

Configuring Azure Storage

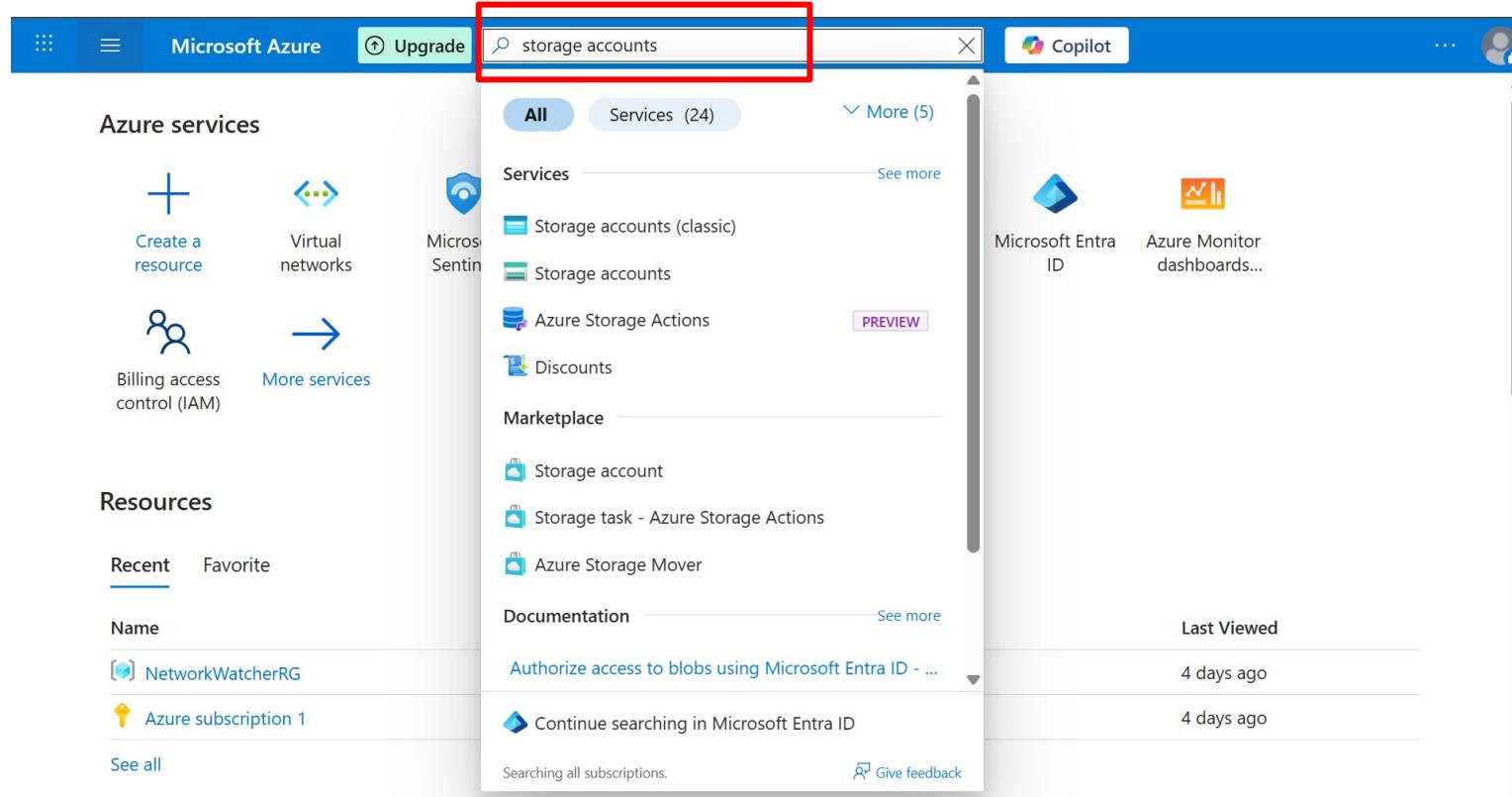
Jan 2026

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, there is a blue header bar with the "Microsoft Azure" logo, an "Upgrade" button, a search bar containing the text "storage accounts" (which is highlighted with a red box), a "Copilot" icon, and a user profile icon.

