

Project - Secure storage for Azure Files and Azure Blob Storage

Summary -storing business data securely by using Azure Blob Storage and Azure Files

Provide storage for different purposes such as IT department testing and training, public website, private company documents, shared file storage for the company offices, and a new company app.

IT Department	Customers	Employees and Partners	Corporate offices	Developers
Test and development storage	Public web site storage	Private internal storage	Shared file storage	Secure app storage

Task List

Create and configure a storage account.

Create and configure blob storage.

Create and configure Azure Files.

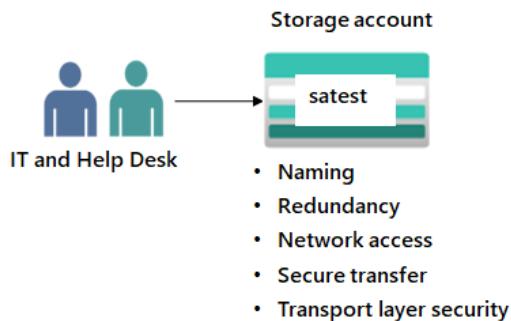
Configure encryption for storage.

Configure networking for storage.

Provide storage for the IT department testing and training

The IT department needs to prototype different storage scenarios and to train new personnel. The content isn't important enough to back up and doesn't need to be restored if the data is overwritten or removed. A simple configuration that can be easily changed is desired.

Architecture diagram



Task to be completed

- Create a storage account.
- Configure basic settings for security and networking.

Step 1 Create a resource group and a storage account

Create the resource group with the following settings

Home > Resource groups >

Create a resource group ...

Basics Tags Review + create

Resource group - A container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group. You decide how you want to allocate resources to resource groups based on what makes the most sense for your organization. [Learn more](#)

Project details

Subscription * Pay-As-You-Go

Resource group * storagergproject

Resource details

Region * (US) East US

[Review + create](#) [< Previous](#) [Next : Tags >](#)

Review and create to validate the resource group

The screenshot shows the Azure Resource Groups blade. On the left, there's a navigation pane with 'Resource groups' selected. The main area displays the details for the 'storagegerproject' resource group. The 'Essentials' section includes information like the subscription ID (8148d5d5-df15-44ef-beb3-5960d3dc42eb), location (East US), and deployment status (No deployments). The 'Resources' section shows a list view with filters applied, resulting in 0 records found. A message indicates 'No resources match your filters'.

Step 2 - Create and deploy a storage account to support testing and training

Create storage with the following setting

The screenshot shows the 'Create a storage account' wizard. The 'Basics' tab is active, showing the subscription set to 'Pay-As-You-Go' and the resource group set to 'storagegerproject'. In the 'Instance details' tab, the storage account name is 'azurestorageproject01', the region is '(US) East US', and the performance tier is set to 'Standard'. Under 'Redundancy', 'Geo-redundant storage (GRS)' is selected, and the 'Make read access to data available in the event of regional unavailability' checkbox is checked. Navigation buttons at the bottom include 'Review', '< Previous', 'Next : Advanced >', and 'Give feedback'.

Disable the recovery for the storage account as this is not needed but if you need backups then this would be import.

The screenshot shows the 'Create a storage account' wizard on the 'Data protection' tab. It includes sections for 'Recovery', 'Tracking', and 'Access control'. Under 'Recovery', there are four checkboxes: 'Enable point-in-time restore for containers', 'Enable soft delete for blobs', 'Enable soft delete for containers', and 'Enable soft delete for file shares'. Under 'Tracking', there are three checkboxes: 'Enable versioning for blobs', 'Enable blob change feed', and 'Enable hierarchical namespace'. Under 'Access control', there is a table showing basic settings like subscription, resource group, location, and deployment model. At the bottom are 'Review', 'Next : Encryption >', and 'Give feedback' buttons.

Leave other settings as default and click on review then create.

The screenshot shows the 'Create a storage account' wizard on the 'Review' tab. It displays the final configuration for the storage account, including the basics (Subscription: Pay-As-You-Go, Resource Group: storagergproject, Location: eastus, Storage account name: azurestorageproject01, Deployment model: Resource manager, Performance: Standard, Replication: Read-access geo-redundant storage (RA-GRS)), advanced settings (Enable hierarchical namespace: Disabled, Enable network file system v3: Disabled, Allow cross-tenant replication: Disabled, Access tier: Hot, Enable SFTP: Disabled, Large file shares: Disabled), networking (Network connectivity: Public endpoint (all networks), Default routing tier: Microsoft network routing, Endpoint type: Standard), and security (Secure transfer: Enabled, Allow storage account key access: Enabled, Default to Microsoft Entra authorization in: Disabled). At the bottom are 'Create', '< Previous', 'Next >', 'Download a template for automation', and 'Give feedback' buttons.

Click go to resource on deployment completed.

The screenshot shows the Azure Deployment Overview page for a deployment named "azurestorageproject01_1705787592467". The status is "Your deployment is complete". Deployment details include a start time of 20/01/2024, 21:56:17. A "Go to resource" button is visible. On the right, there are promotional cards for Cost Management, Microsoft Defender for Cloud, Free Microsoft tutorials, and Work with an expert.

Step 3 - Configure simple settings in the storage account

The data in this storage account doesn't require high availability or durability. A lowest cost storage solution is desired.

Under the left navigation in the **Data management** section, select the **Redundancy** blade

Select Locally-redundant storage (LRS) in the Redundancy drop-down

The screenshot shows the "Redundancy" blade for the "azurestorageproject01" storage account. The redundancy dropdown is set to "Locally redundant storage (LRS)". The table below shows two storage endpoints: East US (Primary, Available) and West US (Secondary, Available). A world map indicates the locations of the primary and secondary endpoints.

Location	Data center type	Status	Failover
East US	Primary	Available	-
West US	Secondary	Available	-

Primary location: East US
Secondary location: West US

Click on save or else the settings will not be saved.

Home > azurestorageproject01_1705787592467 | Overview > azurestorageproject01

azurestorageproject01 | Redundancy

Storage account

Search Save Discard Prepare for failover Refresh Give feedback

Data management

- Redundancy
- Data protection
- Object replication
- Blob inventory
- Static website
- Lifecycle management
- Azure AI Search

Settings

- Configuration
- Data Lake Gen2 upgrade
- Resource sharing (CORS)
- Advisor recommendations
- Endpoints
- Locks

Monitoring

- Insights
- Alerts
- Metrics
- Workbooks
- Diagnostic settings
- Logs

Monitoring (classic)

- Metrics (classic)
- Diagnostic settings (classic)
- Usage (classic)

Azure Storage redundancy copies your data so that it is protected from transient hardware failures, network or power outages, and natural disasters. If an outage renders the primary endpoint unavailable, then you can initiate a failover to the secondary endpoint to rapidly restore write access to your data. [Learn more about storage account failover](#)

Redundancy (Locally-redundant storage (LRS))

Last failover time -

Storage endpoints View all

Location	Data center type	Status
East US	Primary	Available

World map showing the location of the storage account in the East US region.

Primary location

Step 4 - The storage account should only accept requests from secure connections

In the **Settings** section, select the **Configuration** blade

Home > azurestorageproject01

azurestorageproject01 | Configuration

Storage account

Search Save Discard Refresh Give feedback

Data management

- Redundancy
- Data protection
- Object replication
- Blob inventory
- Static website
- Lifecycle management
- Azure AI Search

Settings

- Configuration
- Data Lake Gen2 upgrade
- Resource sharing (CORS)
- Advisor recommendations
- Endpoints
- Locks

Monitoring

- Insights
- Alerts
- Metrics
- Workbooks
- Diagnostic settings
- Logs

Monitoring (classic)

- Metrics (classic)
- Diagnostic settings (classic)
- Usage (classic)

The cost of your storage account depends on the usage and the options you choose below. [Learn more about storage pricing](#)

Account kind: StorageV2 (general purpose v2)

Performance:

- Standard
- Premium

This setting cannot be changed after the storage account is created.

Secure transfer required:

- Disabled
- Enabled

Allow Blob anonymous access:

- Disabled
- Enabled

Allow storage account key access:

- Disabled
- Enabled

Allow recommended upper limit for shared access signature (SAS) expiry interval:

- Disabled
- Enabled

Default to Microsoft Entra authorization in the Azure portal:

- Disabled
- Enabled

Minimum TLS version:

Version 1.2

Permitted scope for copy operations (preview):

From any storage account

Blob access tier (default):

- Hot
- Cool

Large file shares:

- Disabled
- Enabled

Ensure **Secure transfer required** is Enabled

The screenshot shows the 'Configuration' blade for the 'azurestorageproject01' storage account. In the 'Settings' section, under 'Secure transfer required', the 'Enabled' radio button is selected. Other settings visible include 'Allow Blob anonymous access' (Enabled), 'Allow storage account key access' (Enabled), 'Allow recommended upper limit for shared access signature (SAS) expiry interval' (Enabled), 'Default to Microsoft Entra authorization in the Azure portal' (Enabled), 'Minimum TLS version' (Version 1.2), 'Permitted scope for copy operations (preview)' (From any storage account), 'Blob access tier (default)' (Hot), and 'Large file shares' (Disabled).

Step 5 - Developers would like the storage account to use at least TLS version 1.2

In the **Settings** section, select the **Configuration** blade

The screenshot shows the 'Configuration' blade for the 'azurestorageproject01' storage account. In the 'Settings' section, the 'Minimum TLS version' dropdown is open, showing options: 'Version 1.0', 'Version 1.1', and 'Version 1.2'. The 'Version 1.2' option is highlighted. Other settings visible include 'Secure transfer required' (Enabled), 'Allow Blob anonymous access' (Enabled), 'Allow storage account key access' (Enabled), 'Allow recommended upper limit for shared access signature (SAS) expiry interval' (Enabled), 'Default to Microsoft Entra authorization in the Azure portal' (Enabled), 'Permitted scope for copy operations (preview)' (From any storage account), 'Blob access tier (default)' (Hot), and 'Large file shares' (Disabled).

Ensure the Minimal TLS version is set to Version 1.2

The screenshot shows the 'Configuration' blade for the storage account 'azurestorageproject01'. In the 'Settings' section, the 'Configuration' item is selected. Under 'Minimum TLS version', the dropdown menu is open and shows 'Version 1.2' as the selected option.

Step 6 - Until the storage is needed again, disable requests to the storage account. Learn more about disabling shared keys

In the **Settings** section, select the **Configuration** blade

This screenshot is identical to the one above, showing the 'Configuration' blade for the storage account 'azurestorageproject01'. The 'Configuration' item is selected in the 'Settings' section, and the 'Minimum TLS version' dropdown is set to 'Version 1.2'.

Ensure Allow storage account key access is Disabled

When Allow storage account key access is disabled, any requests to the account that are authorized with Shared Key, including shared access signatures (SAS), will be denied. Client applications that currently access the storage account using Shared Key will no longer work.

The screenshot shows the 'Configuration' tab of an Azure Storage Account named 'azurestorageproject01'. In the 'Settings' section, the 'Allow storage account key access' setting is configured to 'Disabled' (radio button selected). A warning message states: 'When Allow storage account key access is disabled, any requests to the account that are authorized with Shared Key, including shared access signatures (SAS), will be denied. Client applications that currently access the storage account using Shared Key will no longer work.' Other settings visible include 'Account kind' (StorageV2), 'Performance' (Standard), 'Secure transfer required' (Enabled), 'Allow Blob anonymous access' (Disabled), and 'Default to Microsoft Entra authorization in the Azure portal' (Disabled).

Press save to save settings made to storage account

This screenshot is identical to the one above, showing the 'Configuration' tab of the 'azurestorageproject01' storage account. The 'Allow storage account key access' setting remains disabled. The 'Save' button is highlighted in blue at the top of the page, indicating the next step is to save the changes.

Step 7 - Ensure the storage account allows public access from all networks

In the **Security + networking** section, select the **Networking** blade

The screenshot shows the Azure Storage account 'azurestorageproject01' in the Networking blade. Under 'Public network access', the radio button 'Enabled from all networks' is selected. A note below states: 'All networks, including the internet, can access this storage account.' Under 'Network Routing', 'Microsoft network routing' is selected. The left sidebar shows the 'Networking' blade is currently selected.

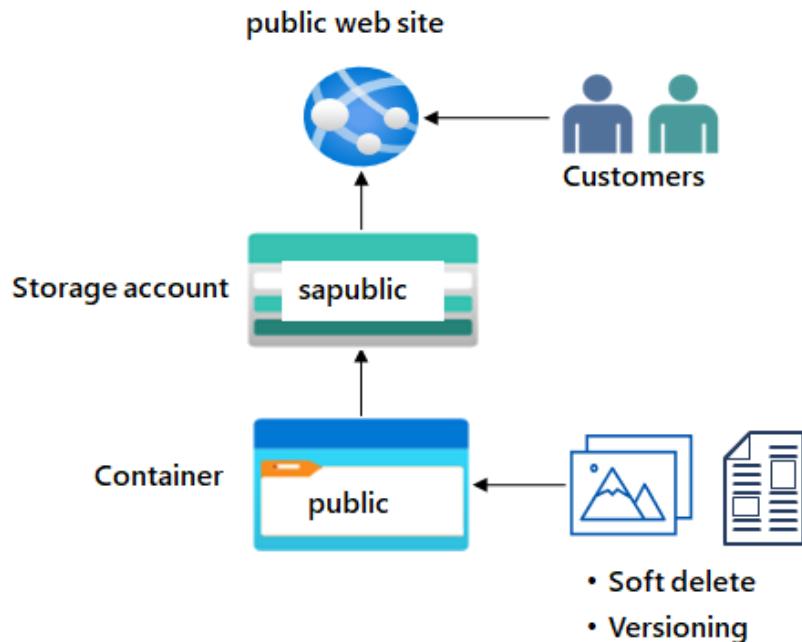
Ensure Public network access is set to Enabled from all networks

This screenshot is identical to the one above, showing the Azure Storage account 'azurestorageproject01' in the Networking blade. The 'Enabled from all networks' option is selected under 'Public network access'. The left sidebar shows the 'Networking' blade is currently selected.

Provide storage for the public website

The company website supplies product images, videos, marketing literature, and customer success stories. Customers are located worldwide and demand is rapidly expanding. The content is mission-critical and requires low latency load times. It's important to keep track of the document versions and to quickly restore documents if they're deleted.

Architecture diagram



Task to be completed

- Create a storage account with high availability.
- Ensure the storage account has anonymous public access.
- Create a blob storage container for the website documents.
- Enable soft delete so files can be easily restored.
- Enable blob versioning.

Step 1 - Create a storage account with high availability

Create a storage account with the following settings to support the public website

The screenshot shows the 'Create a storage account' wizard on the 'Basics' tab. It includes sections for 'Project details' (Subscription: Pay-As-You-Go, Resource group: (New) publicwebsitestoragerg), 'Instance details' (Storage account name: companypublicwebsite, Region: (US) East US, Performance: Standard, Redundancy: Geo-redundant storage (GRS), checked option: Make read access to data available in the event of regional unavailability), and navigation buttons (Review, < Previous, Next : Advanced >, Give feedback).

Disable all data protection this can be enable later.

The screenshot shows the 'Create a storage account' wizard on the 'Data protection' tab. It includes sections for 'Recovery' (checkboxes for point-in-time restore for containers, soft delete for blobs, soft delete for containers, and soft delete for file shares), 'Tracking' (checkboxes for blob versioning, blob change feed), and 'Access control' (checkboxes for blob ownership). Navigation buttons (Review, < Previous, Next : Encryption >, Give feedback) are at the bottom.

All other settings default Click Review and create.

Create a storage account ...



