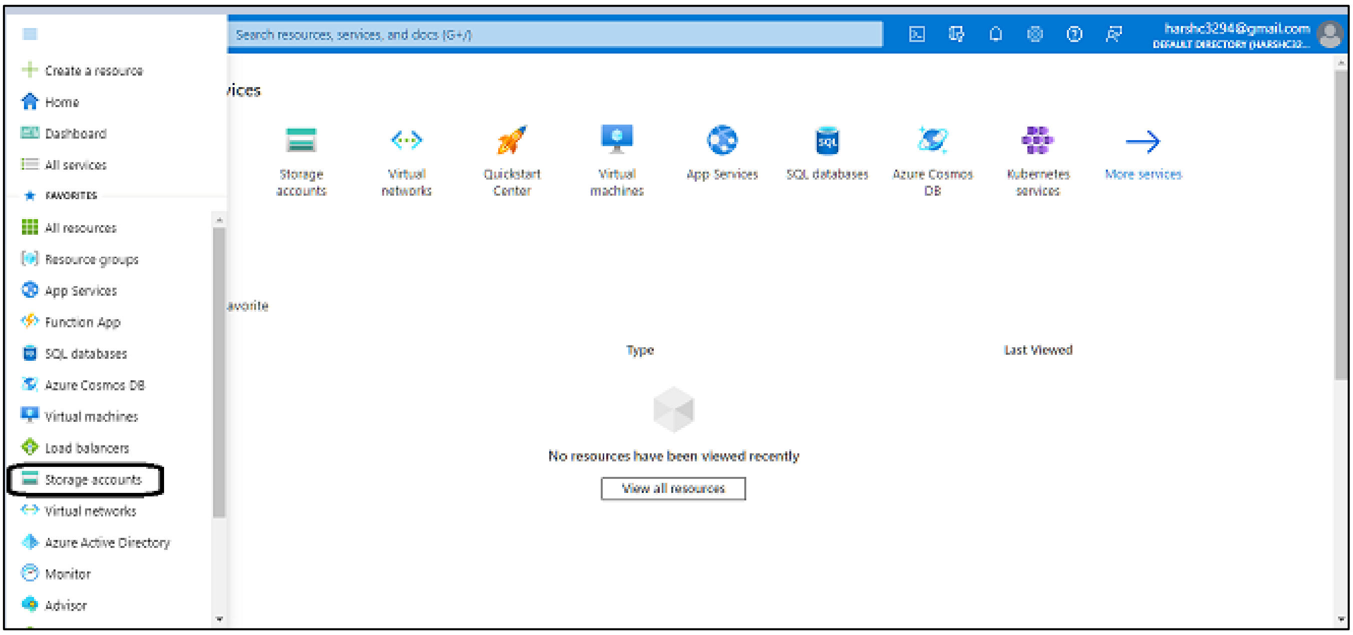
Aim: Demonstration of IaaS cloud

Code:

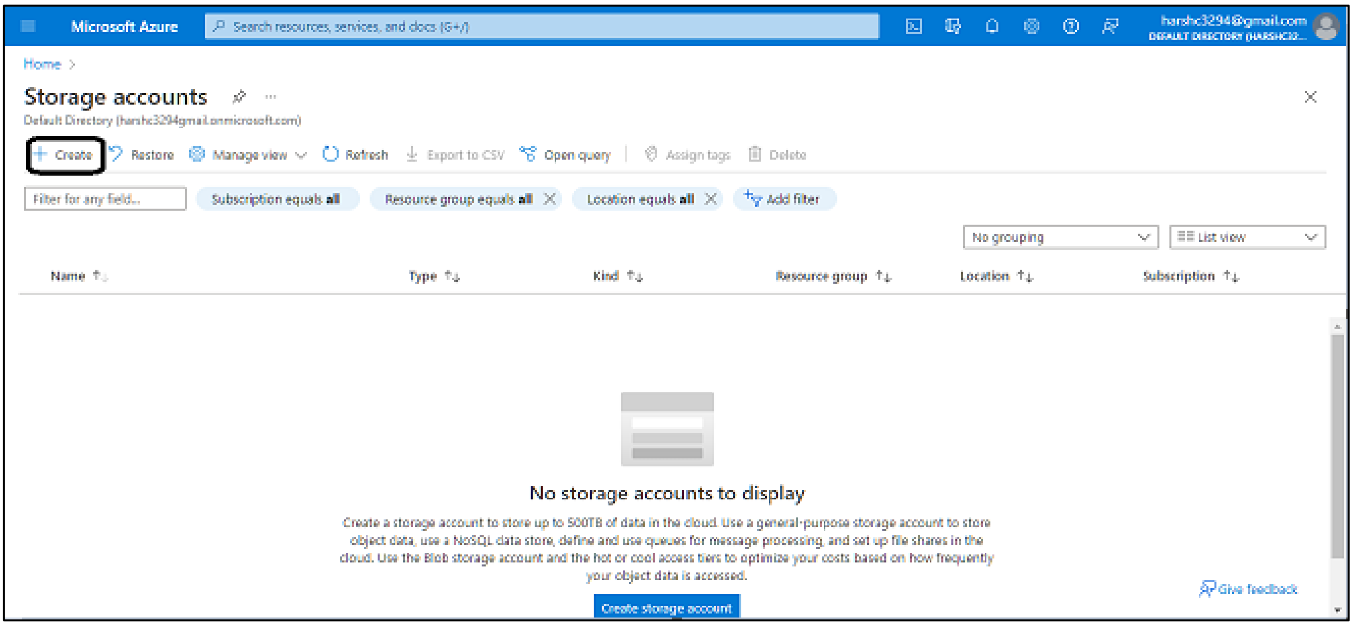
To create an Azure storage account with the Azure portal, follow these steps