Below the header, the main content area is titled "Azure services". It features several quick access icons:

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

On the left side, there is a "Resources" section with tabs for "Recent" (selected) and "Favorite". Under "Recent", there are two items listed: "NetworkWatcherRG" and "Azure subscription 1". Below this is a "See all" link.

The central part of the screen is a search results panel. It has a "Services" tab (selected) showing 24 results and a "More (5)" option. The results are categorized under "Services" and "Marketplace".

- Services:**
 - Storage accounts (classic)
 - Storage accounts
 - Azure Storage Actions (PREVIEW)
 - Discounts
- Marketplace:**
 - Storage account
 - Storage task - Azure Storage Actions
 - Azure Storage Mover

At the bottom of the search panel, there is a "Documentation" section with a link to "Authorize access to blobs using Microsoft Entra ID - ...". There is also a "Continue searching in Microsoft Entra ID" link and a "Give feedback" button.

On the right side of the screen, there are two additional links: "Microsoft Entra ID" and "Azure Monitor dashboards...".

Select “Create”

The screenshot shows the Microsoft Azure Storage center | Blob Storage interface. At the top, there's a navigation bar with 'Microsoft Azure', 'Upgrade', a search bar ('Search resources, services, and docs (G+)'), 'Copilot', and user account information. Below the navigation bar, the title 'Storage center | Blob Storage' is displayed, along with the default directory 'Default Directory (nelcook11@gmail.onmicrosoft.com)'. On the left, a sidebar lists various storage-related options like Overview, All storage resources, Object storage, File storage, Block storage, Data management, Migration, Partner solutions, Management services, and Help. The main area is titled 'Resources' and contains a 'Create' button, which is highlighted with a red box. Other buttons include 'Restore', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Group by none'. A message at the top of this section says, 'You are viewing a new version of Browse experience. Click here to access the old experience.' Below the 'Create' button is a 'Filter for any field...' input field and three filter buttons: 'Subscription equals all', 'Resource Group equals all', and 'Location equals all'. A large central message states 'No storage accounts to display' with a descriptive text below it: '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.' At the bottom, there's a 'Showing 1 - 0 of 0. Display count: auto' dropdown, a 'Create' button, and a 'Give feedback' link.

Home

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

Copilot

Storage center | Blob Storage Default Directory (nelcook11@gmail.onmicrosoft.com)

Search Search Summary Resources

Overview All storage resources

Object storage File storage Block storage Data management Migration Partner solutions Management services Help

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

Create Give feedback

<https://portal.azure.com/?l=en-us#%2f#/insights/>

Fill in the required fields

The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal. The page has a blue header with the Microsoft Azure logo, an 'Upgrade' button, a search bar, and a 'Copilot' icon. Below the header, the breadcrumb navigation shows 'Home > Storage center | Blob Storage'. The main title is 'Create a storage account'. The form contains the following fields:

- Resource group ***: A dropdown menu showing '(New) Storage-RG' with a 'Create new' link.
- Instance details**
 - Storage account name ***: An input field containing 'storageplace001'.
 - Region ***: A dropdown menu showing '(US) East US 2' with a 'Deploy to an Azure Extended Zone' link.
 - Preferred storage type**: A dropdown menu with a tooltip explaining it provides relevant guidance without restricting storage type. It lists 'Choose preferred storage type' and 'Standard: Recommended for most scenarios (general-purpose v2 account)'.
 - Performance ***: A section with two radio buttons:
 - Standard**: Recommended for most scenarios (general-purpose v2 account)
 - Premium**: Recommended for scenarios that require low latency.
 - Redundancy ***: A dropdown menu showing 'Geo-redundant storage (GRS)'.

At the bottom, there are 'Previous' and 'Next' buttons, and a 'Review + create' button.

- **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”

The screenshot shows the Microsoft Azure portal interface for creating a storage account. At the top, there's a blue header bar with the Microsoft Azure logo, an 'Upgrade' button, a search bar ('Search resources, services, and docs (G+)'), a 'Copilot' icon, and a user profile icon. Below the header, the breadcrumb navigation shows 'Home > Storage center | Blob Storage'. The main title is 'Create a storage account' with a close button ('X').

