

Configuring Azure Storage

Jan 2026

C. Cook
github.com/nelcook11

Configured Azure Storage to meet the following key requirements:

- **Store and manage unstructured data-** Handle files such as images and documents efficiently
 - **Ensure data security-** Protect sensitive customer information through encryption and secure access methods
 - **Optimize cost and performance-** Implement tiered storage solutions to balance performance with cost-effectiveness
1. Designed an Azure Storage Account aligned to workload and performance needs
 2. Organized unstructured data using containers for efficient management
 3. Enforced encryption and secure access controls to safeguard sensitive information
 4. Automated lifecycle rules to move data between storage tiers based on usage patterns

Select “storage accounts”

The screenshot shows the Microsoft Azure portal interface. At the top, the navigation bar includes the Microsoft Azure logo, an 'Upgrade' button, a search bar containing 'storage accounts', and a Copilot icon. Below the navigation bar, the main content area is divided into sections: 'Azure services', 'Resources', and 'Last Viewed'.

Azure services

- Create a resource
- Virtual networks
- Microsoft Sentinel
- Billing access control (IAM)
- More services

Resources

Recent Favorite

Name

- NetworkWatcherRG
- Azure subscription 1

See all

Search results for 'storage accounts'

All Services (24) More (5)

Services [See more](#)

- Storage accounts (classic)
- Storage accounts
- Azure Storage Actions PREVIEW
- Discounts

Marketplace

- Storage account
- Storage task - Azure Storage Actions
- Azure Storage Mover

Documentation [See more](#)

- Authorize access to blobs using Microsoft Entra ID - ...
- Continue searching in Microsoft Entra ID

Searching all subscriptions. [Give feedback](#)

Last Viewed

Name	Last Viewed
Authorize access to blobs using Microsoft Entra ID - ...	4 days ago
Continue searching in Microsoft Entra ID	4 days ago

Select “Create”

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a Copilot icon. Below the header, the main content area is titled 'Storage center | Blob Storage' with a subtitle 'Default Directory (nelcook11gmail.onmicrosoft.com)'. A search bar is present. On the left, there's a navigation pane with links to Overview, All storage resources, Object storage, File storage, Block storage, Data management, Migration, Partner solutions, Management services, and Help. The main content area has tabs for 'Summary' and 'Resources'. The 'Resources' tab is active, and the '+ Create' button is highlighted with a red box. Below the tabs, there's a message: 'You are viewing a new version of Browse experience. Click here to access the old experience.' Below this, there's a filter bar with 'Subscription equals all', 'Resource Group equals all', and 'Location equals all'. A large message in the center says 'No storage accounts to display' with a subtext explaining how to create a storage account. At the bottom, there's a 'Showing 1 - 0 of 0. Display count: auto' and a 'Give feedback' link.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home

Storage center | Blob Storage
Default Directory (nelcook11gmail.onmicrosoft.com)

Which storage accounts have unused or inactive containers? +2

Search

Summary Resources

+ Create Restore Manage view Refresh Export to CSV Open query Group by none

You are viewing a new version of Browse experience. Click here to access the old experience.

Filter for any field...

Subscription equals all Resource Group equals all Location equals all + Add filter

No storage accounts to display

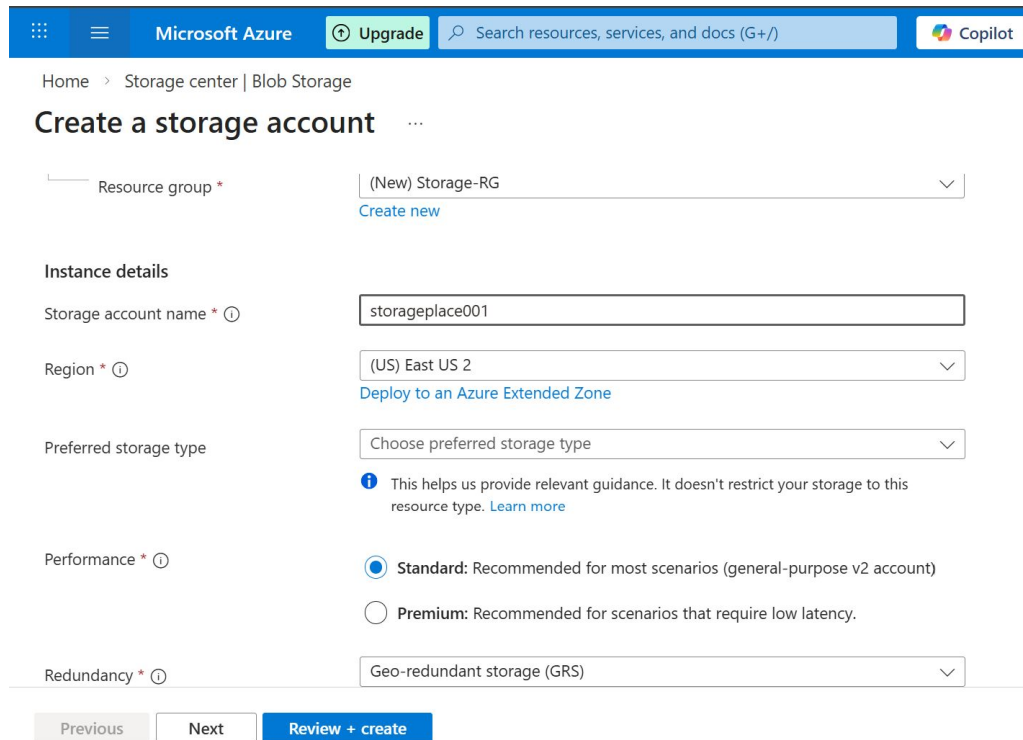
Create a storage account to store up to 500TB of data in the cloud. Use a general-purpose storage account to store object data, use a NoSQL data store, define and use queues for message processing, and set up file shares in the cloud. Use the Blob storage account and the hot or cool access tiers to optimize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