1. From the left portal menu, select Storage accounts to display a list of your storage accounts. If the portal menu isn't visible, click the menu button to toggle it on.





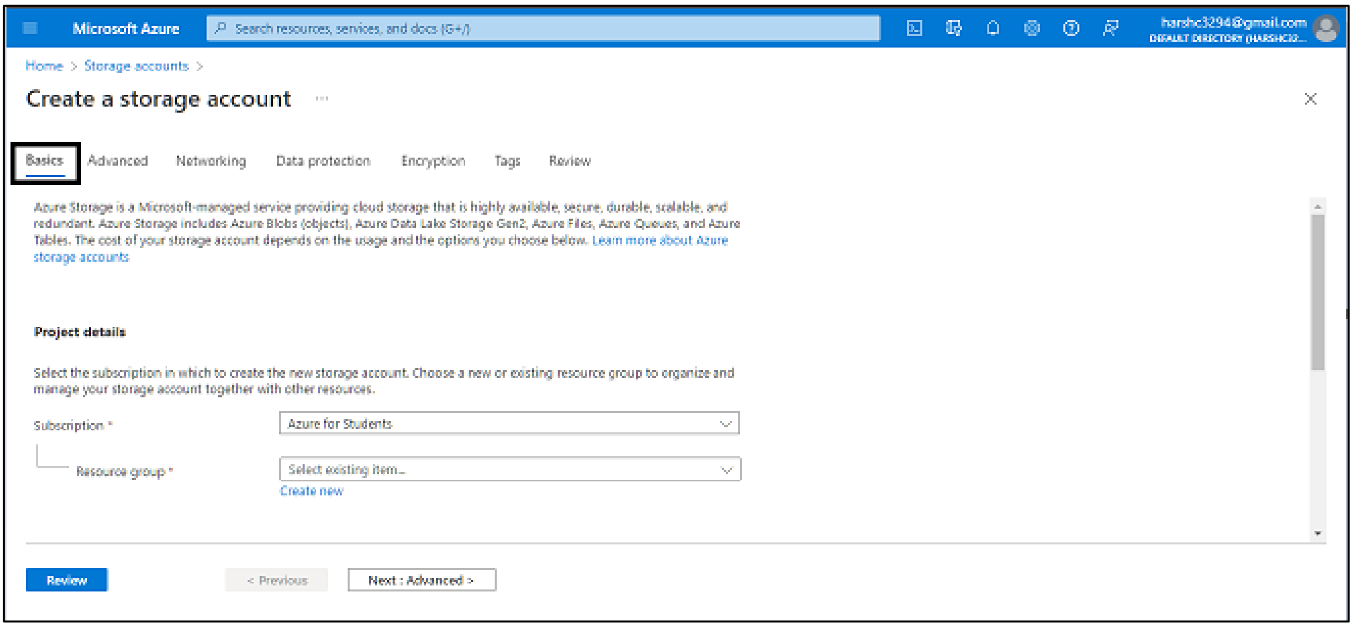
2. On the **Storage accounts** page, select **Create**



No storage accounts to display

Create a storage account to store up to 500TB of data in the cloud. Use a general-purpose storage account to store object data, use a NoSQL data store, define and use queues for message processing, and set up file shares in the cloud. Use the Blob storage account and the hot or cool access tiers to optimize your costs based on how frequently your object data is accessed.