Basics Advanced Networking Data protection Encryption Tags Review

Basics

Subscription	Pay-As-You-Go
Resource Group	publicwebsitesstoragerg
Location	eastus
Storage account name	companypublicwebsite
Deployment model	Resource manager
Performance	Standard
Replication	Read-access geo-redundant storage (RA-GRS)

Advanced

Enable hierarchical namespace	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot
Enable SFTP	Disabled
Large file shares	Disabled

Networking

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

Security

Secure transfer	Enabled
Allow storage account key access	Enabled
Default to Microsoft Entra authorization in	Disabled

Create

< Previous

Next >

Download a template for automation

Give feedback

One storage account is deployed, select **Go to resource**

Home > companypublicwebsite_1705789608282 | Overview >

companypublicwebsite

Storage account

Essentials

Resource group (move)	: publicwebsitesstoragerg	Performance	: Standard
Location	: eastus	Replication	: Read-access geo-redundant storage (RA-GRS)
Primary/Secondary Location	: Primary: East US, Secondary: West US	Account kind	: StorageV2 (general purpose v2)
Subscription (move)	: Pay-As-You-Go	Provisioning state	: Succeeded
Subscription ID	: 8148d5d5-df15-44ef-beb3-5960d3dc42eb	Created	: 20/01/2024, 22:29:53
Disk state	: Primary: Available, Secondary: Available		

Properties

Blob service	Security
Hierarchical namespace	Require secure transfer for REST API operations
Default access tier	Enabled
Blob anonymous access	Storage account key access
Blob soft delete	Enabled
Container soft delete	Minimum TLS version
Versioning	Infrastructure encryption
Change feed	
NFS v3	
Allow cross-tenant replication	

File service

Large file share	Endpoint type
Identity-based access	Standard
Default share-level permissions	
Soft delete	
Share capacity	

Queue service

Step 2 - This storage requires high availability if there's a regional outage. Additionally, enable read access to the secondary region

In the storage account, in the **Data management** section, select the **Redundancy** blade

The screenshot shows the 'Redundancy' blade for a storage account named 'companypublicwebsite'. The left sidebar lists 'File shares', 'Queues', 'Tables', 'Security + networking' (Networking, Front Door and CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud), 'Data management' (Redundancy, Data protection, Object replication, Blob inventory, Static website, Lifecycle management, Azure AI Search), 'Settings' (Configuration, Data Lake Gen2 upgrade, Resource sharing (CORS), Advisor recommendations, Endpoints, Locks), and 'Endpoints'. The 'Redundancy' blade has a dropdown menu set to 'Read-access geo-redundant storage (RA-GRS)'. Below it, a table shows 'Storage endpoints' with two rows: 'Location' (East US and West US), 'Data center type' (Primary and Secondary), 'Status' (Available), and 'Failover' (both are empty). A world map indicates the locations of the primary and secondary endpoints. A legend at the bottom identifies the blue location pin as 'Primary location' and the green location pin as 'Secondary location'.

Ensure **Read-access Geo-redundant storage** is selected

This screenshot is identical to the one above, showing the 'Redundancy' blade for the same storage account 'companypublicwebsite'. The interface, table data, and world map are all the same, confirming that the 'Read-access geo-redundant storage (RA-GRS)' setting is selected.

Primary Reason set to East US and secondary region set to West US

Step 3 - Information on the public website should be accessible without requiring customers to login

In the storage account, in the **Settings** section, select the **Configuration** blade

The screenshot shows the Azure Storage Account Configuration blade for 'companypublicwebsite'. The left sidebar lists various management sections like Data management, Monitoring, and Monitoring (classic). The 'Settings' section is currently selected. Under 'Configuration', the 'Allow Blob anonymous access' setting is highlighted, showing it is set to 'Enabled' (radio button selected). Other settings visible include 'Allow storage account key access' (Enabled), 'Allow recommended upper limit for shared access signature (SAS) expiry interval' (Disabled), and 'Default to Microsoft Entra authorization in the Azure portal' (Enabled).

Ensure the Allow blob anonymous access setting is Enabled

This screenshot is identical to the one above, showing the Azure Storage Account Configuration blade. The 'Allow Blob anonymous access' setting is clearly visible under the 'Configuration' section of the 'Settings' blade, with the 'Enabled' radio button selected. A tooltip indicates that some blobs may become anonymously readable.

Click Save to save settings for allow blob anonymous access

The cost of your storage account depends on the usage and the options you choose below. [Learn more about storage pricing](#)

Account kind: StorageV2 (general purpose v2)

Performance: Standard (radio button selected)

Secure transfer required: Enabled (radio button selected)

Allow Blob anonymous access: Enabled (radio button selected)

Allow storage account key access: Enabled (radio button selected)

Allow recommended upper limit for shared access signature (SAS) expiry interval: Disabled (radio button selected)

Default to Microsoft Entra authorization in the Azure portal: Disabled (radio button selected)

Minimum TLS version: Version 1.2

Permitted scope for copy operations (preview): From any storage account

Blob access tier (default): Hot (radio button selected)

Large file shares: Disabled (radio button selected)

Step 4 - Create a blob storage container with anonymous read access

In the **Data storage** section, select the **Containers** blade

Name	Last modified	Anonymous access level	Lease state
\$logs	20/01/2024, 22:30:18	Private	Available

Select + Container

Ensure the **Name** of the container is public

The screenshot shows the 'Containers' blade in the Azure Storage account 'companypublicwebsite'. A modal window titled 'New container' is open, prompting for a container name. The name 'public' is entered in the 'Name' field. Below it, the 'Anonymous access level' dropdown is set to 'Private (no anonymous access)'. A note indicates that 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.

Click create to create the public container

The screenshot shows the 'Containers' blade in the Azure Storage account 'companypublicwebsite'. The 'Containers' section lists two containers: 'Slogs' and 'public'. Both containers were created on 20/01/2024 at 22:30:18. They both have 'Private' anonymous access level and are in an 'Available' lease state. The 'public' container is highlighted with a blue selection bar. The left sidebar includes links for Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, and Data storage (Containers, File shares, Queues, Tables). The right sidebar includes Security + networking (Networking, Front Door and CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud) and Data management (Redundancy, Data protection, Object replication, Blob inventory).

Step 5 - Customers should be able to view the images without being authenticated. Configure anonymous read access for the public container blobs.

Select the **public** container

The screenshot shows the Azure Storage Container Overview blade for the 'public' container. The left sidebar includes links for Overview, Diagnose and solve problems, Access Control (IAM), Settings (Shared access tokens, Access policy, Properties, Metadata), and a search bar. The main area displays the 'Authentication method' as 'Access key (Switch to Microsoft Entra user account)' and 'Location' as 'public'. A search bar for blobs by prefix is present. Below is a table with columns: Name, Modified, Access tier, Archive status, Blob type, Size, and Lease state. The message 'No results' is displayed.

On the **Overview** blade, select **Change access level**

Ensure the **Public access level** is **Blob (anonymous read access for blobs only)**. Select **OK** to Save

The screenshot shows the 'Change access level' dialog box overlaid on the container overview page. The dialog title is 'Change access level' with the sub-instruction 'Change the access level of container 'public''. It shows the 'Anonymous access level' dropdown set to 'Blob (anonymous read access for blobs only)'. A warning message below states: 'Blobs within the container can be read by anonymous request, but container data is not available. Anonymous clients cannot enumerate the blobs within the container.' At the bottom are 'OK' and 'Cancel' buttons.

Step 6 - Uploading files and testing access

Ensure you are viewing your container

The screenshot shows the Azure Storage Explorer interface. On the left, there's a sidebar with navigation links: Home, companypublicwebsite | Containers, public (Container), Overview, Diagnose and solve problems, Access Control (IAM), Settings, Shared access tokens, Access policy, Properties, and Metadata. The main area is titled 'Overview' and shows the following details:

- Authentication method:** Access key ([Switch to Microsoft Entra user account](#))
- Location:** public
- Search blobs by prefix (case-sensitive):** [Search input field]
- Show deleted blobs:** [checkbox]
- Actions:** Upload, Change access level, Refresh, Delete, Change tier, Acquire lease, Break lease, View snapshots, Create snapshot, ...

A table below lists blob details with columns: Name, Modified, Access tier, Archive status, Blob type, Size, Lease state. The table shows "No results".

Select **Upload**

The screenshot shows the Azure Storage Explorer interface with the 'Upload blob' dialog box open on the right side. The dialog has the following sections:

- Upload blob:** A title bar with a close button.
- File upload area:** A large dashed rectangular area with a cloud icon and the text "Drag and drop files here or Browse for files".
- Advanced options:** A section with a checkbox labeled "Overwrite if files already exist" and a "Advanced" dropdown menu.
- Buttons:** A "Upload" button at the bottom and a "Give feedback" link.

The left side of the screen shows the same container overview as the previous screenshot, with the 'Upload' button highlighted in the toolbar.

Browse to files and select a file. Browse to a file of your choice

The screenshot shows the Azure Storage Blob upload interface. On the left, there's a sidebar with navigation links like Home, companypublicwebsite, Containers, public Container, Overview, Diagnose and solve problems, Access Control (IAM), Settings, Shared access tokens, Access policy, Properties, and Metadata. The main area has tabs for Upload, Change access level, Refresh, Delete, Change tier, Acquire lease, Break lease, View snapshots, Create snapshot, and a search bar for blobs by prefix. A central modal window titled "Upload blob" shows a cloud icon and a message saying "1 file(s) selected: File to Test.txt". It also includes a "Drag and drop files here or Browse for files" button, an "Advanced" section with an "Upload" button, and a "Give feedback" link.

Select Upload

The screenshot shows the Azure Storage Blob list view. The sidebar is identical to the previous screenshot. The main area displays a table with columns: Name, Modified, Access tier, Archive status, Blob type, Size, and Lease state. There is one entry: "File to Test.txt" with details: Modified: 20/01/2024, 22:56:48, Access tier: Hot (Inferred), Archive status: Not yet archived, Blob type: Block blob, Size: 20 B, Lease state: Available. At the bottom of the table, there are three dots (...). A URL "https://portal.azure.com/#" is visible at the bottom of the browser window.

Step 7 - Determine the URL for your uploaded file. Open a browser and test the URL
Select the uploaded file On the **Overview** tab, copy the **URL**

The screenshot shows the Azure Storage Explorer interface. On the left, there's a sidebar with options like 'Search', 'Upload', 'Change access level', 'Overview', 'Diagnose and solve problems', 'Access Control (IAM)', 'Shared access tokens', 'Access policy', 'Properties', and 'Metadata'. The main area is titled 'File to Test.txt' and shows the blob's properties. The 'Overview' tab is selected. Key details include:

Property	Value
URL	https://companypublicwebsite.blob.core.windows.net/public/File%20to%20Test.txt
LAST MODIFIED	20/01/2024, 10:56:48 pm
CREATION TIME	20/01/2024, 10:56:48 pm
VERSION ID	-
TYPE	Block blob
SIZE	20 B
ACCESS TIER	Hot (Inferred)
ARCHIVE STATUS	-
REHYDRATE PRIORITY	-
SERVER ENCRYPTED	true
ETAG	0x8DC1A0B153086C2
VERSION-LEVEL IMMUTABILITY POLICY	Disabled
CACHE-CONTROL	(empty)
CONTENT-TYPE	text/plain
CONTENT-MD5	Pej4sNyUuMjjD6uewLoFBg==
CONTENT-ENCODING	(empty)
CONTENT-LANGUAGE	(empty)
CONTENT-DISPOSITION	(empty)
LEASE STATUS	Unlocked
LEASE STATE	Available
LEASE DURATION	-
COPY STATUS	-
COPY COMPLETION TIME	-

At the bottom, there are buttons for 'Undelete' and 'Metadata'.

Paste the URL into a new browser tab

The screenshot shows a Microsoft Edge browser window with a single tab titled 'File to Test.txt - Microsoft Edge'. The address bar shows the URL: <https://companypublicwebsite.blob.core.windows.net/public/File%20to%20Test.txt>. The page content is a simple text message: 'this is a test file.'

Step 8 - Configure soft delete

It's important that the website documents can be restored if they're deleted. Configure blob soft delete for 21 days.

Go to the **Overview** blade of the **storage account**

The screenshot shows the Azure Storage Account Overview page for 'companypublicwebsite'. In the 'Properties' tab, under the 'Blob service' section, 'Blob soft delete' is listed as 'Disabled'. In the 'Security' section, 'Require secure transfer for REST API operations' and 'Storage account key access' are both set to 'Enabled'. Other settings like 'Hierarchical namespace', 'Default access tier', and 'Container soft delete' are also visible.

On the **Properties** page, locate the **Blob service** section Select the **Blob soft delete** setting

The screenshot shows the Azure Storage Account Data protection page for 'companypublicwebsite'. The 'Data protection' section is selected. Under the 'Access control' heading, the 'Enable version-level immutability support' checkbox is checked. Other sections like 'Recovery' and 'Tracking' are also visible.

Ensure the **Enable soft delete for blobs** is checked

Change the **Keep deleted blobs for (in days)** setting is **21**

Notice you can also **Enable soft delete for containers** leave this option unchecked and click save

The screenshot shows the 'Data protection' section of the Azure Storage account settings for 'companypublicwebsite'. The 'Enable soft delete for blobs' checkbox is checked, and the 'Keep deleted blobs for (in days)' field is set to 21. Other options like 'Enable point-in-time restore for containers' and 'Enable permanent delete for soft deleted items' are unchecked. The 'Save' button is visible at the bottom.

Test is soft delete is working

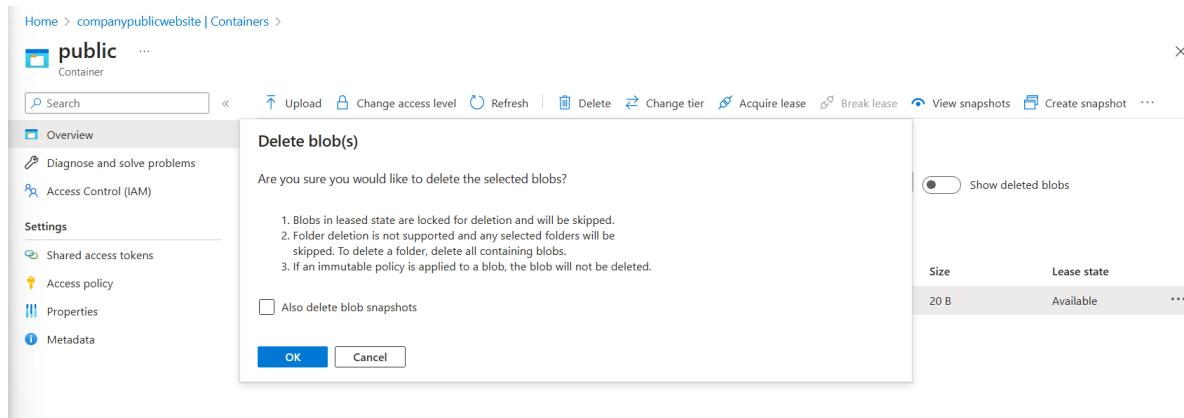
Navigate to the container where you uploaded a file

The screenshot shows the 'Containers' section of the Azure Storage account settings for 'public'. The 'File to Test.txt' blob is listed in the table. The 'Delete' button next to it is highlighted, indicating it is selected for deletion.