Showing 1 - 0 of 0. Display count: auto

Give feedback

<https://portal.azure.com/?l=en-en-us#nift+F>

Fill in the required fields



Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Storage center | Blob Storage

Create a storage account

Resource group * (New) Storage-RG [Create new](#)

Instance details

Storage account name * ① storageplace001

Region * ① (US) East US 2 [Deploy to an Azure Extended Zone](#)

Preferred storage type Choose preferred storage type

① This helps us provide relevant guidance. It doesn't restrict your storage to this resource type. [Learn more](#)

Performance * ①

☒ **Standard:** Recommended for most scenarios (general-purpose v2 account)

☐ **Premium:** Recommended for scenarios that require low latency.

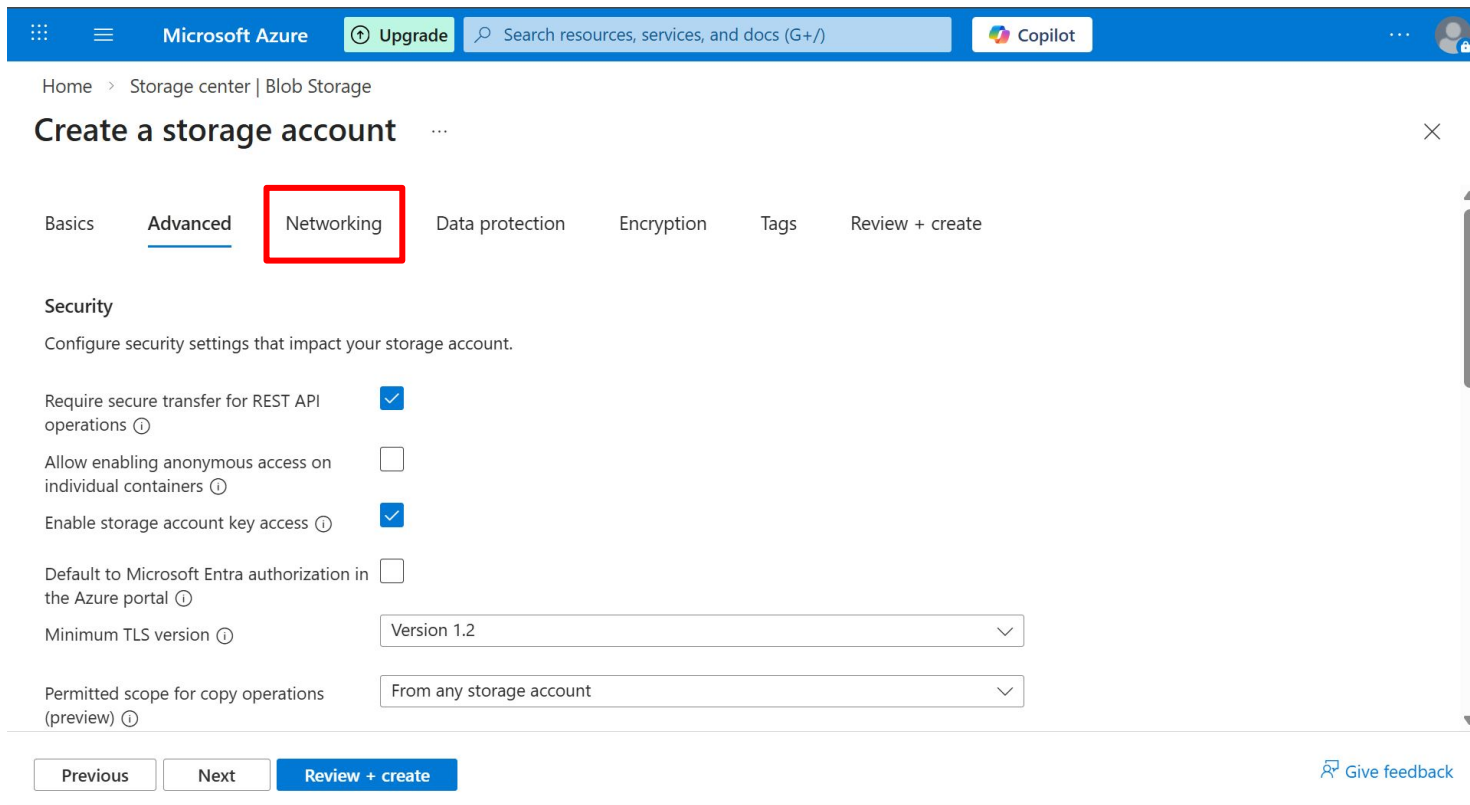
Redundancy * ① Geo-redundant storage (GRS)

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

[Give feedback](#)

- **Resource group:** Select an existing resource group or create a new one.
- **Storage account name:** Choose a globally unique name.
- **Region:** Select the region closest to your users (for better performance).
- **Performance:** Choose **Standard** (lower cost) unless a premium tier is required.
- **Replication:** Select **Geo-redundant storage (GRS)** for fault tolerance.