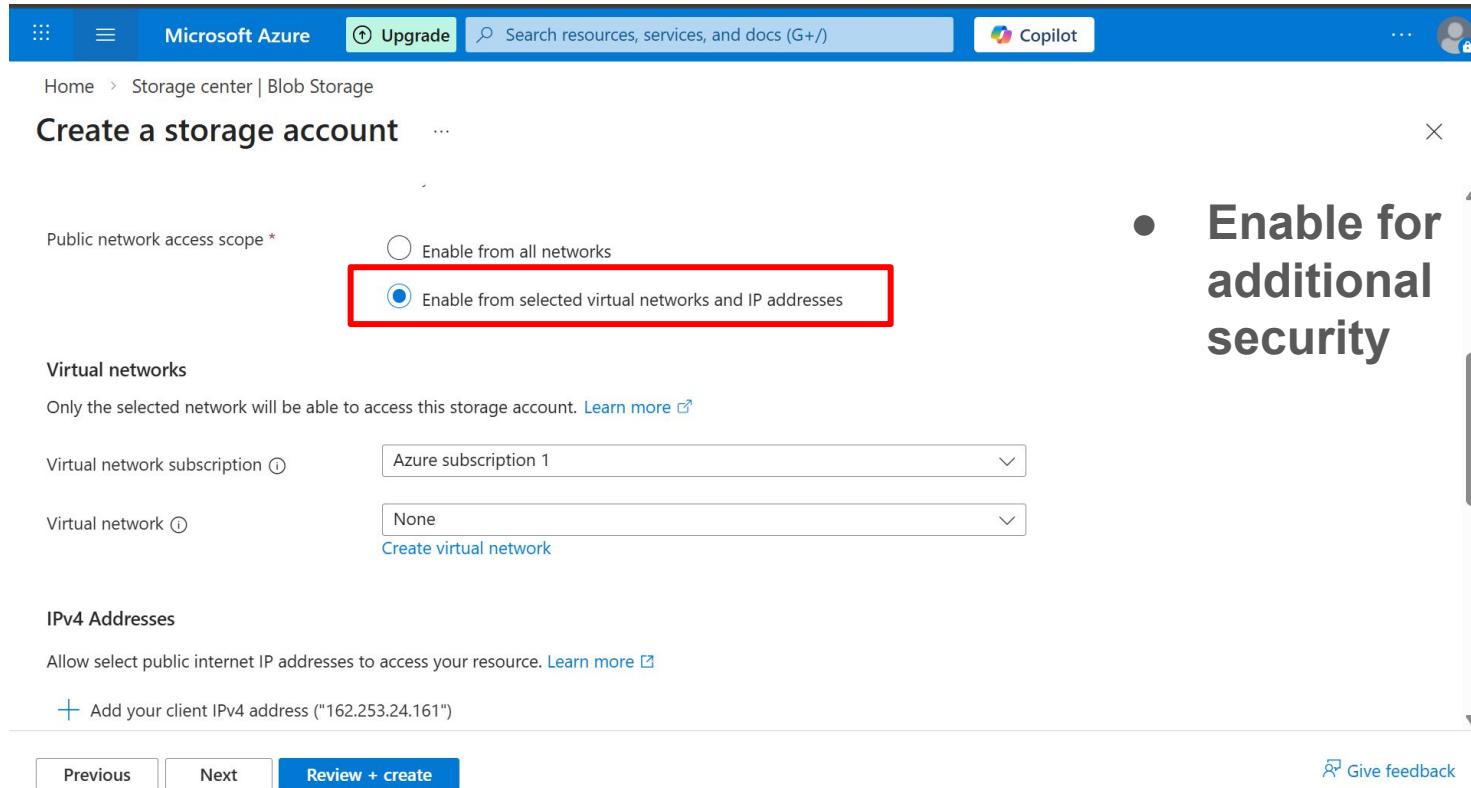
The navigation bar at the top of the form has several tabs: 'Basics', 'Advanced' (which is underlined, indicating it's the active tab), 'Networking' (which is highlighted with a red rectangle), 'Data protection', 'Encryption', 'Tags', and 'Review + create'.

The 'Networking' section contains the following configuration options:

- Require secure transfer for REST API operations**: A checkbox is checked (indicated by a blue checkmark).
- Allow enabling anonymous access on individual containers**: An empty checkbox is shown.
- Enable storage account key access**: A checkbox is checked (indicated by a blue checkmark).
- Default to Microsoft Entra authorization in the Azure portal**: An empty checkbox is shown.
- Minimum TLS version**: A dropdown menu is set to 'Version 1.2'.
- Permitted scope for copy operations (preview)**: A dropdown menu is set to 'From any storage account'.