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
File to Test.txt	20/01/2024, 22:56:48	Hot (Inferred)		Block blob	20 B	Available

Select the file uploaded and then select **Delete**

Select **OK** to confirm deleting the file



The screenshot shows the 'Overview' page of a container named 'public'. It displays a table of blobs with one entry: 'No results'. Above the table, there is a search bar 'Search blobs by prefix (case-sensitive)' and a toggle switch labeled 'Show deleted blobs' which is currently off. The left sidebar includes sections for Overview, Diagnose and solve problems, Access Control (IAM), Settings (Shared access tokens, Access policy, Properties, Metadata), and a note about the authentication method being 'Access key'.

On the container **Overview** page, toggle the slider **Show deleted blobs**. This toggle is to the right of the search box

The screenshot shows the 'Overview' page of a container named 'public'. It displays a table of blobs with one entry: 'File to Test.txt'. The row for this file includes columns for Name, Status (showing 'Deleted'), Retention (20 days), Modified (20/01/2024, 22:56:48), Access tier (Hot (Inferred)), and Archive status (Blo). Above the table, there is a search bar 'Search blobs by prefix (case-sensitive)' and a toggle switch labeled 'Show deleted blobs' which is now turned on. The left sidebar includes sections for Overview, Diagnose and solve problems, Access Control (IAM), Settings (Shared access tokens, Access policy, Properties, Metadata), and a note about the authentication method being 'Access key'.

Select deleted file, and use the ellipses on the far right, to **Undelete** the file

The screenshot shows the 'Overview' blade for a storage container named 'public'. In the main table, there is one row for a blob named 'File to Test.txt'. The 'Status' column shows a red 'Delete' icon. To the right of the table, a context menu is open over the blob row, with the 'Undelete' option highlighted.

Refresh the container and confirm the file has been restored

The screenshot shows the 'Overview' blade for the same 'public' storage container. The table now displays the restored blob 'File to Test.txt' with a green checkmark in the 'Status' column. The context menu is no longer visible.

Step 9 - Configure blob versioning

It's important to keep track of the different website product document versions

Go to the **Overview** blade of the **storage account**

The screenshot shows the 'Overview' blade for a storage account named 'companypublicwebsite'. The blade includes sections for 'Essentials', 'Blob service', 'File service', and 'Networking'. Under 'Blob service', the 'Versioning' setting is set to 'Enabled'. The 'File service' section shows 'Large file share' as 'Disabled'. The 'Networking' section shows 'Allow access from' as 'All networks'.

In the **Properties** section, locate the **Blob service** section

Select the **Versioning** setting

The screenshot shows the 'Data protection' settings for a storage account named 'companypublicwebsite'. The 'Blob service' section is selected. Under 'Versioning', the checkbox 'Enable versioning for blobs' is checked. A note below it says 'Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle.' Below the checkbox, there is a dropdown menu set to 'Keep all versions'.

Ensure the **Enable versioning for blobs** checkbox is checked

Options to **keep all versions** or **delete versions after** select **Keep all versions**

This screenshot is identical to the one above, showing the 'Data protection' settings for the same storage account. The 'Blob service' section is selected, and the 'Enable versioning for blobs' checkbox is checked. The dropdown menu at the bottom is set to 'Keep all versions'.

Experiment with restoring previous blob versions

Upload another version of your container file. This overwrites your existing file

The screenshot shows the Azure Storage Blob upload interface. On the left, there's a sidebar with navigation links like Home, companypublicwebsite | Containers, public Container, Overview, Diagnose and solve problems, Access Control (IAM), Settings, Shared access tokens, Access policy, Properties, and Metadata. The main area has tabs for Upload, Change access level, Refresh, Delete, and Change tier. It also includes sections for Authentication method (Access key, Switch to Microsoft Entra user account) and Location (public). A search bar says 'Search blobs by prefix (case-sensitive)' and a filter section says 'Add Filter'. Below these are tables for Name, Modified, Access tier, and Arc. One row shows 'File to Test.txt' with a modified date of 20/01/2024, 22:56:48 and a Hot (Inferred) access tier. To the right, a modal window titled 'Upload blob' shows a cloud icon and a message '1 file(s) selected: File to Test.txt'. It has a checkbox 'Overwrite if files already exist' which is checked. At the bottom are 'Upload' and 'Give feedback' buttons.

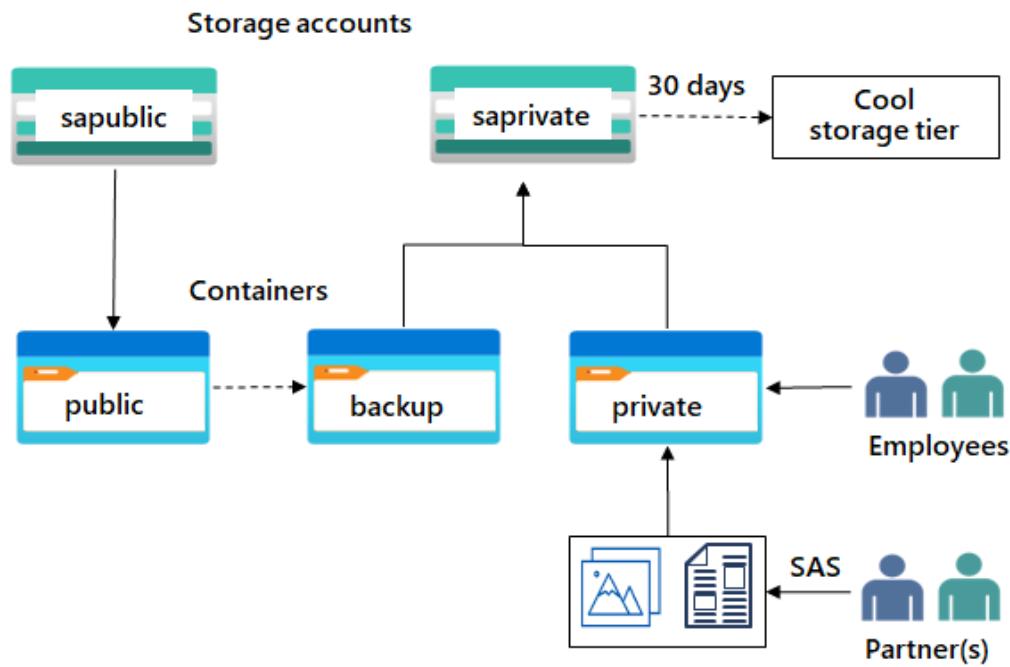
Your previous file version is listed on **Show deleted blobs** page

The screenshot shows the Azure Storage Blob Versions page for 'File to Test.txt'. The left sidebar is identical to the previous screenshot. The main area has tabs for Refresh, Download, Make current version, Delete, and Change tier. Below these are tabs for Overview, Versions (which is selected), Snapshots, Edit, and Generate SAS. There's a 'Show deleted versions' toggle switch which is turned on. A table lists blob versions with columns for Version Id, Status, Retention (days), Modified, and Access tier. One entry is shown: '2024-01-20T22:56:48.22320...', Status 'Previous version', Retention '-' days, Modified '20/01/2024, 10:56:48...', and Access tier 'Hot'.

Provide private storage for internal company documents

The company needs storage for their offices and departments. This content is private to the company and shouldn't be shared without consent. This storage requires high availability if there's a regional outage. The company wants to use this storage to back up the public website storage.

Architecture diagram



Task to be Completed

- Create a storage account for the company private documents.
- Configure redundancy for the storage account.
- Configure a shared access signature so partners have restricted access to a file.
- Back up the public website storage.
- Implement lifecycle management to move content to the cool tier.

Step 1 - Create storage account – Same storage account used for companypublicwebsite

The screenshot shows the Azure Storage Account Overview page for 'companypublicwebsite'. Key details include:

- Resource group (move)**: publicwebsitesstoragerg
- Location**: eastus
- Primary/Secondary Location**: Primary: East US, Secondary: West US
- Subscription (move)**: Pay-As-You-Go
- Subscription ID**: 8148d5d5-df15-44ef-beb3-5960d3dc42eb
- Disk state**: Primary: Available, Secondary: Available
- Tags (edit)**: Add tags

Properties tab selected. Other tabs include Monitoring, Capabilities (7), Recommendations (0), Tutorials, and Tools + SDKs.

Blob service configuration:

- Hierarchical namespace: Disabled
- Default access tier: Hot
- Blob anonymous access: Enabled
- Blob soft delete: Enabled (21 days)
- Container soft delete: Disabled
- Versioning: Enabled
- Change feed: Disabled
- NFS v3: Disabled
- Allow cross-tenant replication: Disabled

File service configuration:

- Large file share: Disabled
- Identity-based access: Not configured
- Default share-level permissions: Disabled
- Soft delete: Disabled
- Share capacity: 5 TiB

Queue service configuration:

- None listed

Security configuration:

- Require secure transfer for REST API operations: Enabled
- Storage account key access: Enabled
- Minimum TLS version: Version 1.2
- Infrastructure encryption: Disabled

Networking configuration:

- Allow access from: All networks
- Number of private endpoint connections: 0
- Network routing: Microsoft network routing
- Access for trusted Microsoft services: Yes
- Endpoint type: Standard

Step 2 Create a storage container, upload a file, and restrict access to the file

Create a private storage container for the corporate data

In the storage account, in the **Data storage** section, select the **Containers** blade

Select + Container

The **Name** of the container is **corporate data**

The screenshot shows the Azure Storage Account Containers blade. The 'Containers' blade is selected in the left sidebar. Two containers are listed:

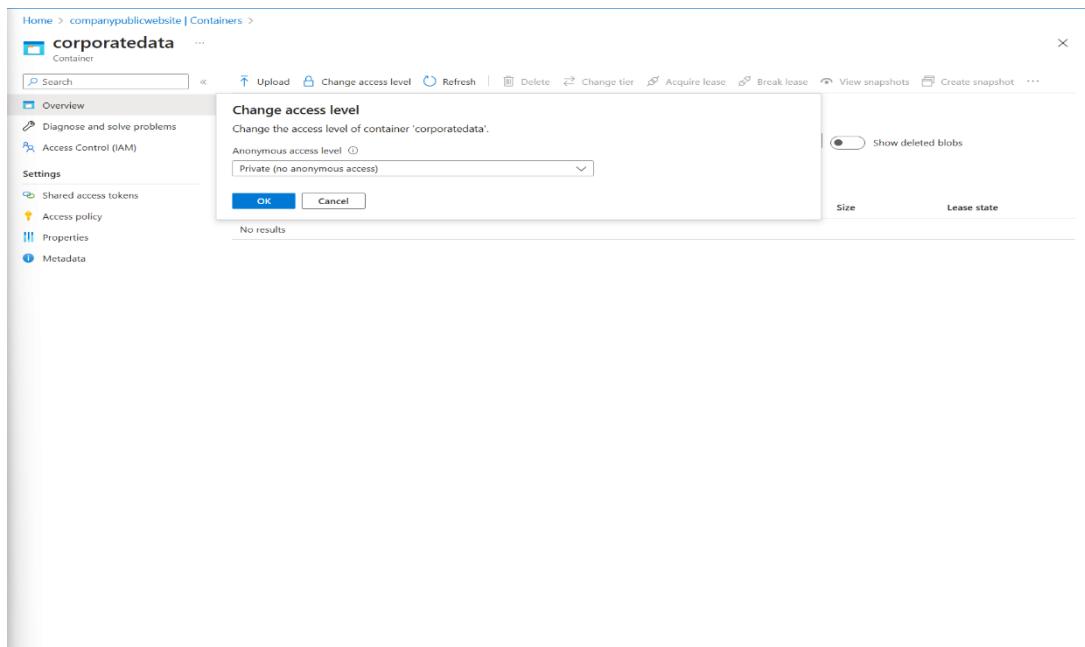
Name	Last modified	Anonymous access level
logs	20/01/2024, 22:30:18	Private
public	20/01/2024, 22:52:24	Public

A 'New container' dialog box is open on the right, showing the following configuration:

- Name**: corporatedata
- Anonymous access level**: Private (no anonymous access)

At the bottom of the dialog, there are 'Create' and 'Give feedback' buttons.

Ensure the Public access level is Private (no anonymous access)

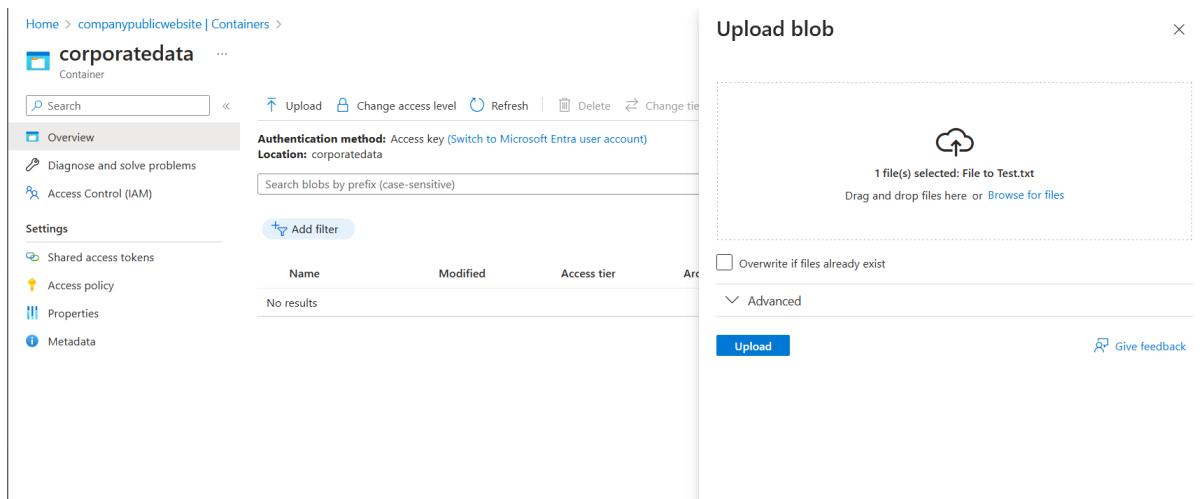


The screenshot shows the 'corporatedata' container settings in the Azure Storage portal. A modal dialog titled 'Change access level' is open, prompting the user to change the access level of the container. The dropdown menu for 'Anonymous access level' is set to 'Private (no anonymous access)'. There are 'OK' and 'Cancel' buttons at the bottom of the dialog. The main container settings page shows a sidebar with options like Overview, Diagnose and solve problems, Access Control (IAM), Settings, Shared access tokens, Access policy, Properties, and Metadata. The 'Overview' tab is selected.

Step 3 - For testing, upload a file to the private container. The type of file doesn't matter. A small image or text file is a good choice. Test to ensure the file isn't publicly accessible

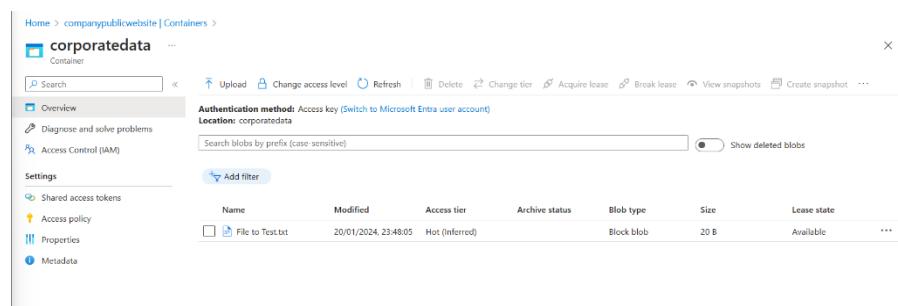
Select the container

Select **Upload**



The screenshot shows the 'corporatedata' container settings page with the 'Upload' button highlighted. To the right, a separate 'Upload blob' dialog is open, showing a file named 'File to Test.txt' being uploaded. The dialog includes fields for overwriting existing files and an 'Advanced' section, with an 'Upload' button at the bottom.