Leave the advanced tab as default, click “Networking”



Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Storage center | Blob Storage

Create a storage account ...

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 (preview) ⓘ From any storage account ▼

Previous Next Review + create

[Give feedback](#)

Click “next” to Data Protection

Microsoft Azure

Upgrade

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

Copilot

Home > Storage center | Blob Storage

Create a storage account

Public network access scope *

☐ Enable from all networks

☒ Enable from selected virtual networks and IP addresses

Virtual networks

Only the selected network will be able to access this storage account. [Learn more](#)

Virtual network subscription ⓘ

Azure subscription 1

Virtual network ⓘ

None

[Create virtual network](#)

IPv4 Addresses

Allow select public internet IP addresses to access your resource. [Learn more](#)

+ Add your client IPv4 address ("162.253.24.161")

Previous

Next

Review + create

Give feedback

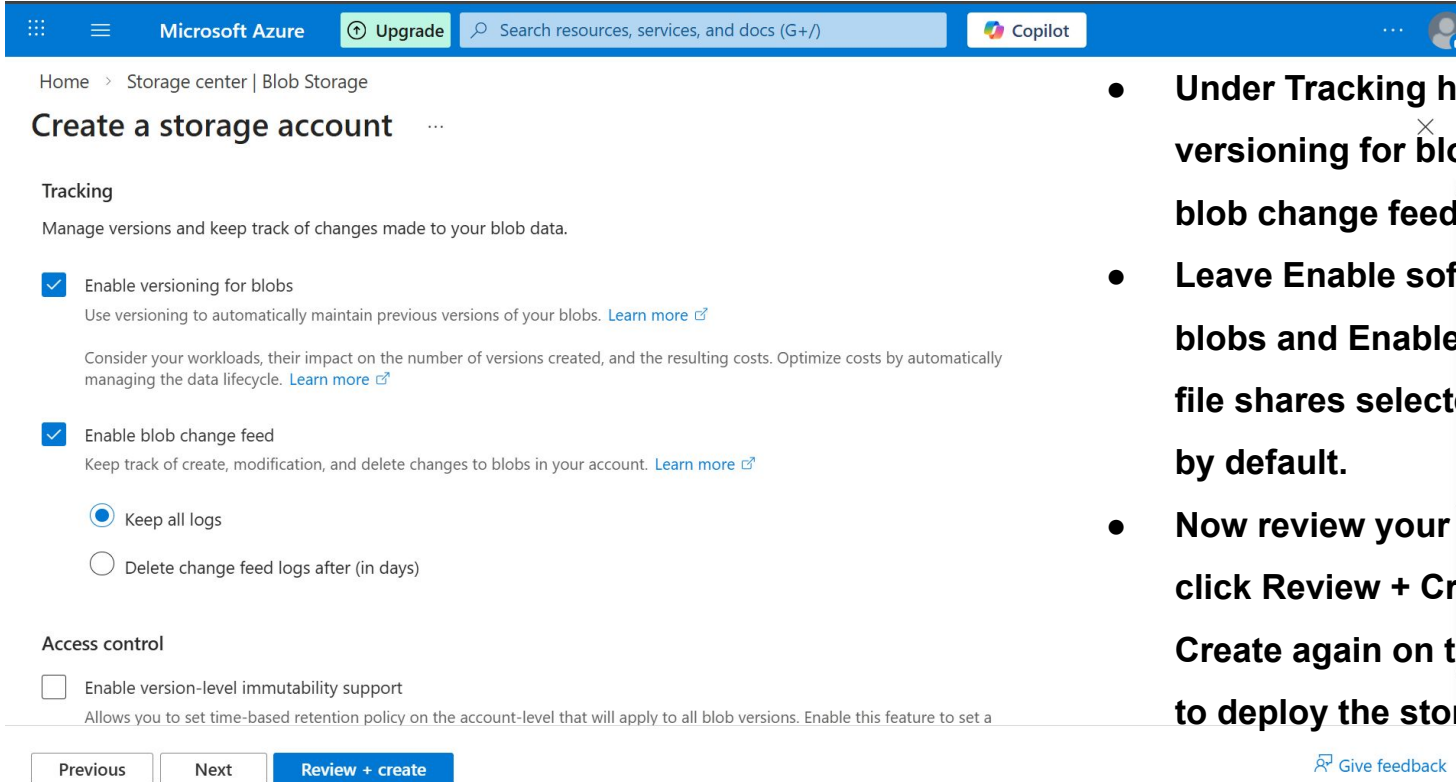
- Enable for additional security

Make selections

The screenshot shows the 'Create a storage account' page in the Microsoft Azure portal. The top navigation bar includes the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a 'Copilot' button. The breadcrumb trail indicates the path: Home > Storage center | Blob Storage. The main heading is 'Create a storage account'. Below this, the 'Recovery' section is expanded, showing a warning icon and text: 'When point-in-time restore is enabled, versioning, blob change feed and blob soft delete are also enabled. The retention periods for each of these features must be greater than that of point-in-time restore, if applicable. [Learn more](#)'. Below the warning, a message states: 'Protect your data from accidental or erroneous deletion or modification.' There are three main configuration options, each with a checked checkbox: 1. 'Enable point-in-time restore for containers': Includes a description about restoring containers to an earlier state and a 'Maximum restore point (days ago)' input field with the value '6'. 2. 'Enable soft delete for blobs': Includes a description about recovering blobs marked for deletion and a 'Days to retain deleted blobs' input field with the value '7'. 3. 'Enable soft delete for containers': This option is partially visible at the bottom. A red error message is displayed: 'Point-in-time restore requires versioning, blob change feed, and blob soft delete to be enabled.'

- Next, click Data protection and enable options such as point-in-time restore for containers and soft delete for blobs. To enable point-in-time restore for containers, this creates error messages.
- Scroll down

Make selections and click “review+create”



Microsoft Azure Upgrade Search resources, services, and docs (G+/)

Home > Storage center | Blob Storage

Create a storage account

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](#)
- ☒ Enable blob change feed
Keep track of create, modification, and delete changes to blobs in your account. [Learn more](#)
- ☒ Keep all logs
- ☐ Delete change feed logs after (in days)

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

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

[Give feedback](#)

- Under Tracking header, Enable versioning for blobs and Enable blob change feed.
- Leave Enable soft delete for blobs and Enable soft delete for file shares selected as they are by default.
- Now review your settings and click Review + Create then Create again on the next screen to deploy the storage account.

Select “create”

Microsoft Azure

Upgrade