At the bottom of the form, there are three buttons: 'Previous', 'Next', and 'Review + create' (which is highlighted in blue).

Click “next” to Data Protection



The screenshot shows the 'Create a storage account' wizard in the Microsoft Azure portal. The 'Public network access scope' section is highlighted with a red box around the 'Enable from selected virtual networks and IP addresses' option. A callout bubble on the right side of the page contains the text: '● Enable for additional security'.

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 [\(i\)](#) Azure subscription 1

Virtual network [\(i\)](#) 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

Make selections

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

Home > Storage center | Blob Storage

Create a storage account

Recovery

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](#)

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](#)

Maximum restore point (days ago)

Point-in-time restore requires versioning, blob change feed, and blob soft delete to be enabled.

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](#)

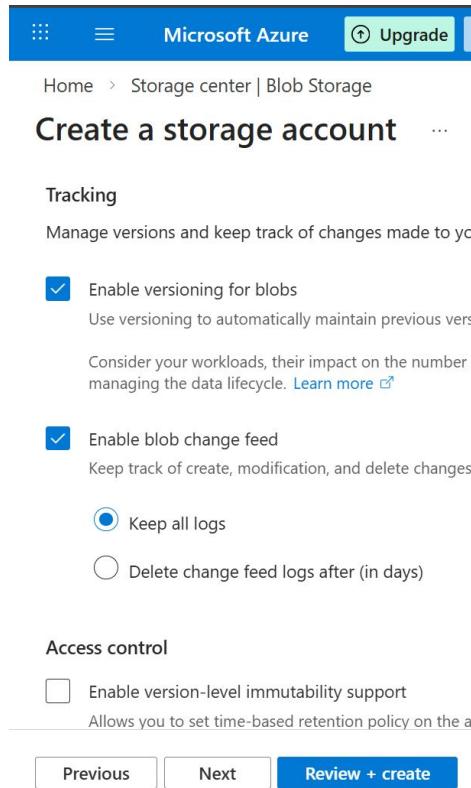
Days to retain deleted blobs

Enable soft delete for containers

- 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](#)

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](#)

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**

- **Under Tracking header, Enable X 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”

The screenshot shows the Microsoft Azure portal interface for creating a new storage account. The top navigation bar includes the Microsoft Azure logo, an 'Upgrade' button, a search bar, a 'Copilot' icon, and user profile information. Below the navigation bar, the breadcrumb path indicates 'Home > Storage center | Blob Storage'. The main title is 'Create a storage account' with a close button ('X'). The top navigation bar for this step includes 'Basics', 'Advanced', 'Networking', 'Data protection', 'Encryption', 'Tags', and 'Review + create', where 'Review + create' is underlined, signifying it is the current step.

[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
-------------------------------	----------

[Previous](#) [Next](#) [Create](#) [Give feedback](#)

Click “Containers”, under “Data Storage”

The screenshot shows the Microsoft Azure Storage account overview for 'storageplace001'. The left sidebar includes sections for Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Partner solutions, Resource visualizer, Data storage (with Containers highlighted by a red box), and File shares. The main content area displays details under the 'Essentials' tab, such as Resource group (Storage-RG), Location (eastus2), Primary/Secondary Location (Primary: East US 2, Secondary: Central US), Subscription (Azure subscription 1), and Subscription ID (1e51f0d0-0ec0-4662-89ea-dcefc9938639). The 'Containers' link is located under the 'Data storage' section of the sidebar.

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

storageplace001 Storage account

Home > storageplace001_1769734294279 | Overview

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

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

Resource group ([move](#)) Performance
Storage-RG Standard

Location Replication
eastus2 Read-access geo-redundant storage (RA-GRS)

Primary/Secondary Location Account kind
Primary: East US 2, Secondary: Central US StorageV2 (general purpose v2)

Subscription ([move](#)) Provisioning state
Azure subscription 1 Succeeded

Subscription ID Created
1e51f0d0-0ec0-4662-89ea-dcefc9938639 1/29/2026, 7:53:47 PM

Disk state
Primary: Available, Secondary: Available

Tags ([edit](#)) Add tags

Click “+add container” and name it, then 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, a 'Copilot' icon, and a user profile icon. Below the header, the URL indicates the user is on the 'storageplace001' storage account overview page, specifically the 'Containers' section.