Upload the file



The screenshot shows the 'corporatedata' container settings page with the uploaded file 'File to Test.txt' listed in the blob list. The file details are: Name: File to Test.txt, Modified: 20/01/2024, 23:48:05, Access tier: Hot (Inferred), Archive status: Not yet archived, Blob type: Block blob, Size: 20 B, Lease state: Available. The 'Upload' button is also visible in the top bar.

Select the uploaded file

On the **Overview** tab, copy the URL

The screenshot shows the Azure Storage Blob service interface. On the left, the 'corporatedata' container is selected. In the center, the properties for the 'File to Test.txt' blob are displayed. The 'Overview' tab is selected. Key details shown include:

- Authentication method:** Access key (Switch to Microsoft Entra user account)
- Location:** corporatedata
- URL:** https://companypublicwebsite.blob.core.windows.net/corporatedata/File to Test.txt
- LAST MODIFIED:** 20/01/2024, 11:48:05 pm
- CREATION TIME:** 20/01/2024, 11:48:05 pm
- VERSION ID:** 2024-01-20T23:48:05.7652598Z
- TYPE:** Block blob
- SIZE:** 20 B
- ACCESS TIER:** Hot (Inferred)
- ACCESS TIER LAST MODIFIED:** N/A
- ARCHIVE STATUS:** -
- REHYDRATE PRIORITY:** -
- SERVER ENCRYPTED:** true
- ETAG:** 0x8DC1A123F8C2D76
- VERSION-LEVEL IMMUTABILITY POLICY:** Disabled
- CACHE-CONTROL:** (empty)
- CONTENT-TYPE:** text/plain
- CONTENT-MDS:** Pej4sNyUuMjjD6uewLoFBg==
- CONTENT-ENCODING:** (empty)
- CONTENT-LANGUAGE:** (empty)
- CONTENT-DISPOSITION:** (empty)
- LEASE STATUS:** Unlocked
- LEASE STATE:** Available
- LEASE DURATION:** -
- COPY STATUS:** -
- COPY COMPLETION TIME:** -

At the bottom, there is a blue 'Undelete' button and a 'Metadata' section.

Paste the URL into a new browser tab Verify the file doesn't display and you receive an error

The screenshot shows a Microsoft Edge browser window with the URL https://companypublicwebsite.blob.core.windows.net/corporatedata/File to Test.txt. The page displays an XML error message:

```
<Error>
<Code>ResourceNotFound</Code>
<Message>
The specified resource does not exist. RequestId:bd52e0e5-a01e-0006-7fb-4b60aa000000 Time:2024-01-20T23:50:07.1873420Z
</Message>
</Error>
```

Step 4 - An external partner requires read and write access to the file for at least the next 24 hours.

Configure and test a shared access signature (SAS)

Select uploaded blob file and move to the **Generate SAS** tab

In the **Permissions** drop-down, ensure the partner has only **Read** permission

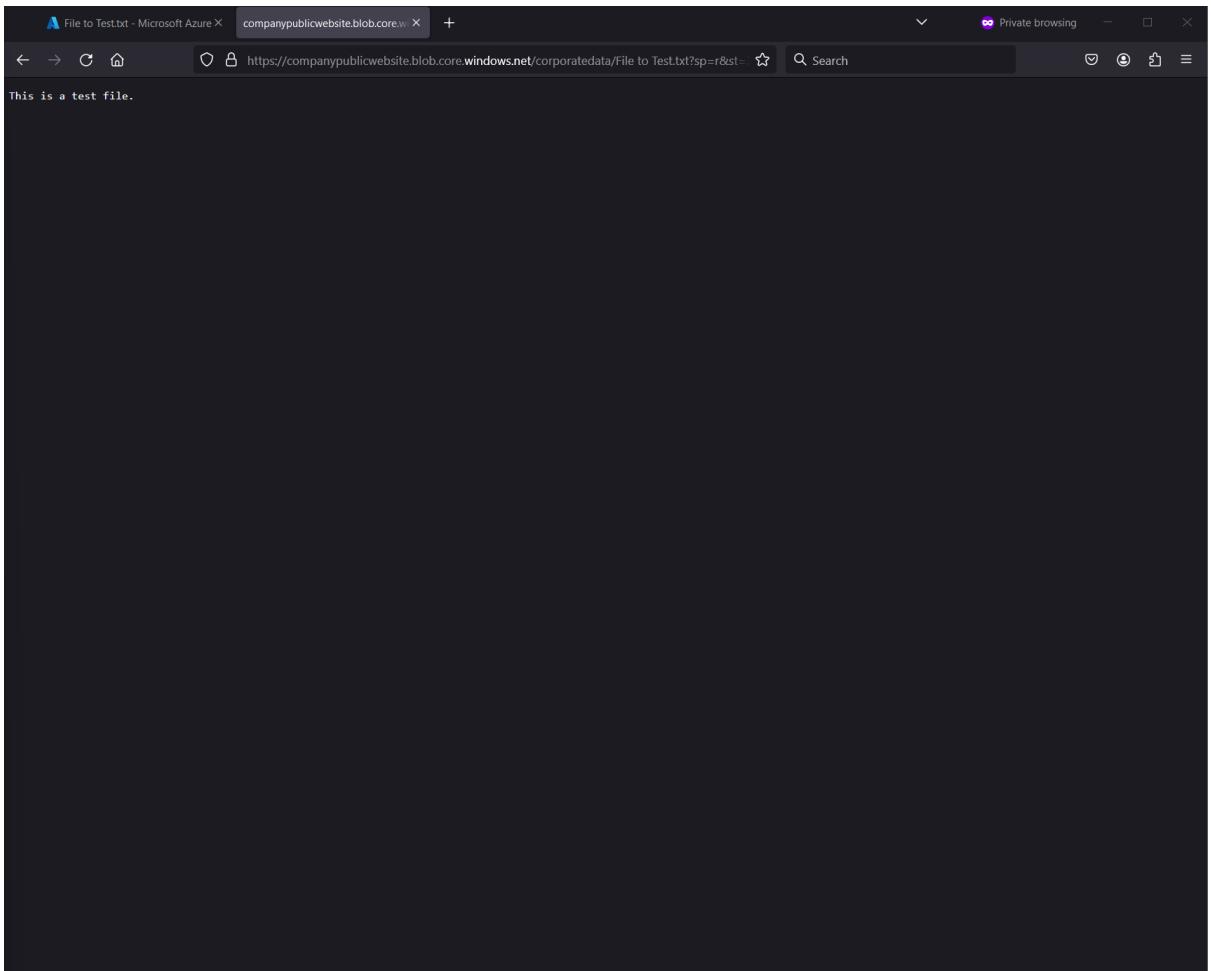
Verify the **Start and expiry date/time** is for the next 24 hours

Select **Generate SAS token and URL**

The screenshot shows the Azure Storage Blob properties for 'File to Test.txt'. The 'Generate SAS' tab is active. The 'Permissions' dropdown is set to 'Read'. The 'Start' and 'Expiry' fields are both set to 20/01/2024 23:49:25. The 'Generate SAS token and URL' button is visible at the bottom.

The screenshot shows the Azure Storage Blob properties for 'File to Test.txt'. The 'Generate SAS token and URL' button is highlighted. Below it, the 'Blob SAS token' and 'Blob SAS URL' fields are populated with the generated SAS information.

Copy the **Blob SAS URL** to a new browser tab



Verify you can access the file. If you have uploaded an image file it will display in the browser. Other file types will be downloaded.

Step 5 - Configure storage access tiers and content replication

To save on costs, after 30 days, move blobs from the hot tier to the cool tier.

Return to the **storage account**

In the **Overview** section, notice the **Default access tier** is set to **Hot**

[Next Image](#)

companypublicwebsite Storage account

Properties

Blob service

Hierarchical namespace	Disabled
Default access tier	Hot
Blob anonymous access	Enabled
Blob soft delete	Enabled (21 days)
Container soft delete	Disabled
Versioning	Enabled
Change feed	Disabled
NFS v3	Disabled
Allow cross-tenant replication	Disabled

File service

Large file share	Disabled
Identity-based access	Not configured
Default share-level permissions	Disabled
Soft delete	Disabled
Share capacity	5 TiB

Queue service

In the Data management section, select the Lifecycle management blade

Lifecycle management

List View

Name	Status	Blob type
No rules		

Code View

```
lifecycle_rule rule1 {
    blob_type = All blob types
    condition {
        blob_age_days >= 30
    }
    actions {
        archive
    }
}
```

Settings

- Configuration
- Data Lake Gen2 upgrade
- Resource sharing (CORS)
- Advisor recommendations
- Endpoints
- Locks

Select Add rule

Set the **Rule name** to movetocool

Set the **Rule scope** to **Apply rule to all blobs in the storage account**

Home > companypublicwebsite | Lifecycle management > Add a rule ...

Details **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

Blob subtype *

Base blobs

Snapshots

Versions

Previous **Next**

Select **Next**

Set **More than (days ago)** to **30**

In the **Then** drop-down select **Move to cool storage**

Home > companypublicwebsite | Lifecycle management > Add a rule ...

Details **Base blobs**

Lifecycle management uses your rules to automatically move blobs to cooler tiers or to delete them. If you create multiple rules, the associated actions must be implemented in tier order (from hot to cool storage, then archive, then deletion).

If

Base blobs were *

Last modified

Created

More than (days ago) *

30

Then

Move to cool storage

+ Add conditions

Previous **Add**

Add the rule.

Home > companypublicwebsite

companypublicwebsite | Lifecycle management ⚡ ⋮

Storage account

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 policy may take up to 48 hours to complete. [Learn more](#)

List View Code View

Enable access tracking ⓘ

Name	Status	Blob type
movetocool	Enabled	Block

File shares

Queues

Tables

Security + networking

- Networking
- Front Door and CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

Data management

- Redundancy
- Data protection
- Object replication
- Blob inventory
- Static website
- Lifecycle management**
- Azure AI Search

Settings

- Configuration
- Data Lake Gen2 upgrade
- Resource sharing (CORS)
- Advisor recommendations
- Endpoints
- Locks

Step 5 - The public website files need to be backed up to another storage account – Configure object replication

Create a new container called backup in **azurestorageproject01** storage account

Home > azurestorageproject01

azurestorageproject01 | Containers ⚡ ⋮

Storage account

Search

+ Container □ Change access level ⏪ Restore containers ⏪ Refresh | 🗑 Delete ⏭ Give feedback

Search containers by prefix

Name	Last modified	Actions
Slogs	20/01/2024, 21:56:43	⋮

New container

Name * ✓

Anonymous access level ⓘ

Private (no anonymous access)

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

Advanced

Create ⏭ Give feedback ↗

Containers

File shares

Queues

Tables

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage browser

Storage Mover

Security + networking

- Networking
- Front Door and CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

Data management

- Redundancy
- Data protection
- Object replication

<https://portal.azure.com/#>

Confirm back up container created.

The screenshot shows the 'Containers' blade in the Azure Storage account 'azurestorageproject01'. The left sidebar contains navigation links for Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Data storage (Containers, File shares, Queues, Tables), Security + networking (Networking, Front Door and CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud), and Data management (Redundancy, Data protection, Object replication, Blob inventory). The 'Containers' link under Data storage is selected. The main area displays a table with columns: Name, Last modified, Anonymous access level, and Lease state. Two containers are listed:

Name	Last modified	Anonymous access level	Lease state
Logs	20/01/2024, 21:56:43	Private	Available
backup	21/01/2024, 00:09:53	Private	Available

Step 5 – Configure object replication settings on companypublicwebsite storage account

In the **Data management** section, select the **Object replication** blade.

The screenshot shows the 'Object replication' blade in the Azure Storage account 'companypublicwebsite'. The left sidebar contains the same navigation links as the previous screenshot. The 'Object replication' link under Data management is selected. The main area has two sections: 'Your accounts' (which is currently selected) and 'Other accounts'. Below these are two tables: 'Objects copied from this account' and 'Objects copied into this account'. Both tables show 'No replication policies found'.

Destination account	Source container	Destination container	Filters
No replication policies found			

Source account	Source container	Destination container	Filters
No replication policies found			

Select **Create replication rules**

Set the **Destination storage account** to the **private** storage account

Set the **Source container** to **public** and the **Destination container** to **backup**

Home > companypublicwebsite | Object replication >

Create replication rules

When you create object replication rules, blob change feed and blob versioning are automatically enabled for the source and destination storage accounts. Enabling these features may increase costs. →

Destination details

To begin replicating objects, specify the source storage account and the destination storage account.

Learn more about copying objects in object replication ↗

Destination subscription * Pay-As-You-Go

Destination storage account * azurestorageproject01
Don't see your account? ↗

Container pair details

A container pair consists of a container in the source account and a container in the destination account. Objects in the source container are copied over to the destination container according to the replication rule. You can optionally filter which objects are copied by specifying a prefix match and by copying objects created only after a specified date and time.

Source container	Destination container	Filters	Copy over
public	backup	0 (add)	Only new objects (change)
Select a source container	Select a destination container		

To configure more than 10 container pairs (up to 1000), see [Configure object replication using a JSON file](#) ↗

Create **Cancel**

Create the replication rule

Uploaded file UserCreateTemplate.csv to public container on company public website as test

Home > companypublicwebsite | Containers >

public

Container

Search

Upload Change access level Refresh Delete Change tier Acquire lease Break lease View snapshots Create snapshot ...

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

Search blobs by prefix (case-sensitive)

Show deleted blobs

Add filter

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
File to Test.txt	20/01/2024, 23:29:56	Hot (Inferred)		Block blob	20 B	Available
UserCreateTemplate.csv	21/01/2024, 00:16:35	Hot (Inferred)		Block blob	574 B	Available

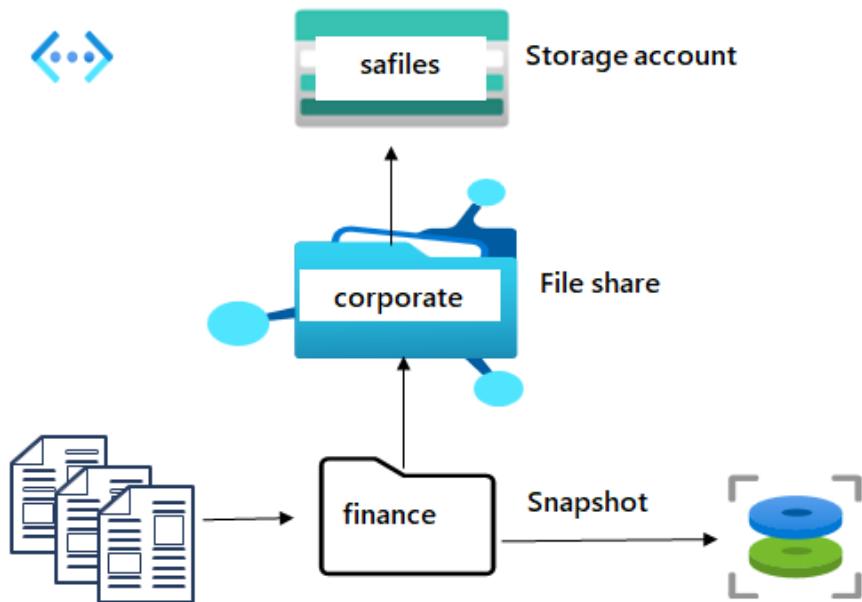
To check replication went back to destination back up storage account azurestorageproject01 and in the back up container file UserCreateTemplate.csv is listed in container showing it was replicated to storage account successfully.