Search resources, services, and docs (G+)

Copilot

Home > Storage center | Blob Storage

Create a storage account ...

BasicsAdvancedNetworkingData protectionEncryptionTagsReview + create

[View automation template](#)

Basics

Subscription	Azure subscription 1
Resource group	Storage-RG
Location	East US 2
Storage account name	storageplace001
Preferred storage type	
Performance	Standard
Replication	Read-access geo-redundant storage (RA-GRS)

Advanced

Enable hierarchical namespace	Disabled
-------------------------------	----------

PreviousNextCreate

[Give feedback](#)

Click “Containers”, under “Data Storage”

The screenshot shows the Microsoft Azure portal interface. At the top, there's a blue header bar with the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a 'Copilot' button. Below the header, the breadcrumb navigation shows 'Home > storageplace001_1769734294279 | Overview'. The main content area is titled 'storageplace001' and 'Storage account'. On the left sidebar, under the 'Data storage' section, the 'Containers' option is highlighted with a red rectangle. The main content area displays various actions like 'Upload', 'Open in Explorer', 'Delete', 'Move', 'Refresh', 'Open in mobile', and 'CLI / PS'. Below these actions, there's a section for 'Essentials' with details about the resource group, location, subscription, and disk state. On the right, there's a 'JSON View' link and a list of properties including Performance, Standard, Replication, Account kind, Provisioning state, and Created.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > storageplace001_1769734294279 | Overview

storageplace001 Storage account

Enhance the security of this storage account How can I make my storage account more resilient? +1

Search

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

Containers

File shares

Upload Open in Explorer Delete Move Refresh Open in mobile CLI / PS

Essentials

Resource group (move)

Storage-RG

Location

eastus2

Primary/Secondary Location

Primary: East US 2, Secondary: Central US

Subscription (move)

Azure subscription 1

Subscription ID

1e51f0d0-0ec0-4662-89ea-dcefc9938639

Disk state

Primary: Available, Secondary: Available

Tags (edit)

Add tags

Performance

Standard

Replication

Read-access geo-redundant storage (RA-GRS)

Account kind

StorageV2 (general purpose v2)

Provisioning state

Succeeded

Created

1/29/2026, 7:53:47 PM

JSON View

Click “+add container” and name it, then select “create”

The screenshot displays the Microsoft Azure portal interface. The top navigation bar includes the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a 'Copilot' button. The main content area shows the 'storageplace001 | Containers' page. A red box highlights the '+ Add container' button. To the right, the 'New container' dialog box is open, showing the 'Name' field with the value 'product-images' and a green checkmark. Below the name field, the 'Anonymous access level' is set to 'Private (no anonymous access)'. A blue information box states: 'The access level is set to private because anonymous access is disabled on this storage account.' At the bottom of the dialog, there is a 'Create' button and a 'Give feedback' link.

Home > storageplace001_1769734294279 | Overview > storageplace001

storageplace001 | Containers ☆ ...

Storage account

Search

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

Containers

File shares

+ Add container Upload Refresh Delete

Search containers by prefix

Showing all 2 items

<input type="checkbox"/>	Name	Last modified
<input type="checkbox"/>	\$logs	1/29/2026, 7:...
<input type="checkbox"/>	\$blobchangefeed	1/29/2026, 7:...