The main area displays the 'storageplace001 | Containers' blade. On the left, a sidebar lists various management tools: Search, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Partner solutions, Resource visualizer, and Data storage. Under Data storage, 'Containers' is selected and highlighted in grey.

In the center, the 'Containers' blade shows a list of existing containers: '\$logs' and '\$blobchangefeed'. Above this list, there are buttons for 'Upload', 'Refresh', and 'Delete'. A prominent red box highlights the '+ Add container' button, which is located next to a search bar labeled 'Search containers by prefix'.

To the right, a modal window titled 'New container' is open. It contains fields for 'Name *' (set to 'product-images') and 'Anonymous access level' (set to 'Private (no anonymous access)'). A note below states: 'The access level is set to private because anonymous access is disabled on this storage account.' At the bottom of the modal are 'Create' and 'Give feedback' buttons.

Container created

Microsoft Azure [Upgrade](#) [Copilot](#) ... 

Home > storageplace001

storageplace001 | Containers

Storage account

Events Storage browser Storage Mover Partner solutions Resource visualizer Data storage **Containers** File shares Queues Tables Security + networking Data management Storage Actions

Search 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	...

Add or remove favorites by pressing **Ctrl+Shift+F**

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

The screenshot shows the Microsoft Azure Storage account settings page for 'storageplace001'. The left sidebar lists various options under 'Security + networking', with 'Access keys' highlighted by a red box. The main content area displays the 'Essentials' section of the storage account, including details like Resource group (Storage-RG), Location (eastus2), Primary/Secondary Location (Primary: East US 2, Secondary: Central US), Subscription (Azure subscription 1), and Account kind (StorageV2 (general purpose v2)).

Storage place001

Storage account

Search

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

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

JSON View

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

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

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

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

Add or remove favorites by pressing **Ctrl+Shift+F**

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

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 containing 'Search resources, services, and docs (G+)', and a 'Copilot' icon. On the far right of the header is a user profile icon.

The main content area has a breadcrumb navigation path: Home > Storage center | All storage resources > storageplace001 > Storage-RG > storageplace001. Below this, the title is 'storageplace001 | Access keys' with a 'Storage account' label.

On the left, there's a sidebar with various links: Storage browser, Storage Mover, Partner solutions, Resource visualizer, Data storage (expanded), Security + networking (expanded), Networking, Front Door and CDN, Access keys (selected and highlighted with a blue border), Shared access signature, Encryption, and Microsoft Defender for Cloud.

The main panel displays two sets of access keys for the storage account:

- key1** (Rotate key) - Last rotated: 1/29/2026 (0 days ago). It includes a 'Key' field with a redacted value and a 'Show' button.
- key2** (Rotate key) - Last rotated: 1/29/2026 (0 days ago). It includes a 'Key' field with a redacted value and a 'Show' button.

Below each key section is a 'Connection string' field with a redacted value and a 'Show' button.

At the bottom of the main panel, there's a note: 'Add or remove favorites by pressing Ctrl+Shift+F'.

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

The screenshot shows the Microsoft Azure portal interface for a storage account named "storageplace001". The left sidebar lists various account management options, with "Encryption" highlighted by a red box. The main content area displays the "Essentials" section of the storage account settings, including details like Resource group, Location, Primary/Secondary Location, Subscription, and Disk state.

Storage account: storageplace001

Essentials

Setting	Value
Resource group (move)	Performance
Storage-RG	Standard
Location	Replication
eastus2	Read-access geo-redundant storage (RA-GRS)
Primary/Secondary Location	Account kind
Primary: East US 2, Secondary: Central US	StorageV2 (general purpose v2)
Subscription (move)	Provisioning state
Azure subscription 1	Succeeded
Subscription ID	Created
1e51f0d0-0ec0-4662-89ea-dcefc9938639	1/29/2026, 7:53:47 PM
Disk state	Primary: Available, Secondary: Available

Add or remove favorites by pressing **Ctrl+Shift+F**

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 for managing storage account encryption. The top navigation bar includes the Microsoft Azure logo, an Upgrade button, a search bar, and a Copilot icon. The main title is "storageplace001 | Encryption".