The screenshot shows the Azure Storage Explorer interface. The left sidebar has a tree view with 'Home > azurestorageproject01 | Containers > backup'. The main area is titled 'Overview' for the 'backup' container. It shows a search bar, navigation buttons (Upload, Change access level, Refresh, Delete, Change tier, Acquire lease, Break lease, View snapshots, Create snapshot), and a message about authentication. Below these are sections for 'Diagnose and solve problems', 'Access Control (IAM)', and 'Settings' (Shared access tokens, Access policy, Properties, Metadata). A table lists blobs: 'UserCreateTemplate.csv' (Modified: 21/01/2024, 00:18:46, Access tier: Hot (Inferred), Archive status: Not yet archived, Blob type: Block blob, Size: 574 B, Lease state: Available). There are also buttons for 'Add filter' and 'Show deleted blobs'.

Provide shared file storage for the company offices

The company is geographically dispersed with offices in different locations. These offices need a way to share files and disseminate information. For example, the Finance department needs to confirm cost information for auditing and compliance. This file shares should be easy to access and load without delay. Some content should only be accessed from selected corporate virtual networks.

Architecture diagram



Task to be completed

- Create a storage account specifically for file shares.
- Configure a file share and directory.
- Configure snapshots and practice restoring files.
- Restrict access to a specific virtual network and subnet.

Step 1 - Create and configure a storage account for Azure Files.

Create a storage account for the finance department's shared files with the following options

Home > Storage accounts >

Create a storage account ...

[X](#)

[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 * [View](#)

Resource group * [View](#) [Create new](#)

Instance details

Storage account name * [View](#)

Region * [View](#)

[Deploy to an edge zone](#)

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

Premium account type * [View](#)

Redundancy * [View](#)

[Review](#) [< Previous](#) [Next : Advanced >](#) [Give feedback](#)

Home > Storage accounts >

Create a storage account ...

[X](#)

[Basics](#) [Advanced](#) [Networking](#) [Data protection](#) [Encryption](#) [Tags](#) [Review](#)

Basics

Subscription	Pay-As-You-Go
Resource Group	storagergproject
Location	eastus
Storage account name	safilesproject
Deployment model	Resource manager
Performance	Premium
Premium account type	File shares
Replication	Zone-redundant storage (ZRS)

Advanced

Enable hierarchical namespace	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Enable SFTP	Disabled
Large file shares	Enabled

Networking

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

Security

Secure transfer	Enabled
Allow storage account key access	Enabled
Default to Microsoft Entra authentication in	Disabled

[Create](#) [< Previous](#) [Next >](#) [Download a template for automation](#) [Give feedback](#)

Review and create

Home > safileoproject_1705796875260 | Overview >

safileoproject Storage account

Upload Open in Explorer Delete Move Refresh Open in mobile Feedback

Overview

Resource group (move) : storagegroupproject

Location : eastus

Subscription (move) : Pay-As-You-Go

Subscription ID : 8148d5d5-df15-44ef-beb3-5960d3dc42eb

Disk state : Available

Tags (edit) : Add tags

Properties Monitoring Capabilities (2) Recommendations (0) Tutorials Tools + SDKs

File service

Large file share	Enabled	Allow access from	All networks
Identity-based access	Not configured	Number of private endpoint connections	0
Default share-level permissions	Disabled	Network routing	Microsoft network routing
Soft delete	Disabled	Access for trusted Microsoft services	Yes
SMB Multichannel	Disabled	Endpoint type	Standard

Networking

Require secure transfer for REST API operations	Enabled
Storage account key access	Enabled
Minimum TLS version	Version 1.2
Infrastructure encryption	Disabled

Security

Identity-based access	Not configured
Default share-level permissions	Disabled
Soft delete	Disabled
SMB Multichannel	Disabled

JSON View

Step 2 - Create and configure a file share with directory

Create a file share for the corporate office

In the storage account, in the **Data storage** section, select the **File shares** blad

Home > safileoproject_1705796875260 | Overview > safileoproject

safileoproject | File shares Storage account

File share settings

Identity-based access: Not configured Default share-level permissions: Disabled Soft delete: Disabled SMB Multichannel: Disabled

Security: Maximum compatibility

Search file shares by prefix (case-sensitive)

Show deleted shares

Name	Protocol	Provisioned capacity
You don't have any file shares yet. Click '+ File share' to get started.		

Select + File share and provide a Name

Home > safesproject_1705796875260 | Overview > safesproject | File shares >

New file share ...

[X](#)

[Basics](#) [Backup](#) [Review + create](#)

A premium file share is billed by provisioned share size, regardless of the used capacity. [Learn more](#)

- The minimum share size is 100 GiB.
- Provision more capacity to get more performance.

Name *

Provisioned capacity * [Set to maximum](#)

Performance

Maximum IO/s	4024
Burst IO/s	10000
Throughput rate	203.0 MiB / s
Maximum capacity	100 TiB

Protocol SMB NFS

To use the SMB protocol with this share, check if you can communicate over port 445. These scripts for [Windows clients](#) and [Linux clients](#) can help. Learn how to [circumvent port 445 issues](#).

[Review + create](#) [< Previous](#) [Next : Backup >](#) [Give feedback](#)

Review and create

Home > safesproject_1705796875260 | Overview > safesproject | File shares > New file share >

fileshareproject

SMB File share

[Search](#) [Connect](#) [Upload](#) [Refresh](#) [Add directory](#) [Delete share](#) [Change size and performance](#) [Give feedback](#)

[Overview](#) [Diagnose and solve problems](#) [Access Control \(IAM\)](#) [Browse](#) [Snapshots](#) [Backup](#) [Monitoring](#) [Metrics](#)

Enable Backup for file share "fileshareproject" to protect your data. [Learn more](#)

[JSON View](#)

Storage account	: safesproject	Share URL	: https://safesproject.file.core.windows.net/fileshareproj...
Resource group (move)	: storagergproject	Redundancy	: Zone-redundant storage (ZRS)
Location	: East US	Configuration modified	: 21/01/2024, 00:34:46
Subscription (move)	: Pay-As-You-Go		
Subscription ID	: 8148d5d5-df15-44ef-beb3-5960d3dc42eb		

[Properties](#) [Monitoring](#) [Capabilities \(2\)](#) [Tutorials](#)

Size

Provisioned capacity	1 TiB
Used capacity	0 B
Tier	Premium

Feature status

Soft delete	Disabled
SMB Multichannel	Disabled
Large file shares	Enabled

Performance

Maximum IO/s	4024
Burst IO/s	10000
Throughput rate	203.0 MiB / s

Identity-based access

Directory service	Not configured
Domain	-

SMB protocol settings

Security profile	Maximum compatibility
SMB protocol versions	-
SMB channel encryption	-
Authentication mechanisms	-
Kerberos ticket encryption	-

Backup

Snapshots	0 snapshots
Last modified	-
Backup	Not configured

Step 3 - Add a directory to the file share for the finance department. For future testing, upload a file
Select your file share and select **+ Add directory**

Name the new directory **finance**

The screenshot shows the 'New directory' dialog box in the Azure portal. The 'Name' field contains 'finance'. Below the dialog is a table with one row:

Name	Type	Size	...
finance	Directory		...

The screenshot shows the 'Browse' view in the Azure portal. The 'Name' column lists a single item: 'finance' (Type: Directory). The '...' column has a single ellipsis icon.

Select **Browse** and then select the **finance** directory

The screenshot shows the 'Browse' view in the Azure portal. The 'Name' column lists a single item: '[...]' (Type: Directory). The '...' column has a single ellipsis icon.

Notice you can **Add directory** to further organize your file share

Upload a file of your choosing

The screenshot shows the Azure portal interface for a file share named 'fileshareproject'. The left sidebar has 'Browse' selected. The main area shows a file named 'UserCreateTemplate.csv' with a size of 574 B. The top navigation bar includes 'Upload', 'Add directory', 'Refresh', 'Delete directory', and 'Properties' buttons.

Step 4 - Configure and test snapshots

Similar to blob storage, you need to protect against accidental deletion of files

Select file share

In the **Operations** section, select the **Snapshots** blade

Select **+ Add snapshot**. The comment is optional. Select **OK**

Select your snapshot and verify your file directory and uploaded file are included

The screenshot shows the Azure portal interface for a file share named 'fileshareproject'. The 'Snapshots' blade is selected. A snapshot named 'finance (2024-01-21T00:43:40.0000000Z)' is listed. The main area shows a file named 'UserCreateTemplate.csv' with a size of 574 B. The top navigation bar includes 'Refresh' and 'Properties' buttons.

Step 5 - using snapshots to restore a file

Return to your **file share**

Browse to your file directory

The screenshot shows the Azure portal interface for a file share named 'fileshareproject'. The 'Browse' blade is selected. A file named 'UserCreateTemplate.csv' is listed. A context menu is open over the file, showing options: Edit, Download, Properties, Edit metadata, Delete, and List handles and leases.

Locate your uploaded file and in the **Properties** pane select **Delete**. Select **Yes** to confirm the deletion

The screenshot shows the 'fileshareproject | Browse' interface. A file named 'UserCreateTemplate.csv' is selected. A delete confirmation dialog box is overlaid on the screen, asking 'Do you want to delete file 'fileshareproject/finance/UserCreateTemplate.csv'? with 'Yes' and 'No' buttons.

The screenshot shows the 'fileshareproject | Browse' interface. The left sidebar shows 'Operations' with 'Snapshots' selected. The main area displays a list of files, including 'UserCreateTemplate.csv'.

Select the **Snapshots** blade and then select your snapshot

The screenshot shows the 'fileshareproject | Snapshots' interface. The left sidebar shows 'Operations' with 'Snapshots' selected. The main area displays a table of snapshots:

Name	Date created	Initiator	Comment
2024-01-21T00:43:40.000000Z	21/01/2024, 12:43:40 am	Manual	-

Navigate to the file you want to restore

The screenshot shows the 'finance (2024-01-21T00:43:40.000000Z) | ...' interface. The left sidebar shows 'Operations' with 'Snapshots' selected. The main area displays a list of files, including 'UserCreateTemplate.csv'.

Select the file and the select **Restore**

The screenshot shows a file properties dialog for 'UserCreateTemplate.csv'. The file was created on 2024-01-21T00:43:40.0000000Z. It has a URL: <https://safesproject.file.core.windows.net/>. The file is 574 B in size and has an ETAG of "0x8DC1A1988A9F45B".

Provide a **Restored file name**

The screenshot shows the 'File properties' dialog with the 'Restore' section open. The file 'UserCreateTemplate.csv' is selected for restoration as a copy and rename. The restored file name is set to 'UserCreateTemplate'. The 'OK' button is highlighted.

Verify file directory has the restored file

The screenshot shows the 'fileshareproject | Browse' interface. The 'Browse' tab is selected in the left sidebar. A file named 'UserCreateTemplate' is listed in the main area, which contains a table with columns: Name, Type, and Size. The file is a File type, 574 B in size.

Step 6 - Configure restricting storage access to selected virtual networks

This section requires a virtual network with subnet. In a production environment these resources would already be created.

Search for and select **Virtual networks**

Select **Create**. Select your resource group, and give the virtual network a **name**

The screenshot shows the 'Create virtual network' wizard in the Azure portal. The current step is 'Basics'. The page includes:

- Project details:** Subscription dropdown set to 'Pay-As-You-Go', Resource group dropdown set to 'storagergproject'.
- Instance details:** Virtual network name input field containing 'filesharevnet', Region dropdown set to '(US) East US'.
- Buttons at the bottom:** 'Previous' (disabled), 'Next', and 'Review + create' (highlighted in blue).
- A 'Give feedback' link in the bottom right corner.

Review and create

Next section configure Vnet settings for file share.

In the **Settings** section, select the **Subnets** blade

The screenshot shows the Azure portal interface for a virtual network named 'fileshareVnet'. On the left, a navigation menu lists various settings like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, and Subnets (which is selected). The main content area displays the 'Subnets' blade for the 'default' subnet. It shows a table with one row: Name (default), IPv4 (10.0.0.0/24), Available IPs (251). Below the table are sections for Subnet address range (10.0.0.0/24), NAT gateway (None), Network security group (None), and Route table (None). A 'SERVICE ENDPOINTS' section is present, showing Microsoft.Storage as the chosen service. At the bottom, there are 'SUBNET DELEGATION' and 'NETWORK POLICY FOR PRIVATE ENDPOINTS' sections, along with 'Save' and 'Cancel' buttons.

Select the **default** subnet

In the **Service endpoints** section choose **Microsoft.Storage** in the **Services** drop-down

This screenshot is identical to the one above, but the 'Services' dropdown in the 'SERVICE ENDPOINTS' section is now set to 'Microsoft.Storage', indicating it has been selected.

Save to save settings to redirect storage traffic to Microsoft backbone network to storage account

Step 7 - The storage account should only be accessed from the virtual network just created

Back to storage account **safilesproject**

In the **Security + networking** section, select the **Networking** blade

Home > Storage accounts > safilesproject

safilesproject | Networking Storage account

Search

Firewalls and virtual networks Private endpoint connections

Save Discard Refresh Give feedback

Public network access

Enabled from all networks

Enabled from selected virtual networks and IP addresses

Disabled

All networks, including the internet, can access this storage account. [Learn more](#)

Network Routing

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference

Microsoft network routing

Internet routing

The current combination of storage account kind, performance, replication, and location does not support network routing.

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Storage browser

Data storage

File shares

Security + networking

Networking

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Data management

Redundancy

Settings

Configuration

Resource sharing (CORS)

Advisor recommendations

Endpoints

Locks

Monitoring

Insights

Change the **Public network access** to **Enabled from selected virtual networks and IP addresses**

Home > Storage accounts > safilesproject

safilesproject | Networking Storage account

Search

Firewalls and virtual networks Private endpoint connections

Save Discard Refresh Give feedback

Firewall settings restricting access to storage services will remain in effect for up to a minute after saving updated settings allowing access.

Public network access

Enabled from all networks

Enabled from selected virtual networks and IP addresses

Disabled

Configure network security for your storage accounts. [Learn more](#)

Virtual networks

+ Add existing virtual network + Add new virtual network

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
No network selected.					

Firewall

Add IP ranges to allow access from the internet or your on-premises networks. [Learn more](#).

Add your client IP address (82.10.15.118)

Address range

IP address or CIDR

Exceptions

Allow Azure services on the trusted services list to access this storage account.

Allow read access to storage logging from any network

Allow read access to storage metrics from any network

Network Routing

Determine how you would like to route your traffic as it travels from its source to an Azure endpoint. Microsoft routing is recommended for most customers.

Routing preference

Microsoft network routing

Internet routing

The current combination of storage account kind, performance, replication, and location does not support network routing.

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Storage browser

Data storage

File shares

Security + networking

Networking

Access keys

Shared access signature

Encryption

Microsoft Defender for Cloud

Data management

Redundancy

Settings

Configuration

Resource sharing (CORS)

Advisor recommendations

Endpoints

Locks

Monitoring

Insights

In the **Virtual networks** section, select **Add existing virtual network**

Select your virtual network and subnet, select **Add**

The screenshot shows the Azure Storage account settings for 'safilesproject'. The left sidebar has 'Networking' selected under 'Security + networking'. The main area shows 'Firewalls and virtual networks' with a 'Virtual networks' section containing a table:

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
fileshareVnet	1			storagergproject	Pay-As-You-Go

To the right, a modal window titled 'Add networks' is open, showing the configuration for adding a new virtual network:

- Subscription:** Pay-As-You-Go
- Virtual networks:** fileshareVnet
- Subnets:** default

Below these fields are sections for 'Public network access' (radio buttons for 'Enabled from all networks', 'Enabled from selected virtual networks and IP addresses', and 'Disabled'), 'Address range' (input field), 'Exceptions' (checkboxes for 'Allow Azure services on the trusted services list to access this storage account.', 'Allow read access to storage logging from any network.', and 'Allow read access to storage metrics from any network.'), and 'Network Routing' (radio buttons for 'Microsoft network routing' and 'Internet routing'). A blue 'Add' button is at the bottom right of the modal.