New container

Name *

product-images ✓

Anonymous access level ⓘ

Private (no anonymous access) ▾

i The access level is set to private because anonymous access is disabled on this storage account.

Advanced ▾

Create

Give feedback

Container created

The screenshot shows the Microsoft Azure portal interface. At the top, the navigation bar includes the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a 'Copilot' button. Below the navigation bar, the breadcrumb path is 'Home > storageplace001'. The main heading is 'storageplace001 | Containers', with a star icon and a close button. Below the heading, there is a search bar and a set of action buttons: '+ Add container', 'Upload', 'Refresh', 'Delete', 'Change access level', and 'Restore containers'. A secondary search bar for 'Search containers by prefix' and a dropdown for 'Only show active containers' are also present. The main content area displays a table of containers, with the 'product-images' container highlighted by a red box. The left sidebar contains a list of navigation options, with 'Containers' selected. At the bottom, there is a note about adding or removing favorites.

Home > storageplace001

storageplace001 | Containers ☆

Storage account

Search

Events

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

Containers

File shares

Queues

Tables

Security + networking

Data management

Storage Actions

Add or remove favorites by pressing Ctrl+Shift+F

+ Add container Upload Refresh Delete Change access level Restore containers

Search containers by prefix

Only show active containers

Showing all 3 items

<input type="checkbox"/>	Name	Last modified	Anonymous access level	Lease state
<input type="checkbox"/>	\$logs	1/29/2026, 7:54:09 PM	Private	Available
<input type="checkbox"/>	\$blobchangefeed	1/29/2026, 7:54:09 PM	Private	Available
<input type="checkbox"/>	product-images	1/29/2026, 7:59:30 PM	Private	Available

On left column in storage account, click on “access keys” under “security+networking”

The screenshot displays the Microsoft Azure portal interface. At the top, the navigation bar includes the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a 'Copilot' button. The breadcrumb trail indicates the path: Home > Storage center | All storage resources > storageplace001 > Storage-RG. The main header for the storage account 'storageplace001' includes a search bar, a star icon, and two buttons: 'Does this storage account follow security best practices' and 'Enhance the security of this storage account'. Below the header, a left-hand navigation pane lists various storage and security options. The 'Access keys' option under the 'Security + networking' section is highlighted with a red rectangle. The main content area shows the 'Essentials' tab for the 'Storage-RG' resource group. It displays details such as the resource group (Storage-RG), location (eastus2), primary/secondary locations (East US 2, Central US), subscription (Azure subscription 1), subscription ID (1e51fd0d0-0ec0-4662-89ea-dcefc9938639), disk state (Primary: Available, Secondary: Available), and tags. A right-hand pane shows performance and replication settings, including 'Standard', 'Replication', 'Read-access geo-redundant storage (RA-GRS)', 'Account kind', 'StorageV2 (general purpose v2)', 'Provisioning state', 'Succeeded', 'Created', and '1/29/2026, 7:53:47 PM'. A 'JSON View' link is visible in the top right corner of the main content area.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Storage center | All storage resources > storageplace001 > Storage-RG

storageplace001 Storage account

Does this storage account follow security best practices Enhance the security of this storage account +1

Search

Storage browser Storage Mover Partner solutions Resource visualizer Data storage Security + networking Networking Front Door and CDN Access keys Shared access signature Encryption Microsoft Defender for Cloud

Upload Open in Explorer Delete Move Refresh Open in mobile CLI / PS

Essentials JSON View

Resource group (move) Storage-RG

Location eastus2

Primary/Secondary Location Primary: East US 2, Secondary: Central US

Subscription (move) Azure subscription 1

Subscription ID 1e51fd0d0-0ec0-4662-89ea-dcefc9938639

Disk state Primary: Available, Secondary: Available

Tags (edit) Add tags

Performance Standard Replication Read-access geo-redundant storage (RA-GRS) Account kind StorageV2 (general purpose v2) Provisioning state Succeeded Created 1/29/2026, 7:53:47 PM

Add or remove favorites by pressing Ctrl+Shift+F

Note the access keys, but avoid sharing them for security purposes

The screenshot displays the Microsoft Azure portal interface. At the top, the navigation bar includes the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a Copilot icon. The breadcrumb trail indicates the path: Home > Storage center | All storage resources > storageplace001 > Storage-RG > storageplace001. The main heading is 'storageplace001 | Access keys', with a star icon and a close button (X) to the right. Below the heading, there is a search bar and a link to 'Learn more about managing storage account access keys'. The left sidebar contains a list of navigation options: Storage browser, Storage Mover, Partner solutions, Resource visualizer, Data storage, Security + networking (expanded), Networking, Front Door and CDN, Access keys (selected), Shared access signature, Encryption, and Microsoft Defender for Cloud. The main content area shows the 'Storage account name' as 'storageplace001'. It lists two keys, 'key1' and 'key2', each with a 'Rotate key' button. For each key, it shows the 'Last rotated' date as '1/29/2026 (0 days ago)'. Below the date, there are fields for the 'Key' and the 'Connection string', both masked with dots, and a 'Show' button to reveal them. At the bottom left, a note states: 'Add or remove favorites by pressing Ctrl+Shift+F'.