The left sidebar menu lists various services: Storage browser, Storage Mover, Partner solutions, Resource visualizer, Data storage, Security + networking (Networking, Front Door and CDN, Access keys, Shared access signature), and two highlighted sections: Encryption and Microsoft Defender for Cloud.

The central content area is titled "Encryption" and "Encryption scopes". It explains that storage service encryption protects data at rest and automatically decrypts it. A note states that after enabling, only new data will be encrypted, and existing files will be retroactively encrypted.

The "Encryption selection" section contains two options:

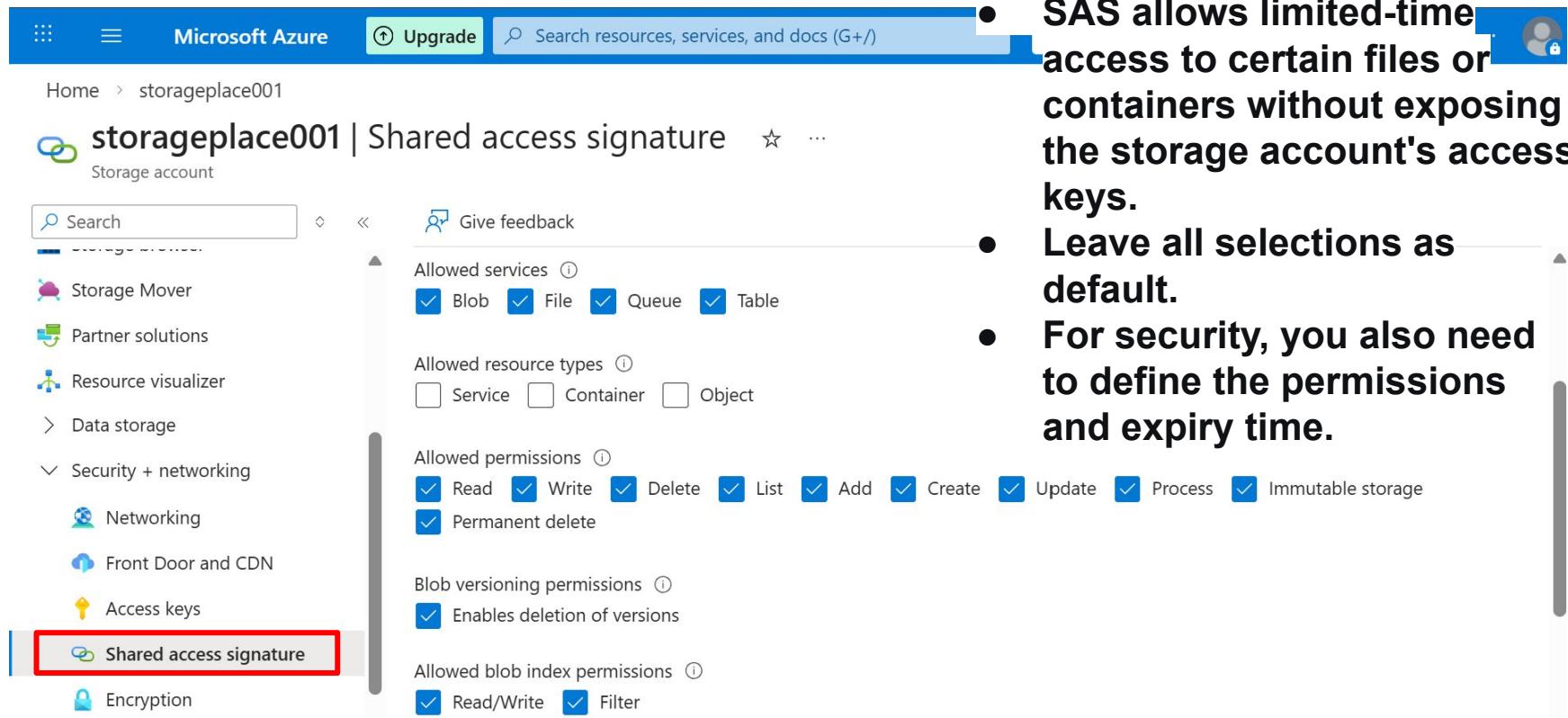
- "Enable support for customer-managed keys" (radio button) is selected, and the value is "Blobs and files only".
- "Infrastructure encryption" is set to "Disabled".