3. The following image shows a standard configuration of the basic properties for a new storage account.



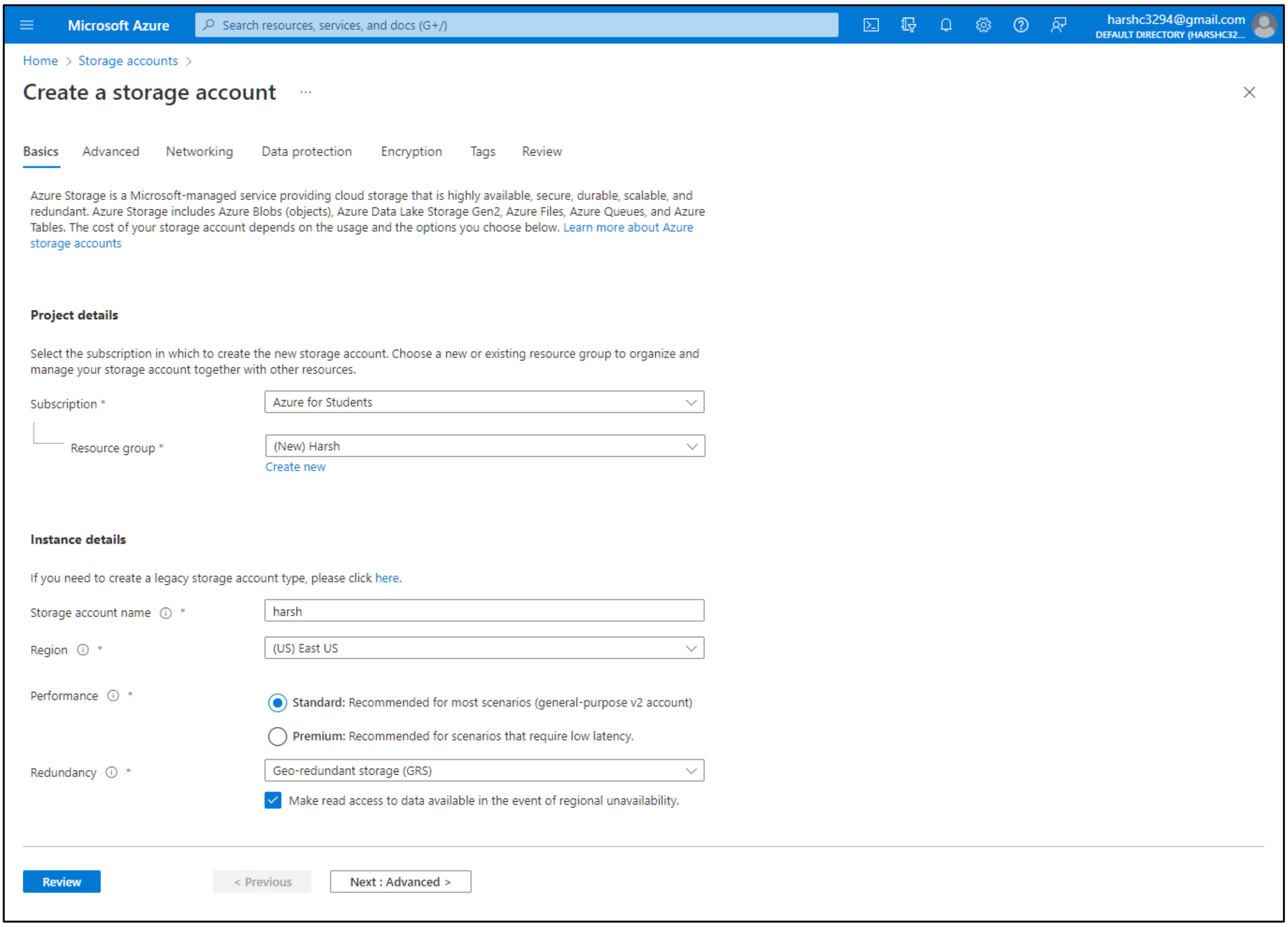
Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. Learn more about Azure storage accounts

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * Azure for Students

Resource group * Select existing item...


Microsoft Azure
Search resources, services, and docs (G+/)
harshc3294@gmail.com
DEFAULT DIRECTORY (HARSHC32...
Home > Storage accounts >

Create a storage account

Basics Advanced Networking Data protection Encryption Tags Review

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. Learn more about Azure storage accounts

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Subscription * : Azure for Students

Resource group * : (New) Harsh
Create new

Instance details

If you need to create a legacy storage account type, please click here.