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Storage center | All storage resources > storageplace001 > Storage-RG > storageplace001

storageplace001 | Access keys ☆ ...

Storage account

Search

Storage browser

Storage Mover

Partner solutions

Resource visualizer

Data storage

Security + networking

Networking

Front Door and CDN

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Learn more about managing storage account access keys

Storage account name

storageplace001

key1 Rotate key

Last rotated: 1/29/2026 (0 days ago)

Key

..... Show

Connection string

..... Show

key2 Rotate key

Last rotated: 1/29/2026 (0 days ago)

Key

..... Show

Connection string

..... Show

Add or remove favorites by pressing Ctrl+Shift+F

On left column in storage account, click on “encryption” under “security+networking”

The screenshot displays the Microsoft Azure portal interface for a storage account named 'storageplace001'. The left-hand navigation pane is expanded, showing the 'Security + networking' section. Within this section, the 'Encryption' option is highlighted with a red rectangular box. Other options visible in the left pane include 'Storage browser', 'Storage Mover', 'Partner solutions', 'Resource visualizer', 'Data storage', 'Networking', 'Front Door and CDN', 'Access keys', 'Shared access signature', and 'Microsoft Defender for Cloud'. The main content area on the right shows the 'Essentials' tab for the storage account, displaying details such as 'Resource group (move)', 'Location' (eastus2), 'Primary/Secondary Location' (Primary: East US 2, Secondary: Central US), 'Subscription (move)' (Azure subscription 1), 'Subscription ID' (1e51f0d0-0ec0-4662-89ea-dcefc9938639), 'Disk state' (Primary: Available, Secondary: Available), and 'Tags (edit)'. A 'JSON View' link is also present in the top right of the main content area. The top of the page features the Microsoft Azure header with a search bar and a 'Copilot' button.

Ensure “Microsoft-managed keys” is enabled under Encryption (this will be on by default). Your encryption keys can be managed using “Customer-managed keys”.

The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a Copilot button. Below the navigation bar, the breadcrumb path is 'Home > storageplace001'. The main heading is 'storageplace001 | Encryption', with a subheading 'Storage account'. A search bar is present below the heading. On the left, there's a sidebar with various navigation options: 'Storage browser', 'Storage Mover', 'Partner solutions', 'Resource visualizer', 'Data storage', 'Security + networking', 'Networking', 'Front Door and CDN', 'Access keys', 'Shared access signature', 'Encryption' (highlighted), and 'Microsoft Defender for Cloud'. The main content area is titled 'Encryption' and 'Encryption scopes'. It contains a paragraph explaining that Storage service encryption protects data at rest and is enabled by default. Below this, there's a section titled 'Encryption selection' with two rows of settings: 'Enable support for customer-managed keys' (set to 'Blobs and files only') and 'Infrastructure encryption' (set to 'Disabled'). Under 'Infrastructure encryption', there are two radio buttons for 'Encryption type': 'Microsoft-managed keys' (selected and highlighted with a red box) and 'Customer-managed keys'. At the bottom, there are 'Save' and 'Discard' buttons, and a 'Give feedback' link.

Home > storageplace001

storageplace001 | Encryption
Storage account

Search

Storage browser
Storage Mover
Partner solutions
Resource visualizer
Data storage
Security + networking
Networking
Front Door and CDN
Access keys
Shared access signature
Encryption
Microsoft Defender for Cloud

Encryption Encryption scopes

Storage service encryption protects your data at rest. Azure Storage encrypts your data as it's written in our datacenters, and automatically decrypts it for you as you access it.

Please note that after enabling Storage Service Encryption, only new data will be encrypted, and any existing files in this storage account will retroactively get encrypted by a background encryption process. [Learn more about Azure Storage encryption](#)