The "Encryption type" section shows two radio buttons:

- Microsoft-managed keys (selected)
- Customer-managed keys

At the bottom, there are "Save" and "Discard" buttons, and a "Give feedback" link.

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



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, and a search bar. Below the header, the URL 'storageplace001' is visible. The main content area is titled 'storageplace001 | Shared access signature'. On the left, a sidebar lists various services: Storage Mover, Partner solutions, Resource visualizer, Data storage, Security + networking (which is expanded), Networking, Front Door and CDN, Access keys, Shared access signature (which is highlighted with a red box), and Encryption.

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”

The screenshot shows the Microsoft Azure interface for managing a storage account named 'storageplace001'. In the left sidebar, under 'Data management', the 'Lifecycle management' option is selected and highlighted with a red box. At the top of the main content area, there is a button labeled '+ Add a rule' which is also highlighted with a red box. The main content area displays information about lifecycle management and a table showing 'No rules'.

Name	Actions
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”

The screenshot shows the Microsoft Azure Storage center Blob Storage Lifecycle management interface. At the top, there's a blue header bar with the Microsoft Azure logo, an 'Upgrade' button, a search bar, a 'Copilot' button, and a user profile icon. Below the header, the navigation path is 'Home > Storage center | Blob Storage > storageplace001 | Lifecycle management'. A large title 'Add a rule' is centered above two tabs: '1 Details' (which is selected) and '2 Base blobs'. The main content area contains the following fields:

- Rule name ***: A text input field containing '30day-doolmigrate'.
- Rule scope ***: A section with two radio buttons:
 - Apply rule to all blobs in your storage account
 - Limit blobs with filters
- Blob type ***: A section with two checkboxes:
 - Block blobs
 - Append blobs

At the bottom, there are 'Previous' and 'Next' buttons. The 'Next' button is highlighted in blue, indicating it is the next step in the process.

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

The screenshot shows the Microsoft Azure Storage center | Blob Storage lifecycle management rule configuration interface. At the top, there's a blue header bar with the Microsoft Azure logo, an Upgrade button, a search bar, a Copilot button, and user profile icons. Below the header, the breadcrumb navigation shows: Home > Storage center | Blob Storage > storageplace001 | Lifecycle management. The main title is "Add a rule".

The configuration form is divided into two main sections: "If" and "Then".

If Section:

- Condition: "Base blobs were *"
 - Last modified
 - Created
- Value: "More than (days ago) *"
Input field: "30"

Then Section:

- Action: "Move to cold storage"

At the bottom of the "If" section, there's a red rectangular box highlighting the "Add conditions" button.

At the very bottom of the page, there are "Previous" and "Add" buttons.

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

The screenshot shows the Microsoft Azure Storage center Blob Storage Lifecycle management rule creation interface. At the top, there's a navigation bar with icons for three, Microsoft Azure, Upgrade, Search resources, services, and docs (G+), Copilot, and user authentication.

The main title is "Add a rule" with a close button (X) to its right. Below it, the "If" section is active, indicated by a blue header. It asks "Base blobs were *" and has two options: "Last modified" (selected) and "Created". The "More than (days ago) *" input field contains "180".

The "Then" section is active, indicated by a green header. It shows a dropdown menu set to "Move to archive storage" and a checked checkbox "Skip blobs that have been rehydrated in the last [7] days". A warning message below states: "⚠ 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](#)".

At the bottom, there are "Previous" and "Add" buttons.

Rule created!

Microsoft Azure [Upgrade](#) [Search resources,](#)

Home > Storage center | Blob Storage > storageplace001

storageplace001 | Lifecycle management

Storage account

Search Add a rule Enable []

Resource visualizer

- > Data storage
- > Security + networking
- ✓ Data management
 - Storage Actions
 - Redundancy
 - Data protection
 - Object replication
 - Blob inventory
 - Static website
 - Lifecycle management
- > Settings

Lifecycle management offers a rich set of rules to move data to the appropriate access tier over time. [Learn more](#)

List View Code View

Enable access tracking

Name	Status	Blob type
30day-coolmigrate	Enabled	Block

Add or remove favorites by pressing **Ctrl+Shift+F**

Lifecycle management

Create rule-based policies for storage accounts.

Configured