Storage account name * : harsh

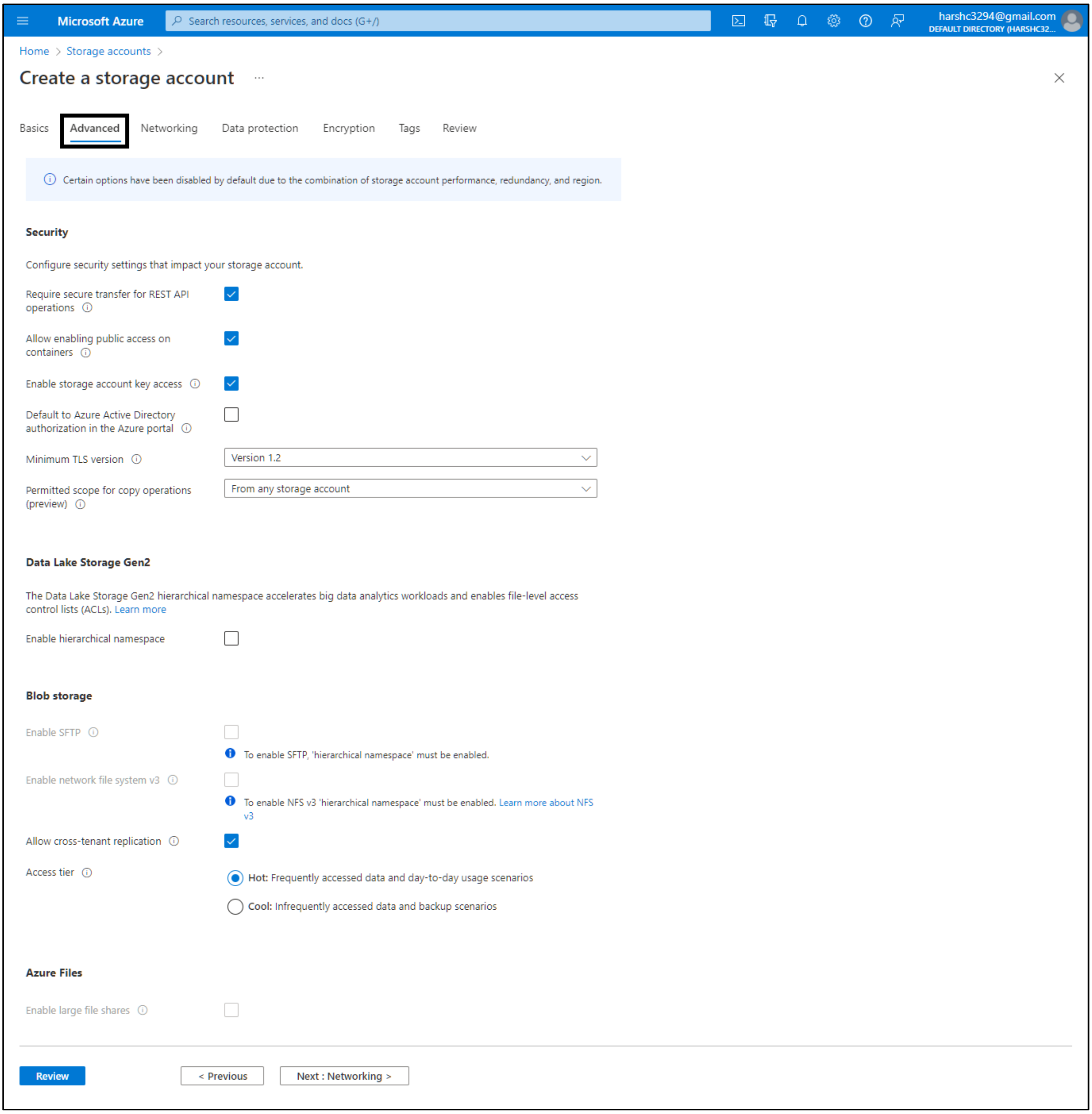
Region * : (US) East US

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

Redundancy * : Geo-redundant storage (GRS)

☑ Make read access to data available in the event of regional unavailability.

4. The following image shows a standard configuration of the advanced properties for a new storage account.



Microsoft Azure
Search resources, services, and docs (G+/)
harshc3294@gmail.com
DEFAULT DIRECTORY (HARSHC32...
Home > Storage accounts >

Create a storage account

Basics
Advanced
Networking
Data protection
Encryption
Tags
Review

ⓘ Certain options have been disabled by default due to the combination of storage account performance, redundancy, and region.

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations ⓘ	☑
Allow enabling public access on containers ⓘ	☑
Enable storage account key access ⓘ	☑
Default to Azure Active Directory authorization in the Azure portal ⓘ	□
Minimum TLS version ⓘ	Version 1.2
Permitted scope for copy operations (preview) ⓘ	From any storage account

Data Lake Storage Gen2

The Data Lake Storage Gen2 hierarchical namespace accelerates big data analytics workloads and enables file-level access control lists (ACLs). Learn more