Encryption selection

Enable support for customer-managed keys Blobs and files only

Infrastructure encryption Disabled

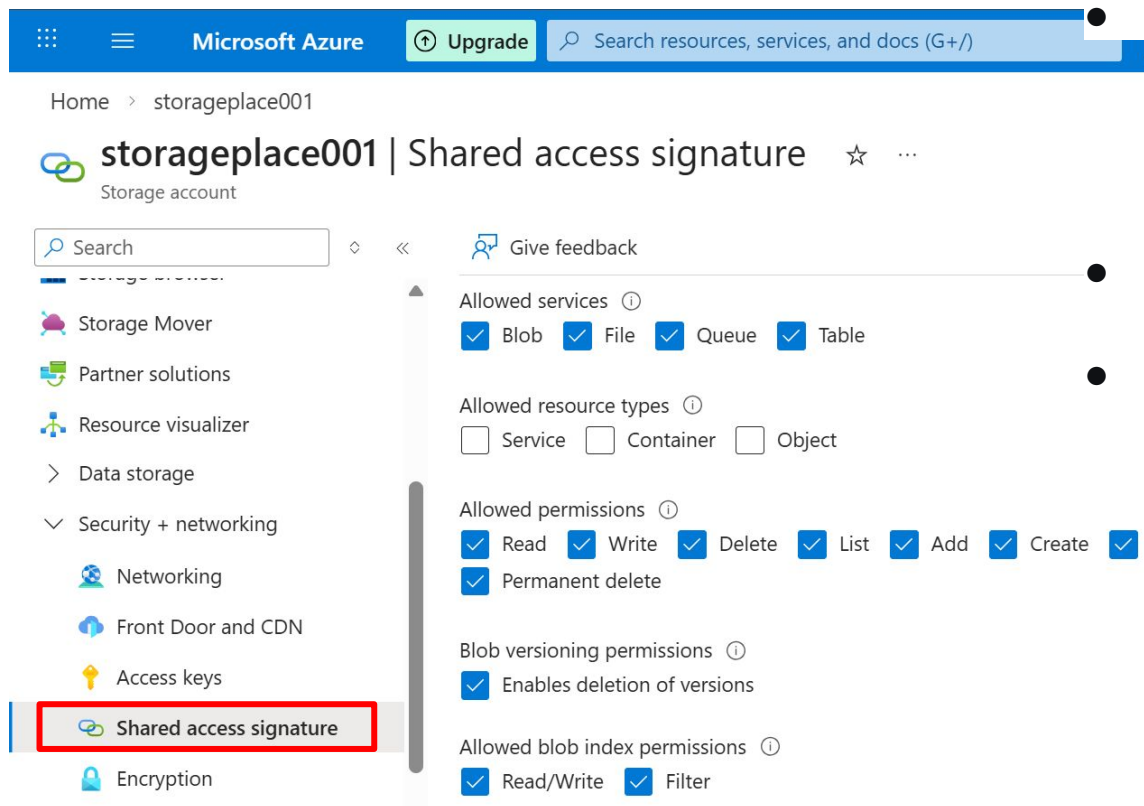
Encryption type

☒ Microsoft-managed keys
☐ Customer-managed keys

Save Discard

[Give feedback](#)

Select **Shared access signature** under **Security + networking** to configure shared access signatures (SAS)



Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > storageplace001

storageplace001 | Shared access signature ☆ ...

Storage account

Search

Give feedback

Allowed services ⓘ

- ☒ Blob
- ☒ File
- ☒ Queue
- ☒ Table

Allowed resource types ⓘ

- ☐ Service
- ☐ Container
- ☐ Object

Allowed permissions ⓘ

- ☒ Read
- ☒ Write
- ☒ Delete
- ☒ List
- ☒ Add
- ☒ Create
- ☒ Update
- ☒ Process
- ☒ Immutable storage
- ☒ Permanent delete