Save settings

The screenshot shows the same Azure Storage account settings page after saving the changes. The 'Virtual networks' table now includes the newly added entry:

Virtual Network	Subnet	Address range	Endpoint Status	Resource Group	Subscription
fileshareVnet	1			storagergproject	Pay-As-You-Go
safilesVnet	1			safilesproject	Pay-As-You-Go

The rest of the interface remains the same, with the 'Networking' section still selected in the sidebar.

Select the **Storage browser** and navigate to your file share

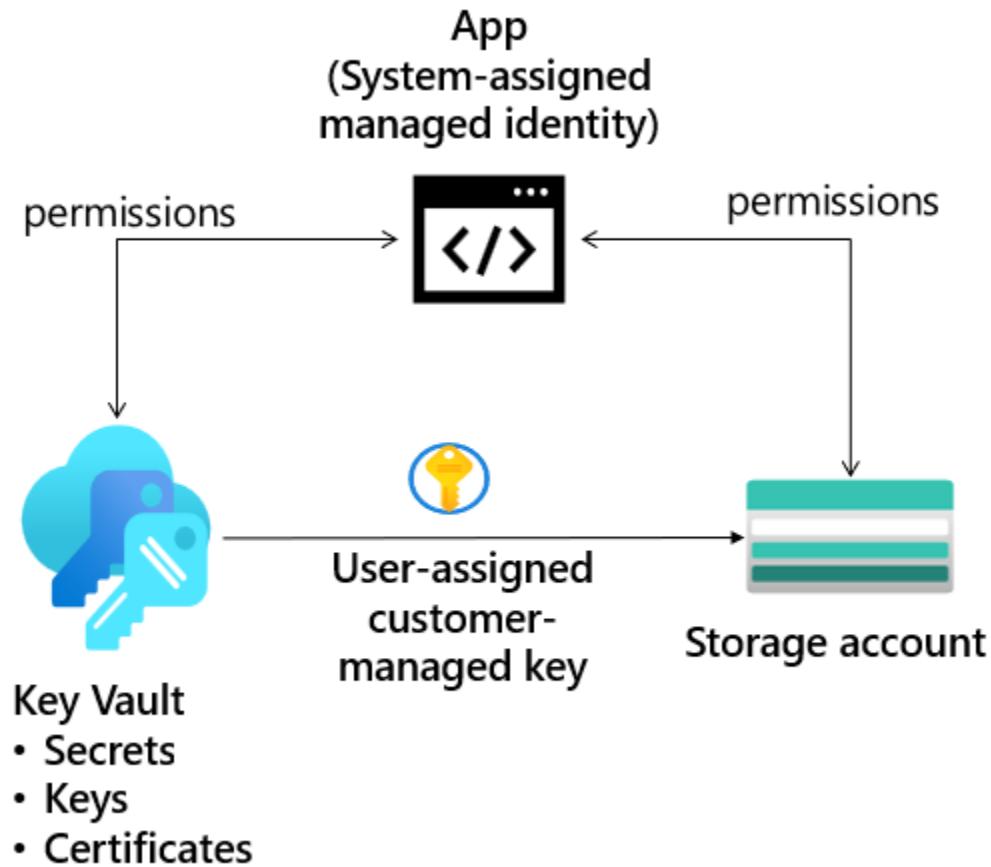
Verify the message *not authorized to perform this operation*. You are not connecting from the virtual network

The screenshot shows the Azure Storage browser interface for the 'saflesproject' storage account. The left sidebar lists various management options like Overview, Activity log, Tags, and Storage browser. The 'Storage browser' option is selected. In the center, under 'File shares', 'fileshareproject' is selected. A large error message box is displayed with the text: 'This request is not authorized to perform this operation.' Below this, the 'Summary' section provides details about the request: Session ID (6b858700023344eb978bdf0847061a09), Extension (Microsoft_Azure_Storage), Error code (403), Resource ID (/subscriptions/8148d5d5-df15-44ef-beb3-5960d3dc42e...), Content (Filesblade), and Storage Request ID (07d75047-a01a-0043-6605-4c3d52000000). The 'Details' section lists two bullet points: 'This request is not authorized to perform this operation. RequestId:07d75047-a01a-0043-6605-4c3d52000000 Time:2024-01-21T01:04:20.0544580Z' and 'This storage account's firewalls and virtual networks' settings may be blocking access to storage services. Try adding your client IP address to the firewall exceptions, or by allowing access from 'all networks' instead of 'selected networks'. Learn more'

Provide storage for a new company app

The company is designing and developing a new app. Developers need to ensure the storage is only accessed using keys and managed identities. The developers would like to use role-based access control. To help with testing, protected immutable storage is needed.

Architecture diagram



Task to be completed

- Create the storage account and managed identity.
- Secure access to the storage account with a key vault and key.
- Configure the storage account to use the customer managed key in the key vault
- Configure a time-based retention policy and an encryption scope.

Step 1 - Create the storage account and managed identity

Create a storage account for the web app with the following options

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 * Pay-As-You-Go

Resource group * storagergproject

[Create new](#)

Instance details

Storage account name * storagefordevs01

Region * (US) East US

[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)

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

[Review](#) < Previous Next : Advanced > [Give feedback](#)

Home > storagefordevs01_1705799284687 | Overview >

storagefordevs01

Storage account

Search

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

Overview

Activity log Tags Diagnose and solve problems Access Control (IAM) Data migration Events Storage browser Storage Mover

Essentials

Resource group (move)	: storagergproject	Performance	: Standard
Location	: eastus	Replication	: Read-access geo-redundant storage (RA-GRS)
Primary/Secondary Location	: Primary: East US, Secondary: West US	Account kind	: StorageV2 (general purpose v2)
Subscription (move)	: Pay-As-You-Go	Provisioning state	: Succeeded
Subscription ID	: 8148d5d5-df15-44ef-beb3-5960d3dc42eb	Created	: 21/01/2024, 01:11:11
Disk state	: Primary: Available, Secondary: Available		
Tags (edit)	: Add tags		

Properties Monitoring Capabilities (7) Recommendations (0) Tutorials Tools + SDKs

Blob service

Hierarchical namespace	: Disabled	Security	Require secure transfer for REST API operations	: Enabled
Default access tier	: Hot	Storage account key access	: Enabled	
Blob anonymous access	: Disabled	Minimum TLS version	: Version 1.2	
Blob soft delete	: Disabled	Infrastructure encryption	: Disabled	
Container soft delete	: Disabled			
Versioning	: Disabled			
Change feed	: Disabled			
NFS v3	: Disabled			
Allow cross-tenant replication	: Disabled			

File service

Large file share	: Disabled	Endpoint type	: Standard
Identity-based access	: Not configured		
Default share-level permissions	: Disabled		
Soft delete	: Disabled		
Share capacity	: 5 TiB		

Networking

Allow access from	: All networks
Number of private endpoint connections	: 0
Network routing	: Microsoft network routing
Access for trusted Microsoft services	: Yes

Queue service

Step 2 - Provide a managed identity for the web app to use

Search for and select **Managed identities**

The screenshot shows the 'Managed Identities' blade in the Azure portal. At the top, there are navigation links ('Home >'), a title ('Managed Identities'), and a 'Default Directory' dropdown. Below the title is a toolbar with icons for 'Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', 'Assign tags', and 'Delete'. A search bar contains the placeholder 'Filter for any field...'. To its right are three filter buttons: 'Subscription equals all', 'Resource group equals all', and 'Location equals all'. A 'Add filter' button is also present. On the far right, there are buttons for 'No grouping' and 'List view'. The main area displays the message 'Showing 0 to 0 of 0 records.' followed by a key icon and the text 'No managed identities to display'. Below this, a note says 'Try changing or clearing your filters.' and two buttons: 'Create managed identity' (blue) and 'Learn more'.

Select **Create**

Select **resource group**

Give your managed identity a name

The screenshot shows the 'Create User Assigned Managed Identity' blade. At the top, it says 'Home > Managed Identities > Create User Assigned Managed Identity'. Below this is a 'Basics' tab, which is selected, and 'Tags' and 'Review + create' tabs. The 'Project details' section asks to select a subscription and resource group. The 'Subscription' dropdown is set to 'Pay-As-You-Go' and the 'Resource group' dropdown is set to 'storagergproject'. The 'Instance details' section asks to select a region and name. The 'Region' dropdown is set to 'East US' and the 'Name' dropdown is set to 'Identityforstoragewebapp'. At the bottom, there are 'Previous' and 'Next' buttons, and a prominent 'Review + create' button.

Review and create

Home > Microsoft.ManagedIdentity-20240121011103 | Overview >

identityforstoragegewebapp | Overview

Managed Identity

<> Delete

- Overview**
- Activity log
- Access control (IAM)
- Tags
- Azure role assignments
- Associated resources (preview)

Essentials

Type : Microsoft.ManagedIdentity/UserAssignedIdentities
 Client ID : Da391258-04ac-45e4-89ea-4865563bb104
 Object (principal) ID : e8387caa-e2fe-4c00-a73b-0f6cf2b16130

Resource group : storagergproject
 Location : East US
 Subscription : Pay-As-You-Go
 Subscription ID : 8148d5d5-df15-44ef-beb3-5960d3dc42eb

JSON View

- Settings
 - Federated credentials
 - Properties
 - Locks
- Monitoring
 - Advisor recommendations
- Automation
 - CLI / PS
 - Tasks (preview)
 - Export template
- Help
 - Support + Troubleshooting

Step 3 - Assign the correct permissions to the managed identity. The identity only needs to read and list containers and blobs

Search for and select your storage account

Home > Storage accounts >

storagefordevs01 | Overview

Storage account

<> Upload Open in Explorer Delete Move Refresh Open in mobile CLI / PS Feedback

Overview

Resource group (move) : storagergproject
 Location : eastus
 Primary/Secondary Location : Primary: East US, Secondary: West US
 Subscription (move) : Pay-As-You-Go
 Subscription ID : 8148d5d5-df15-44ef-beb3-5960d3dc42eb
 Disk state : Primary: Available, Secondary: Available
 Tags (edit) : Add tags

Essentials

Performance : Standard
 Replication : Read-access geo-redundant storage (RA-GRS)
 Account kind : StorageV2 (general purpose v2)
 Provisioning state : Succeeded
 Created : 21/01/2024, 01:11:11

Properties Monitoring Capabilities (7) Recommendations (0) Tutorials Tools + SDKs

Blob service		Security	
Hierarchical namespace	Disabled	Require secure transfer for REST API operations	Enabled
Default access tier	Hot	Storage account key access	Enabled
Blob anonymous access	Disabled	Minimum TLS version	Version 1.2
Blob soft delete	Disabled	Infrastructure encryption	Disabled
Container soft delete	Disabled		
Versioning	Disabled		
Change feed	Disabled		
NFS v3	Disabled		
Allow cross-tenant replication	Disabled		

File service		Networking	
Large file share	Disabled	Allow access from	All networks
Identity-based access	Not configured	Number of private endpoint connections	0
Default share-level permissions	Disabled	Network routing	Microsoft network routing
Soft delete	Disabled	Access for trusted Microsoft services	Yes
Share capacity	5 TiB	Endpoint type	Standard

Queue service	

Data storage

- Containers
- File shares
- Queues
- Tables

Security + networking

- Networking
- Front Door and CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud

Data management

- Redundancy
- Data protection
- Object replication
- Blob inventory

Select the Access Control (IAM) blade

The screenshot shows the Azure Storage Account Access Control (IAM) blade for the storagefordevs01 account. The 'Check access' tab is active. The interface is divided into three main sections:

- Grant access to this resource:** Allows you to assign a role to grant access to resources. A 'Learn more' link and a 'Add role assignment' button are present.
- View access to this resource:** Shows the role assignments that grant access to this and other resources. A 'Learn more' link and a 'View' button are present.
- View deny assignments:** Shows the role assignments that have been denied access to specific actions at this scope. A 'Learn more' link and a 'View' button are present.

On the left side, there is a sidebar with the following navigation links:

- Overview
- Activity log
- Tags
- Diagnose and solve problems
- Access Control (IAM)** (selected)
- Data migration
- Events
- Storage browser
- Storage Mover
- Data storage**
- Containers
- File shares
- Queues
- Tables
- Security + networking**
- Networking
- Front Door and CDN
- Access keys
- Shared access signature
- Encryption
- Microsoft Defender for Cloud
- Data management**
- Redundancy
- Data protection
- Object replication
- Blob inventory

Select Add role assignment

On the Job functions roles page, search for and select the **Storage Blob Data Reader** role

Role name	Description	BuiltInRole	Permissions
Site Recovery Operator	Lets you failover and fallback but not perform other Site Recovery management operations	BuiltinRole	Management + Gover...
SqlMI Migration Role	Role for SqlMI migration	BuiltinRole	None
SqlVM Migration Role	Role for SqlVM migration	BuiltinRole	None
Storage Account Backup Contributor	Lets you perform backup and restore operations using Azure Backup on the storage account.	BuiltinRole	Storage
Storage Account Contributor	Lets you manage storage accounts, including accessing storage account keys which provide full access to...	BuiltinRole	Storage
Storage Account Encryption Scope Contr...	Allows management of Encryption Scopes on a Storage Account	BuiltinRole	None
Storage Account Key Operator Service R...	Storage Account Key Operators are allowed to list and regenerate keys on Storage Accounts	BuiltinRole	Storage
Storage Blob Data Contributor	Allows for read, write and delete access to Azure Storage blob containers and data	BuiltinRole	Storage
Storage Blob Data Owner	Allows for full access to Azure Storage blob containers and data, including assigning POSIX access control.	BuiltinRole	Storage
Storage Blob Data Reader	Allows for read access to Azure Storage blob containers and data	BuiltinRole	Storage
Storage Blob Delegator	Allows for generation of a user delegation key which can be used to sign SAS tokens	BuiltinRole	Storage
Storage File Data Privileged Contributor	Customer has read, write, delete and modify NTFS permission access on Azure Storage file shares.	BuiltinRole	None
Storage File Data Privileged Reader	Customer has read access on Azure Storage file shares.	BuiltinRole	None
Storage File Data SMB Share Contributor	Allows for read, write, and delete access in Azure Storage file shares over SMB	BuiltinRole	Storage
Storage File Data SMB Share Elevated Co...	Allows for read, write, delete and modify NTFS permission access in Azure Storage file shares over SMB	BuiltinRole	Storage
Storage File Data SMB Share Reader	Allows for read access to Azure File Share over SMB	BuiltinRole	Storage
Storage Queue Data Contributor	Allows for read, write, and delete access to Azure Storage queues and queue messages	BuiltinRole	Storage
Storage Queue Data Message Processor	Allows for peek, receive, and delete access to Azure Storage queue messages	BuiltinRole	Storage
Storage Queue Data Message Sender	Allows for sending of Azure Storage queue messages	BuiltinRole	Storage
Storage Queue Data Reader	Allows for read access to Azure Storage queues and queue messages	BuiltinRole	Storage
Storage Table Data Contributor	Allows for read, write and delete access to Azure Storage tables and entities	BuiltinRole	Storage
Storage Table Data Reader	Allows for read access to Azure Storage tables and entities	BuiltinRole	Storage
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtual network or storage account.	BuiltinRole	Compute

Showing 1 - 49 of 49 results.

Review + assign Previous Next Feedback

On the **Members** page, select **Managed identity**

Home > Storage accounts > storagefordevs01 | Access Control (IAM) >
Add role assignment ...