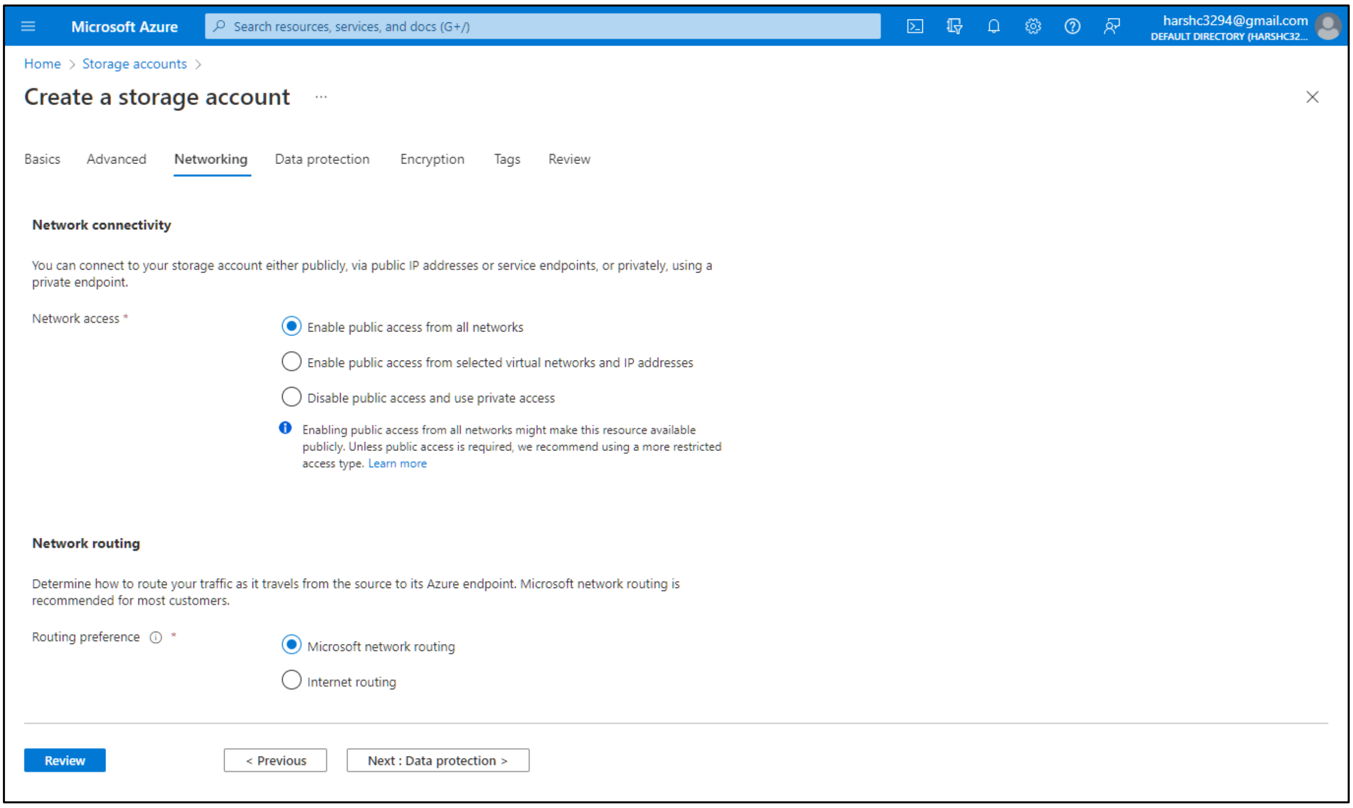
Enable hierarchical namespace	□

Blob storage

Enable SFTP ⓘ	□ To enable SFTP, 'hierarchical namespace' must be enabled.
Enable network file system v3 ⓘ	□ To enable NFS v3 'hierarchical namespace' must be enabled. Learn more about NFS v3
Allow cross-tenant replication ⓘ	☑
Access tier ⓘ	● **Hot:** Frequently accessed data and day-to-day usage scenarios ○ **Cool:** Infrequently accessed data and backup scenarios

Azure Files

Enable large file shares ⓘ	□



Microsoft Azure
Search resources, services, and docs (G+/)
harshc3294@gmail.com
DEFAULT DIRECTORY (HARSHC32...
Home > Storage accounts >