Blob versioning permissions ⓘ

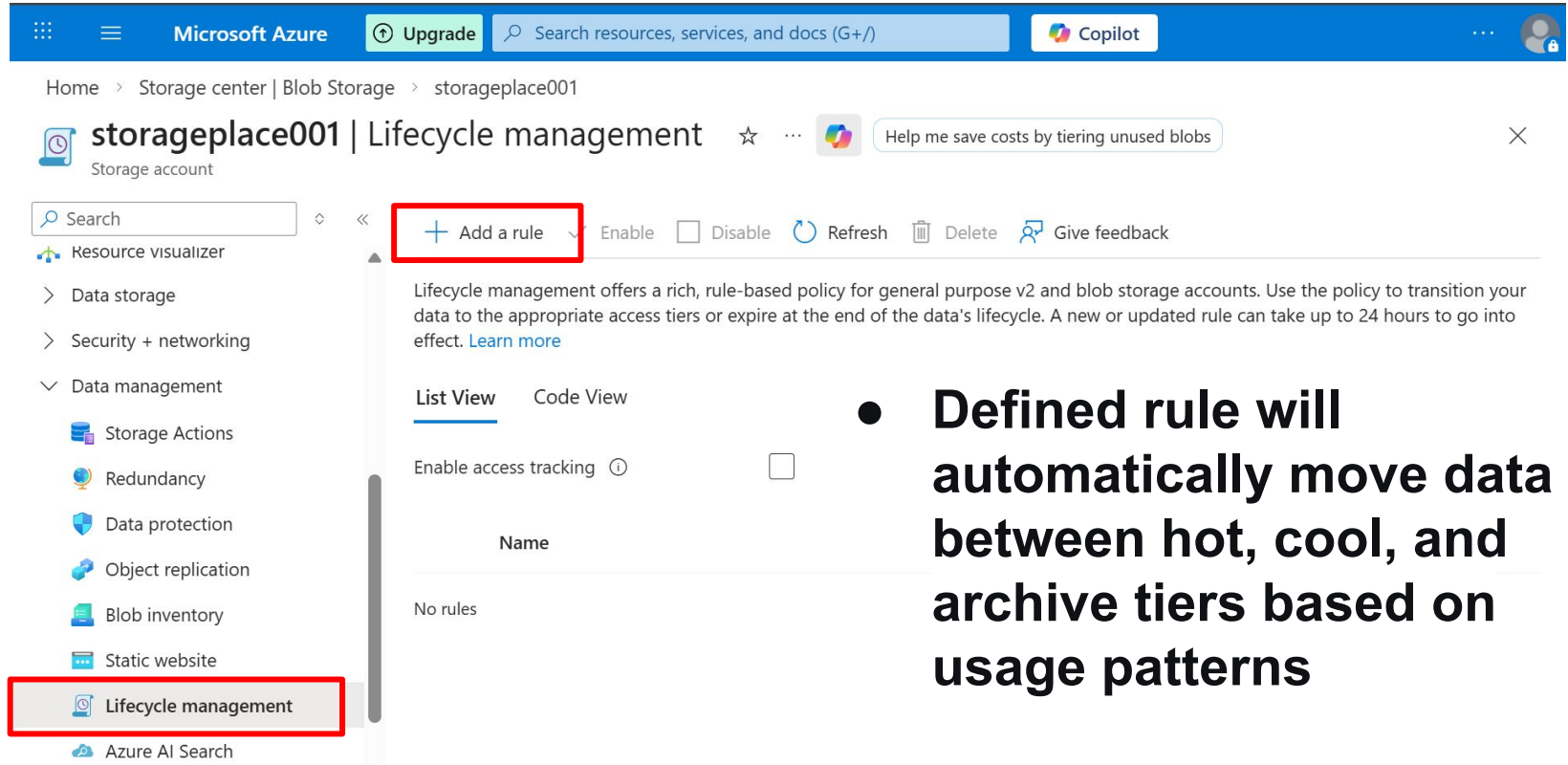
- ☒ Enables deletion of versions

Allowed blob index permissions ⓘ

- ☒ Read/Write
- ☒ Filter

- **SAS allows limited-time access to certain files or containers without exposing the storage account's access keys.**
- **Leave all selections as default.**
- **For security, you also need to define the permissions and expiry time.**

In the left column, select “Lifecycle management” under “Data management”.
Then select “+ add a rule”



Microsoft Azure

Upgrade

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

Copilot

Home > Storage center | Blob Storage > storageplace001

storageplace001 | Lifecycle management

Storage account

Search

Resource visualizer

Data storage

Security + networking

Data management

Storage Actions

Redundancy

Data protection

Object replication

Blob inventory

Static website

Lifecycle management

Azure AI Search

+ Add a rule

Enable

Disable

Refresh

Delete

Give feedback

Lifecycle management offers a rich, rule-based policy for general purpose v2 and blob storage accounts. Use the policy to transition your data to the appropriate access tiers or expire at the end of the data's lifecycle. A new or updated rule can take up to 24 hours to go into effect. [Learn more](#)

List View

Code View




Enable access tracking ⓘ



Name

No rules

- Defined rule will automatically move data between hot, cool, and archive tiers based on usage patterns

Name rule, leave all other settings on default, select “Next”

 Microsoft Azure  Search resources, services, and docs (G+/)



Home > Storage center | Blob Storage > storageplace001 | Lifecycle management

Add a rule

1 Details

2 Base blobs

A rule is made up of one or more conditions and actions that apply to the entire storage account. Optionally, specify that rules will apply to particular blobs by limiting with filters.

Rule name *

Rule scope *

☒ Apply rule to all blobs in your storage account

☐ Limit blobs with filters

Blob type *

☒ Block blobs

☐ Append blobs

Previous

Next

Select “last modified” and specify that data more than than 30 days should “move to cold storage”, then select “+add conditions”

Microsoft Azure Upgrade Search resources, services, and docs (G+/) Copilot

Home > Storage center | Blob Storage > storageplace001 | Lifecycle management

Add a rule

If

Base blobs were *

☒ Last modified

☐ Created

More than (days ago) *

30





Then

Move to cold storage

+ Add conditions

Previous Add

Select "last modified" data more than 180 days old "move to archive storage". Moving this tier for long-term storage reduces costs. Select "add".

 Microsoft Azure  Search resources, services, and docs (G+/) 

Home > Storage center | Blob Storage > storageplace001 | Lifecycle management

Add a rule

If

Base blobs were *

☒ Last modified

☐ Created


More than (days ago) *

180

Then

Move to archive storage

☒ Skip blobs that have been rehydrated in the last days

 If you have workloads that require real-time read-access to these blobs, moving them to archive is not recommended. Blobs in archive must first be rehydrated to hot or cool to read them. [Learn more](#)


Previous

Add

Rule created!

Microsoft Azure Upgrade Search resources

Home > Storage center | Blob Storage > storageplace001

 **storageplace001** | Lifecycle manager
Storage account

Search

- Resource visualizer
- > Data storage
- > Security + networking
- ▼ Data management
 - Storage Actions
 - Redundancy
 - Data protection
 - Object replication
 - Blob inventory
 - Static website
 - Lifecycle management**
 - Azure AI Search
- > Settings

+ Add a rule ✓ Enable [

Lifecycle management offers a rich set of policies to move data to the appropriate access tier or delete it. [Learn more](#)

List View Code View

Enable access tracking ⓘ

Name	Status	Blob type
30day-coolmigrate	Enabled	Block



Lifecycle management

Create rule-based policies for storage accounts.



Configured