Role Members * Conditions (optional) Review + assign

Selected role Storage Blob Data Reader

Assign access to User, group, or service principal Managed identity

Members [+ Select members](#)

Name	Object ID	Type
No members selected		

Description

Review + assign Previous Next Feedback

Select **Select members**, in the **Managed identity** drop-down select **User-assigned managed identity**

Select the managed identity

Home > Storage accounts > storagefordevs01 | Access Control (IAM) >
Add role assignment ...

Role Members * Conditions (optional) Review + assign

Selected role Storage Blob Data Reader

Assign access to User, group, or service principal Managed identity

Members [+ Select members](#)

Name	Object ID	Type
No members selected		

Description

Select managed identities

⚠ Some results might be hidden due to your ABAC condition.

Subscription * Pay-As-You-Go

Managed identity User-assigned managed identity (1)

Select [\(1\)](#) Search by name

Selected members:
identityforstoragewebapp
/subscriptions/8148d5d5-df15-44ef-beb3-5960d3dc42eb/resourceGroups... [Remove](#)

Select Close Feedback

Click **Select** and then **Review + assign** the role

Home > Storage accounts > storagefordevs01 | Access Control (IAM) >
Add role assignment ...

Role Members Conditions (optional) Review + assign

Selected role Storage Blob Data Reader

Assign access to
 User, group, or service principal
 Managed identity

Members + Select members

Name	Object ID	Type
identityforstoragewebapp	e8387caa-e2fe-4c00-a73b-0f6cf2b16130	Managed Identity ⓘ

Description Optional

Review + assign Previous Next ⓘ Feedback

Select **Review + assign** a second time to add the role assignment

Home > Storage accounts > storagefordevs01 | Access Control (IAM) >
Add role assignment ...

Role Members Conditions (optional) **Review + assign**

Role Storage Blob Data Reader

Scope /subscriptions/8148d5d5-df15-44ef-beb3-5960d3dc42eb/resourceGroups/storagergproject/providers/Microsoft.Storage/storageAccounts/storagefordevs01

Members

Name	Object ID	Type
identityforstoragewebapp	e8387caa-e2fe-4c00-a73b-0f6cf2b16130	Managed Identity ⓘ

Description No description

Condition None

Review + assign Previous Next ⓘ Feedback

Storage account can now be accessed by a managed identity with the Storage Data Blob Reader permissions

The screenshot shows the 'storagefordevs01 | Access Control (IAM)' blade in the Azure portal. The left sidebar lists various management categories like Overview, Activity log, Tags, Diagnose and solve problems, and Data storage. The 'Access Control (IAM)' blade is selected. The main area displays the 'Role assignments' tab, which shows one assignment for a 'User-assigned Managed Identity' named 'identityforstoragewebapp'. This identity has been assigned the 'Storage Blob Data Reader' role. The assignment is scoped to 'This resource'. There are filters at the top for 'Type: All', 'Role: All', 'Scope: All scopes', and 'Group by: Role'.

Step 4 - Secure access to the storage account with a key vault and key

To create the key vault and key needed for this part your user account must have Key Vault Administrator permissions

In the portal, search for and select **Resource groups**

Select your **resource group**, and then the **Access Control (IAM)** blade.

Next Image

Select Add role assignment

On the **Job functions roles** page, search for and select the **Key Vault Administrator** role

Name ↑	Description ↑	Type ↑	Category ↑	Details
Classic Storage Account Key Operator Se...	Classic Storage Account Key Operators are allowed to list and regenerate keys on Classic Storage Accounts	BuiltinRole	Storage	View
Cognitive Services Contributor	Lets you create, read, update, delete and manage keys of Cognitive Services.	BuiltinRole	AI + Machine Learning	View
Cognitive Services User	Lets you read and list keys of Cognitive Services.	BuiltinRole	AI + Machine Learning	View
Cosmos DB Operator	Lets you manage Azure Cosmos DB accounts, but not access data in them. Prevents access to account ke...	BuiltinRole	Databases	View
Key Vault Administrator	Perform all data plane operations on a key vault and all objects in it, including certificates, keys, and secre...	BuiltinRole	Security	View
Key Vault Certificate User	Read certificate contents. Only works for key vaults that use the 'Azure role-based access control' permis...	BuiltinRole	None	View
Key Vault Certificates Officer	Perform any action on the certificates of a key vault, except manage permissions. Only works for key vault...	BuiltinRole	Security	View
Key Vault Contributor	Lets you manage key vaults, but not access to them.	BuiltinRole	Security	View
Key Vault Crypto Officer	Perform any action on the keys of a key vault, except manage permissions. Only works for key vaults that ...	BuiltinRole	Security	View
Key Vault Crypto Service Encryption User	Read metadata of keys and perform wrap/unwrap operations. Only works for key vaults that use the 'Azu...	BuiltinRole	Security	View
Key Vault Crypto Service Release User	Release keys. Only works for key vaults that use the 'Azure role-based access control' permission model.	BuiltinRole	None	View
Key Vault Crypto User	Perform cryptographic operations using keys. Only works for key vaults that use the 'Azure role-based ac...	BuiltinRole	Security	View
Key Vault Data Access Administrator	Manage access to Azure Key Vault by adding or removing role assignments for the Key Vault Administrat...	BuiltinRole	None	View
Key Vault Reader	Read metadata of key vaults and its certificates, keys, and secrets. Cannot read sensitive values such as se...	BuiltinRole	Security	View
Key Vault Secrets Officer	Perform any action on the secrets of a key vault, except manage permissions. Only works for key vaults th...	BuiltinRole	Security	View
Key Vault Secrets User	Read secret contents. Only works for key vaults that use the 'Azure role-based access control' permission ...	BuiltinRole	Security	View
Log Analytics Contributor	Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring s...	BuiltinRole	Analytics	View

On the **Members** page, select **User, group, or service principal**

Select **Select members**

Search for and select your user account. Your user account is shown in the top right of the portal

The screenshot shows the Azure portal interface for adding a role assignment. On the left, the 'Members' tab is selected under the 'Add role assignment' wizard. The 'Selected role' is set to 'Key Vault Administrator'. Under 'Assign access to', the 'User, group, or service principal' option is selected. The 'Members' section shows a table with columns 'Name', 'Object ID', and 'Type'. A note says 'No members selected'. Below the table is a 'Description' field labeled 'Optional'. At the bottom are buttons for 'Review + assign', 'Previous', 'Next', 'Select', and 'Close'.

On the right, a separate 'Select members' dialog is open. It has a search bar with placeholder 'Search by name or email address'. Below it is a list of users, with one user's name highlighted in red. The 'Selected members:' section at the bottom also has a user's name highlighted in red. The 'Select' and 'Close' buttons are at the bottom of this dialog.

Hid my azure account for security reasons.

This screenshot shows the 'Add role assignment' wizard again. The 'Members' tab is selected. The 'Selected role' is 'Key Vault Administrator'. The 'Assign access to' section shows 'User, group, or service principal' selected. In the 'Members' section, there is a table with one row: 'Vikar Ramtirat' (Object ID: 9a31cdff-f770-48b3-8a69-c6b94e994cfb, Type: User). The 'Description' field is empty. At the bottom are buttons for 'Review + assign', 'Previous', 'Next', and 'Feedback'.

Click **Select** and then **Review + assign**

Select **Review + assign** a second time to add the role assignment

Home > Resource groups > storagergproject | Access control (IAM) >

Add role assignment ... X

Role Members **Review + assign**

Role Key Vault Administrator

Scope /subscriptions/8148d5d5-df15-44ef-beb3-5960d3dc42eb/resourceGroups/storagergproject

Members	Name	Object ID	Type
	Vikar Ramtirat	9a31cddf-f770-48b3-8a69-c6b94e994cfb	User

Description No description

Review + assign Previous Next Feedback

Step 5 - Create a key vault to store the access keys

In the portal, search for and select **Key vaults**

Select **Create**

Home >

Key vaults X

Default Directory

+ Create Manage deleted vaults Manage view Refresh Export to CSV Open query | Assign tags

Filter for any field... Subscription equals all Resource group equals all Location equals all + Add filter

Show 0 to 0 of 0 records.

Name ↑↓	Type ↑↓	Resource group ↑↓	Location ↑↓	Subscription ↑↓	Tags
---------	---------	-------------------	-------------	-----------------	------

No grouping List view

 **No key vaults to display**

Safeguard cryptographic keys and other secrets used by cloud apps and services.

Create key vault Learn more

Home > Key vaults >

Create a key vault

X

Basics Access configuration Networking Tags Review + create

Azure Key Vault is a cloud service used to manage keys, secrets, and certificates. Key Vault eliminates the need for developers to store security information in their code. It allows you to centralize the storage of your application secrets which greatly reduces the chances that secrets may be leaked. Key Vault also allows you to securely store secrets and keys backed by Hardware Security Modules or HSMs. The HSMs used are Federal Information Processing Standards (FIPS) 140-2 Level 2 validated. In addition, key vault provides logs of all access and usage attempts of your secrets so you have a complete audit trail for compliance.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Pay-As-You-Go
Resource group * storagergproject
Create new

Instance details

Key vault name * webappstorekv
Region * East US
Pricing tier * Standard

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

Soft-delete Enabled
Days to retain deleted vaults * 90

Previous Next Review + create

Give feedback

Ensure on the Access configuration tab that Azure role-based access control (recommended) is selected

Home > Key vaults >

Create a key vault

X

Basics Access configuration Networking Tags Review + create

Configure data plane access for this key vault

To access a key vault in data plane, all callers (users or applications) must have proper authentication and authorization. Authentication establishes the identity of the caller. Authorization determines which operations the caller can execute. [Learn more](#)

Permission model

Grant data plane access by using a [Azure RBAC](#) or [Key Vault access policy](#)

- Azure role-based access control (recommended)
 Vault access policy

Resource access

- Azure Virtual Machines for deployment
 Azure Resource Manager for template deployment
 Azure Disk Encryption for volume encryption

Previous Next Review + create

Give feedback

Review and create

Wait for the validation checks to complete and then select **Create**

The screenshot shows the 'Create a key vault' wizard in the Azure portal. The current step is 'Review + create'. The configuration details are as follows:

Setting	Value
Subscription	Pay-As-You-Go
Resource group	storagergproject
Key vault name	webappstorekv
Region	East US
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	90 days

Access configuration

Setting	Value
Azure Virtual Machines for deployment	Disabled
Azure Resource Manager for template deployment	Disabled
Azure Disk Encryption for volume encryption	Disabled
Permission model	Azure role-based access control

Networking

Setting	Value
Connectivity method	Public endpoint (all networks)

At the bottom, there are 'Previous' and 'Next' buttons, a large blue 'Create' button, and a 'Give feedback' link.

After the deployment, select **Go to resource**

The screenshot shows the 'webappstorekv | Overview' page. The deployment status is 'Your deployment is complete'. Deployment details are listed:

Detail	Value
Deployment name	webappstorekv
Subscription	: Pay-As-You-Go
Resource group	: storagergproject

Deployment logs show a start time of 21/01/2024, 01:42:28 and a Correlation ID of 47210dd6-582b-4a9c-b8a9-37ea2e2a1... . There are sections for 'Deployment details' and 'Next steps', with a prominent blue 'Go to resource' button.

On the right side, there are several promotional cards:

- Cost management**: Get notified to stay within your budget and prevent unexpected charges on your bill. [Set up cost alerts >](#)
- Microsoft Defender for Cloud**: Secure your apps and infrastructure. [Go to Microsoft Defender for Cloud >](#)
- Free Microsoft tutorials**: Start learning today. [Start learning today >](#)
- Work with an expert**: Azure experts are service provider partners who can help manage your assets on Azure and be your first line of support. [Find an Azure expert >](#)

On the **Overview** blade ensure both **Soft-delete** and **Purge protection** are **enabled**

The screenshot shows the Azure Key Vault Overview blade for the key vault "webappstorekv". The left sidebar contains navigation links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Access policies, Events, Objects (Keys, Secrets, Certificates), Settings (Access configuration, Networking, Microsoft Defender for Cloud, Properties, Locks), Monitoring (Alerts, Metrics, Diagnostic settings, Logs, Insights, Workbooks), and Automation. The main content area displays the following details:

- Upcoming TLS 1.0, 1.1 deprecation:** Please enable support for TLS 1.2 or later on clients (applications/platform) to avoid any service impact.
- Essentials:**
 - Resource group: [storagegrproject](#)
 - Location: East US
 - Subscription: [Pay-As-You-Go](#)
 - Subscription ID: 8148d5d5-df15-44ef-beb3-5960d3dc42eb
 - Vault URI: <https://webappstorekv.vault.azure.net/>
 - Sku (Pricing tier): Standard
 - Directory ID: 3e838170-4582-4b4e-9281-cfb26fff07b
 - Directory Name: Default Directory
 - Soft-delete:** Enabled
 - Purge protection: Disabled
- Tags (edit):** Add tags
- Get started:** Properties, Monitoring, Tools + SDKs, Tutorials
- Manage keys and secrets used by apps and services:** A note about using a vault per application per environment (Development, Pre-Production and Production).
- Control access to key vault:** Assign access policy and determine whether a given service principal can perform different operations on key vault keys, secrets or certificate.
- Access configuration:** Options for Access policies and Access control (IAM).
- Enable logging and set up alerts:** Enable logging to monitor how, when and by whom your key vaults are accessed. Monitor performance and configure alerts for key vault metrics e.g., service API latency, error count.

Step 5 - Create a customer-managed key in the key vault

In your **key vault**, in the **Objects** section, select the **Keys** blade

The screenshot shows the 'Keys' blade in the Azure Key Vault 'Objects' section. On the left, there's a navigation menu with 'Keys' selected. The main area displays a table with columns 'Name', 'Status', and 'Expiration date'. A message at the top states: 'The connection to data plane failed. Please refresh and try again. If Private Links are enabled on the vault and the issue persists please follow the steps in the following link https://go.microsoft.com/fwlink/?linkid=2156688.' Below the table, it says 'There are no keys available.'

Select **Generate/Import** and **Name** the key

Take the defaults for the rest of the parameters, and **Create** the key

The screenshot shows the 'Create a key' dialog. It has several sections: 'Options' (dropdown set to 'Generate'), 'Name' (input field containing 'storekey01'), 'Key type' (radio button selected 'RSA'), 'RSA key size' (radio button selected '2048'), 'Set activation date' (checkbox unchecked), 'Set expiration date' (checkbox unchecked), 'Enabled' (radio button selected 'Yes'), 'Tags' (button showing '0 tags'), 'Set key rotation policy' (button showing 'Not configured'), 'Confidential Key Options' (checkboxes for 'Exportable' and 'Immutable' both unchecked), and 'Confidential operation policy' (dropdown menu open). At the bottom are 'Create' and 'Cancel' buttons.

Step 6 - Configure the storage account to use the customer managed key in the key vault

Before you can complete the next steps, you must assign the Key Vault Crypto Service Encryption User role to the managed identity

In the portal, search for and select **Resource groups**

Select your **resource group**, and then the **Access Control (IAM)** blade

<https://portal.azure.com/#/vickarrramitiratoutlook.onmicrosoft.com/resource/subscriptions/8148d5d5-df15-44ef-beb3-5960d3dc42eb/resourceGroups/storagergproject/users>

Select Add role assignment

The screenshot shows the 'Access control (IAM)' section of the Azure Resource Groups blade. On the left, there's a sidebar with various navigation options like Overview, Activity log, Tags, Resource visualizer, Events, Settings, Cost Management, Monitoring, and Workbooks. The main area has a search bar and a toolbar with 'Add', 'Download role assignments', 'Edit columns', 'Refresh', 'Remove', and 'Feedback'. A dropdown menu is open, showing 'Add role assignment' as the first option. Below the toolbar, there are sections for 'Check access' (with 'View my access' and 'Check access' buttons), 'Grant access to this resource' (with 'Add role assignments' button), 'View access to this resource' (with 'View' button), 'View deny assignments' (with 'View' button), and 'Create a custom role' (with 'Add' button). There's also a note about reviewing access levels.