Create a storage account

Basics
Advanced
Networking
Data protection
Encryption
Tags
Review

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

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

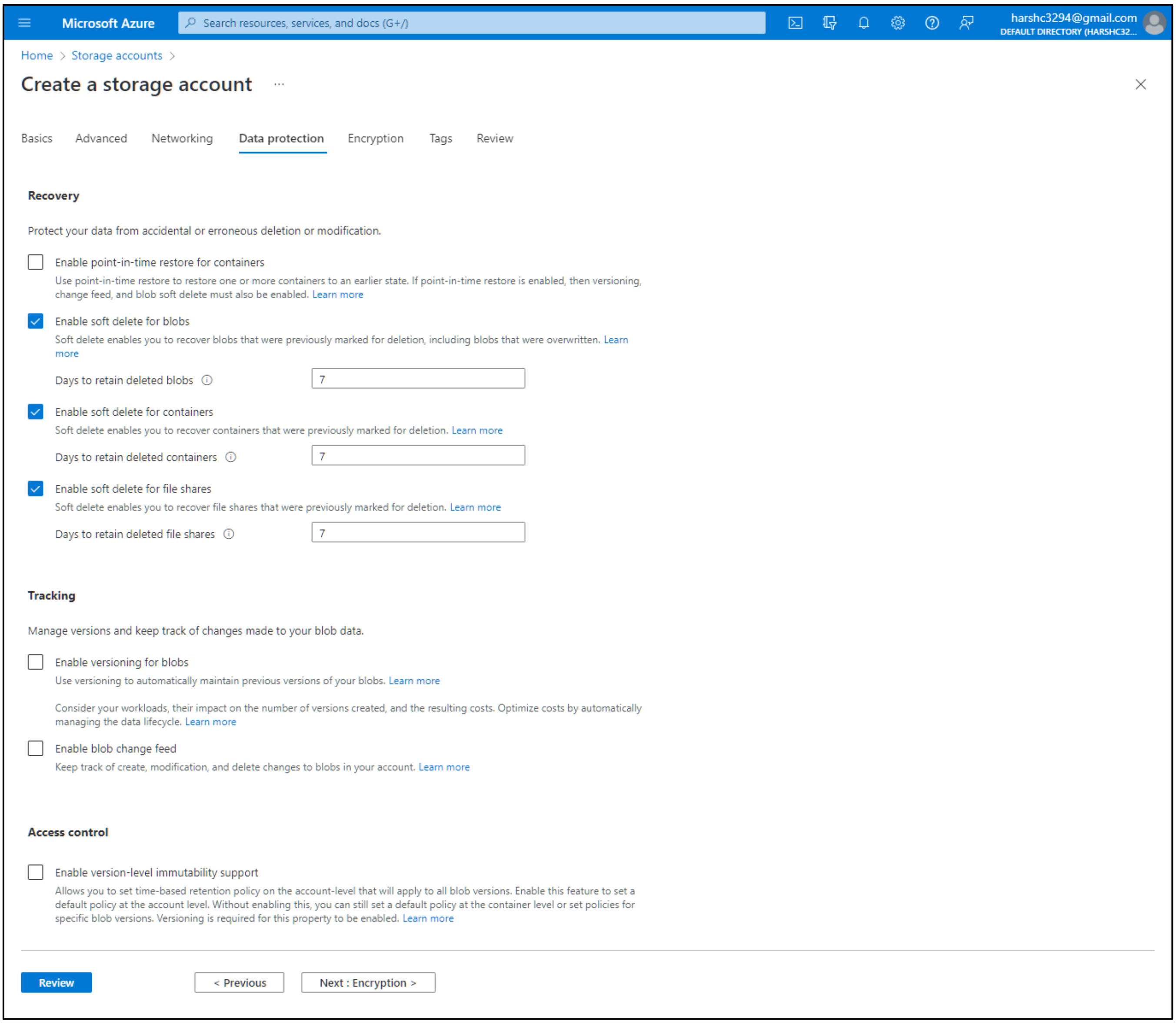
Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference *

● Microsoft network routing

○ Internet routing


Microsoft Azure
Search resources, services, and docs (G+/)
harshc3294@gmail.com
DEFAULT DIRECTORY (HARSHC32...
Home > Storage accounts >

Create a storage account

Basics | Advanced | Networking | **Data protection** | Encryption | Tags | Review

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: 7

☑ Enable soft delete for containers
Soft delete enables you to recover containers that were previously marked for deletion. Learn more

Days to retain deleted containers: 7

☑ Enable soft delete for file shares
Soft delete enables you to recover file shares that were previously marked for deletion. Learn more

Days to retain deleted file shares: 7

Tracking

Manage versions and keep track of changes made to your blob data.

□ Enable versioning for blobs
Use versioning to automatically maintain previous versions of your blobs. Learn more

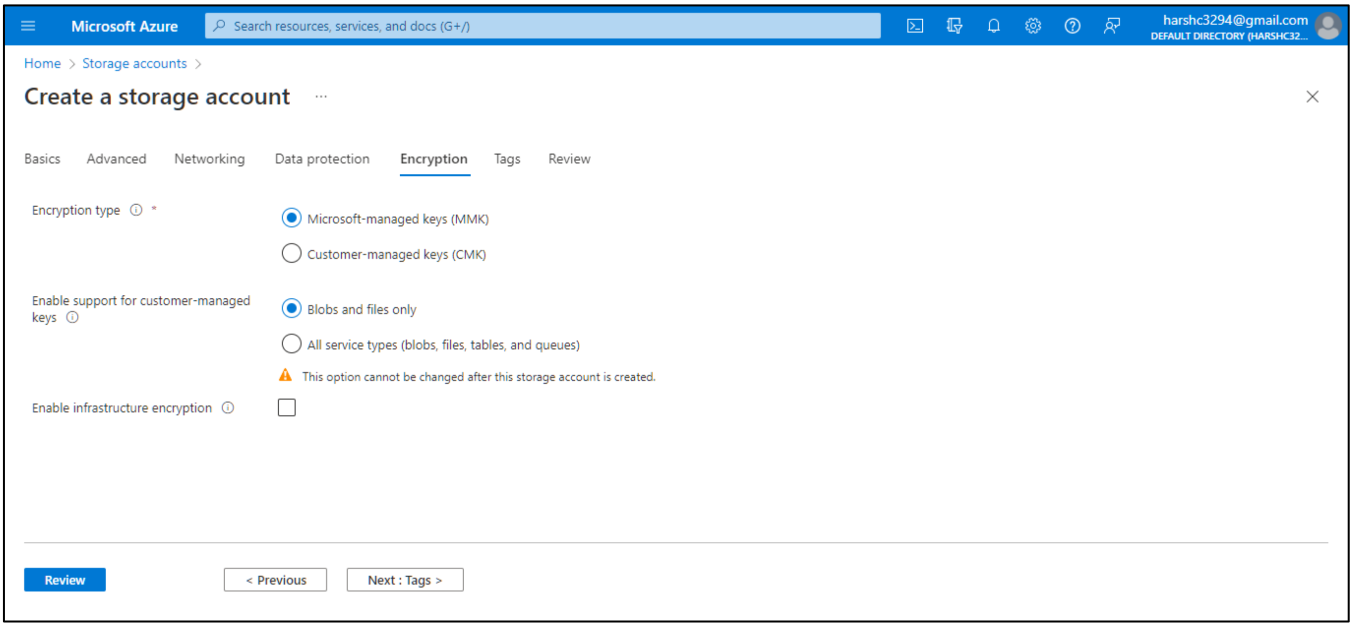
Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle. Learn more

□ Enable blob change feed
Keep track of create, modification, and delete changes to blobs in your account. Learn more

Access control

□ Enable version-level immutability support
Allows you to set time-based retention policy on the account-level that will apply to all blob versions. Enable this feature to set a default policy at the account level. Without enabling this, you can still set a default policy at the container level or set policies for specific blob versions. Versioning is required for this property to be enabled. Learn more

Review
< Previous
Next : Encryption >


Microsoft Azure
Search resources, services, and docs (G+/)
harshc3294@gmail.com
DEFAULT DIRECTORY (HARSHC32...
Home > Storage accounts >

Create a storage account

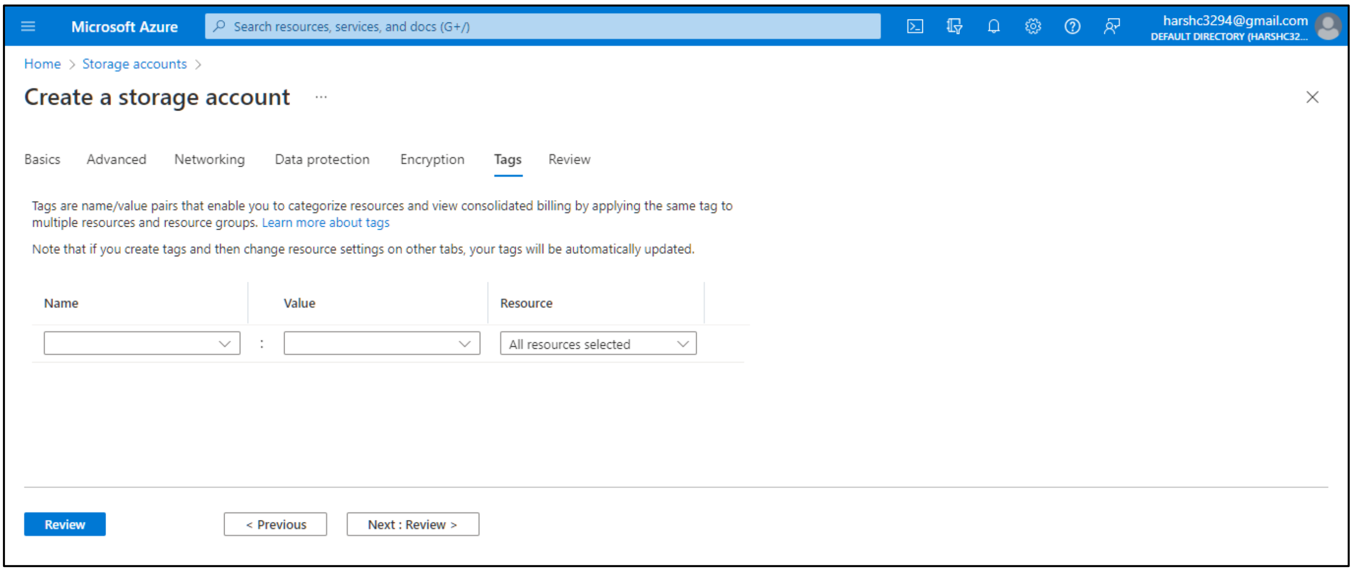
Basics | Advanced | Networking | Data protection | **Encryption** | Tags | Review

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: □


Microsoft Azure
Search resources, services, and docs (G+/)
harshc3294@gmail.com
DEFAULT DIRECTORY (HARSHC32...
Home > Storage accounts >

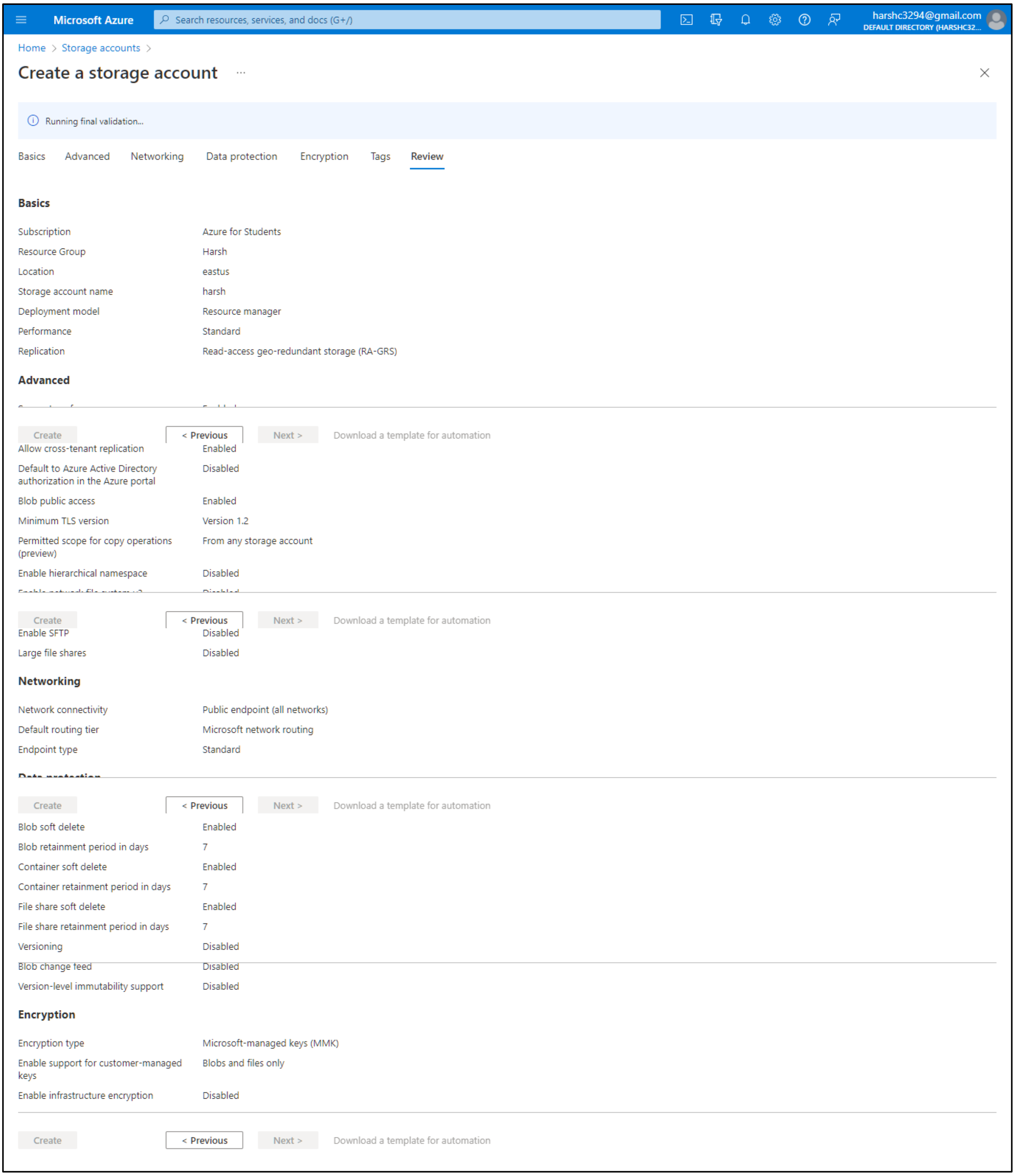
Create a storage account

Basics
Advanced
Networking
Data protection
Encryption
Tags
Review

Tags are name/value pairs that enable you to categorize resources and view consolidated billing by applying the same tag to multiple resources and resource groups. Learn more about tags

Note that if you create tags and then change resource settings on other tabs, your tags will be automatically updated.

Name	Value	Resource
		All resources selected


Microsoft Azure
Search resources, services, and docs (G+/)
harshc3294@gmail.com
DEFAULT DIRECTORY (HARSHC32...
Home > Storage accounts >

Create a storage account

Running final validation...

Basics
Advanced
Networking
Data protection
Encryption
Tags
Review

Basics

Subscription	Azure for Students
Resource Group	Harsh
Location	eastus
Storage account name	harsh
Deployment model	Resource manager
Performance	Standard
Replication	Read-access geo-redundant storage (RA-GRS)

Advanced

Create
< Previous
Next >
Download a template for automation

Allow cross-tenant replication	Enabled
Default to Azure Active Directory authorization in the Azure portal	Disabled
Blob public access	Enabled
Minimum TLS version	Version 1.2
Permitted scope for copy operations (preview)	From any storage account
Enable hierarchical namespace	Disabled

Enable SFTP	Disabled
Large file shares	Disabled

Networking

Network connectivity	Public endpoint (all networks)
Default routing tier	Microsoft network routing
Endpoint type	Standard

Data protection

Blob soft delete	Enabled
Blob retainment period in days	7
Container soft delete	Enabled
Container retainment period in days	7
File share soft delete	Enabled
File share retainment period in days	7
Versioning	Disabled
Blob change feed	Disabled
Version-level immutability support	Disabled

Encryption

Encryption type	Microsoft-managed keys (MMK)
Enable support for customer-managed keys	Blobs and files only
Enable infrastructure encryption	Disabled