On the **Job functions roles** page, search for and select the **Key Vault Crypto Service Encryption User** role

The screenshot shows the 'Add role assignment' page. At the top, there are tabs for 'Role' (which is selected), 'Members' (with a red asterisk indicating it's required), and 'Review + assign'. Below that, a note says 'A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles.' with a 'Learn more' link. The 'Assignment type' dropdown is set to 'Job function roles'. Under 'Job function roles', it says 'Privileged administrator roles' and 'Grant access to Azure resources based on job function, such as the ability to create virtual machines.' A search bar contains 'key vault service en', and filters for 'Type : All' and 'Category : All' are applied. The results table shows two entries:

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Key Vault Crypto Service Encryption User	Read metadata of keys and perform wrap/unwrap operations. Only works for key vaults that use the 'Azu...	BuiltinRole	Security	View
Key Vault Data Access Administrator	Manage access to Azure Key Vault by adding or removing role assignments for the Key Vault Administrat...	BuiltinRole	None	View

Below the table, it says 'Showing 1 - 2 of 2 results.' At the bottom, there are buttons for 'Review + assign', 'Previous', 'Next', and 'Feedback'.

On the **Members** page, select **Managed identity**

The screenshot shows the 'Add role assignment' interface. At the top, there are tabs for 'Role' and 'Members *'. The 'Members' tab is selected, indicated by a red asterisk. Below the tabs, the 'Selected role' is set to 'Key Vault Crypto Service Encryption User'. Under 'Assign access to', the 'Managed identity' option is selected. A 'Description' field is present with the placeholder 'Optional'. At the bottom, there are buttons for 'Review + assign', 'Previous', 'Next', and 'Feedback'.

Select **Select members**, in the **Managed identity** drop-down select **User-assigned managed identity**

The screenshot shows the 'Add role assignment' interface with the 'Members' tab selected. The 'Selected role' is 'Key Vault Crypto Service Encryption User' and 'Assign access to' is 'Managed identity'. The 'Description' field contains 'Optional'. On the right, a modal window titled 'Select managed identities' is open. It shows a warning message: 'Some results might be hidden due to your ABAC condition.' The 'Subscription' dropdown is set to 'Pay-As-You-Go'. Under 'Managed identity', it shows 'User-assigned managed identity (1)'. A 'Select' button is available, along with a search bar. Below the modal, the 'Selected members' section shows a yellow key icon and the path '/subscriptions/8148d5d5-df15-44ef-beb3-5960d3dc42eb/resourceGroups...'. At the bottom of the main interface, there are 'Review + assign', 'Previous', 'Next', 'Select', 'Close', and 'Feedback' buttons.

Select the managed identity

Home > Resource groups > storagergproject | Access control (IAM) >

Add role assignment

Role Members Review + assign

Selected role Key Vault Crypto Service Encryption User

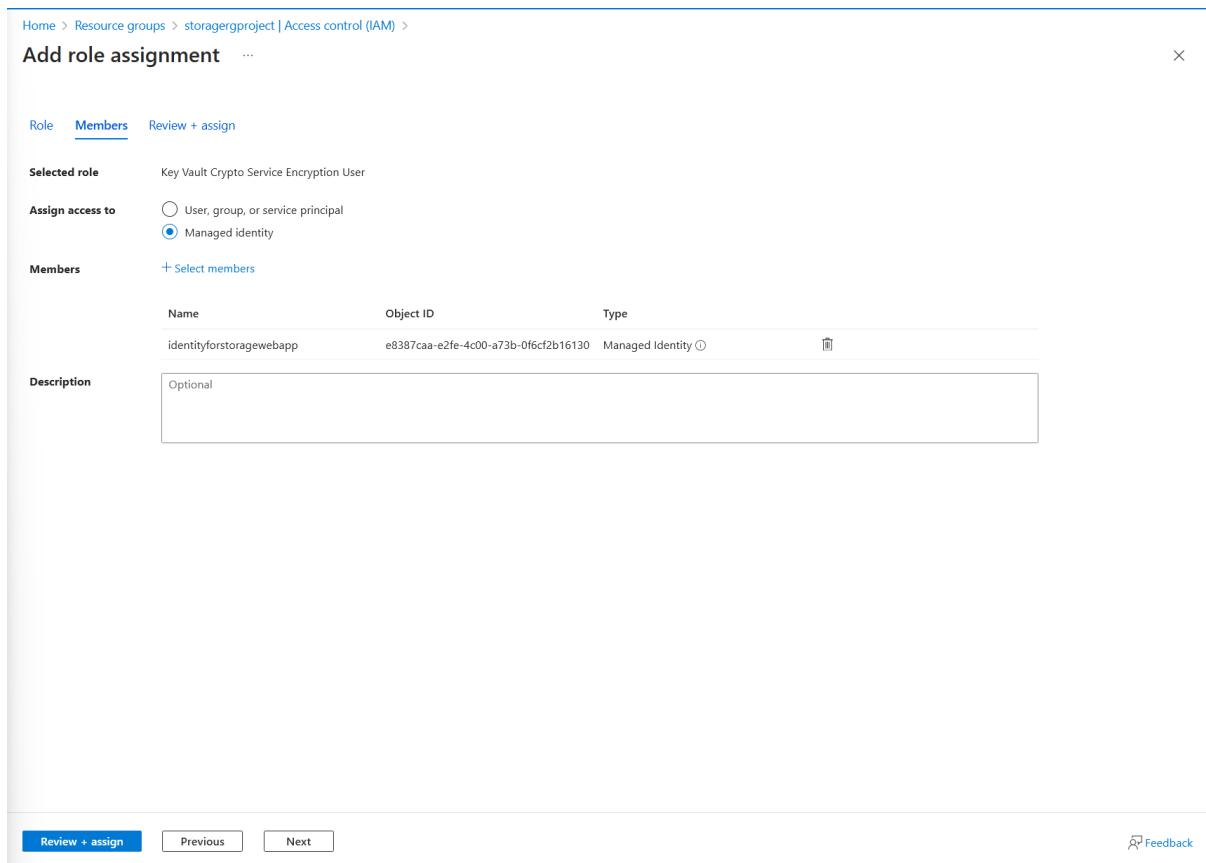
Assign access to
 User, group, or service principal
 Managed identity

Members + Select members

Name	Object ID	Type
identityforstoragewebapp	e8387caa-e2fe-4c00-a73b-0f6cf2b16130	Managed Identity ⓘ

Description Optional

Review + assign Previous Next ⓘ Feedback



Click **Select** and then **Review + assign**

Select **Review + assign** a second time to add the role assignment

Home > Resource groups > storagergproject | Access control (IAM) >

Add role assignment

Role Members Review + assign

Role Key Vault Crypto Service Encryption User

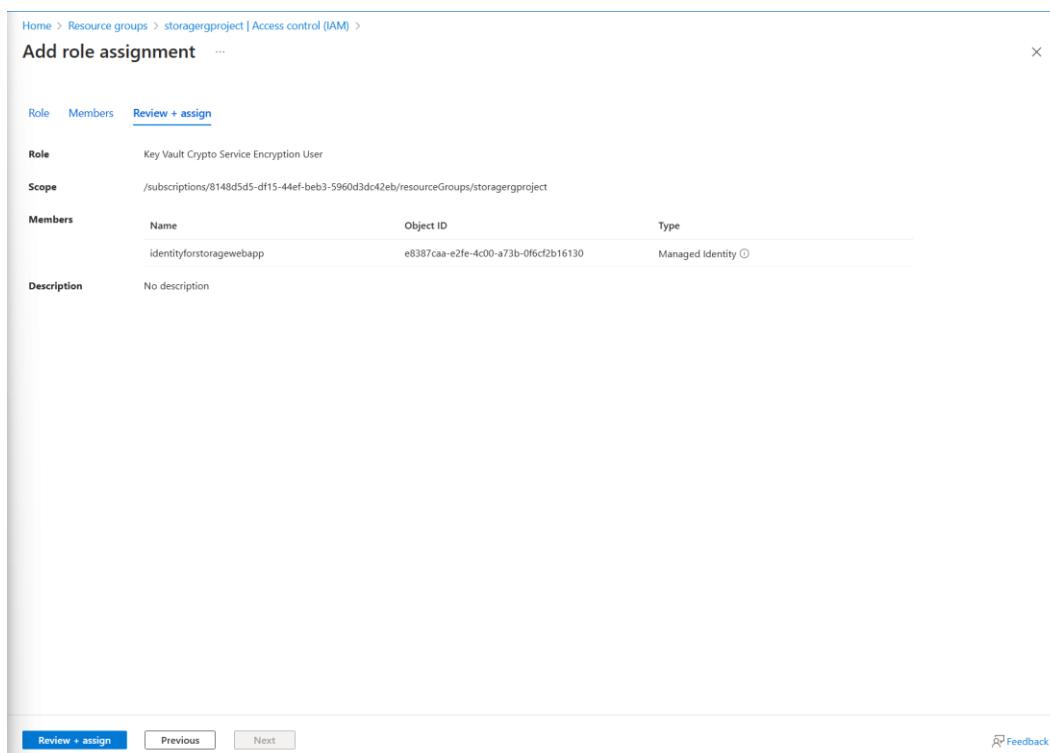
Scope /subscriptions/8148d5d5-df15-44ef-beb3-5960d3dc42eb/resourceGroups/storagergproject

Members

Name	Object ID	Type
identityforstoragewebapp	e8387caa-e2fe-4c00-a73b-0f6cf2b16130	Managed Identity ⓘ

Description No description

Review + assign Previous Next ⓘ Feedback



Step 7 - Configure the storage account to use the customer managed key in your key vault

[Return to the storage account](#)

The screenshot shows the Azure Storage account overview page for 'storagefordevs01'. The 'Encryption' blade is selected in the left navigation menu. The main content area displays various configuration settings under the 'Security + networking' section, including 'Blob service', 'File service', and 'Queue service'. Key settings shown include 'Require secure transfer for REST API operations' (Enabled), 'Storage account key access' (Enabled), and 'Endpoint type' (Standard). The 'Encryption' blade also includes sections for 'Encryption selection' (Enable support for customer-managed keys, Infrastructure encryption, Encryption type) and 'Encryption scopes'.

In the **Security + networking** section, select the **Encryption** blade

The screenshot shows the Azure Storage account overview page for 'storagefordevs01'. The 'Encryption' blade is selected in the left navigation menu. The main content area displays various configuration settings under the 'Security + networking' section, including 'Encryption selection' (Enable support for customer-managed keys, Infrastructure encryption, Encryption type) and 'Encryption scopes'. Key settings shown include 'Require secure transfer for REST API operations' (Enabled), 'Storage account key access' (Enabled), and 'Endpoint type' (Standard). The 'Encryption' blade also includes sections for 'Encryption selection' (Enable support for customer-managed keys, Infrastructure encryption, Encryption type) and 'Encryption scopes'.

Select Customer-managed keys

The screenshot shows the 'Encryption' blade for the storage account 'storagefordevs01'. On the left, there's a navigation menu with sections like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, and Storage Mover. Under Data storage, it lists Containers, File shares, Queues, and Tables. In Security + networking, it lists Networking, Front Door and CDN, Access keys, Shared access signature, and Encryption (which is selected). Under Data management, it lists Redundancy, Data protection, Object replication, and Blob inventory. The main content area is titled 'Encryption selection' and includes a note about enabling Storage Service Encryption. It shows 'Enable support for customer-managed keys' is set to 'Blobs and files only'. Under 'Infrastructure encryption', it says 'Disabled'. Under 'Encryption type', 'Customer-managed keys' is selected. A note states: 'When customer-managed keys are enabled, the storage account named 'storagefordevs01' is granted access to the selected key vault. Both soft delete and purge protection are also enabled on the key vault and cannot be disabled.' Below this, under 'Key selection', 'Encryption key' is selected, and 'Select from key vault' is chosen. Under 'Identity type', 'System-assigned' is selected. At the bottom, there are 'Save' and 'Discard' buttons, and a 'Give feedback' link.

Select a key vault and key. Select your key vault and key

This is a modal dialog box titled 'Select a key'. It has fields for 'Subscription' (set to 'Pay-As-You-Go'), 'Key store type' (set to 'Key vault'), and 'Key vault' (set to 'webappstorekv'). Under 'Key', it shows 'storekey01' with a 'Create new key' link. At the bottom, there are 'Select' and 'Cancel' buttons.

Select to confirm your choices

Ensure the Identity type is User-assigned

The screenshot shows the 'Encryption' blade for the storage account 'storagefordevs01'. In the 'Identity type' section, the 'User-assigned' option is selected, highlighted with a yellow box. The 'Select an identity' dropdown is open, showing a single result: 'identityforstoragewebapp' from the 'Resource Group: storagergproject' under 'Subscription: Pay-As-You-Go'. Other options like 'System-assigned' and 'Select from key vault' are also visible.

Select an identity

Select your managed identity then select Add

The screenshot shows the same 'Encryption' blade for 'storagefordevs01'. The 'User-assigned' identity type is selected. To the right, a modal dialog titled 'Select user assigned managed...' is open. It shows a list of managed identities under 'User assigned managed identities'. One item, 'identityforstoragewebapp', is selected and highlighted with a yellow box. The 'Selected identity:' section shows the details: 'identityforstoragewebapp', 'Resource Group: storagergproject', and 'Subscription: Pay-As-You-Go'. A 'Remove' button is also present in this section. At the bottom of the modal is a blue 'Add' button.

Click Save to save settings

If an error occurs purge protection on key vault needs to be turned on key vault.

The screenshot shows the 'Encryption' settings page for the storage account 'storagefordevs01'. The left sidebar lists various account management sections like Overview, Activity log, Tags, etc. The 'Encryption' section is currently selected and highlighted with a grey background. The main content area displays the encryption configuration. It includes sections for 'Encryption selection', 'Key selection', and 'Identity type'. Under 'Encryption selection', 'Enable support for customer-managed keys' is set to 'Blobs and files only'. Under 'Key selection', the 'Current key' is set to a specific URL, and 'Automated key rotation' is enabled. Under 'Identity type', it is set to 'User-assigned', with a corresponding object ID listed. At the bottom, there are 'Save' and 'Discard' buttons, and a 'Give feedback' link.

Step 8 - Configure a time-based retention policy and an encryption scope

The developers require a storage container where files can't be modified, even by the administrator

Navigate to your **storage account**

The screenshot shows the Azure Storage account overview for 'storagefordevs01'. The left sidebar includes sections for Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Data storage (Containers, File shares, Queues, Tables), Security + networking (Networking, Front Door and CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud), and Data management (Redundancy, Data protection, Object replication, Blob inventory). The main content area displays the 'Essentials' blade, which provides details about the resource group, location, primary/secondary location, subscription, disk state, and tags. It also lists properties for Blob service, File service, and Queue service, including security settings like require secure transfer for REST API operations and storage account key access. A success message at the top right indicates 'Successfully created storage container'.

In the **Data storage** section, select the **Containers** blade

Create a container called **hold**. Take the defaults. Be sure to **Create** the container

The screenshot shows the 'Containers' blade within the 'storagefordevs01' storage account. The left sidebar is identical to the previous screenshot. The main content area displays a table of existing containers: '\$logs' and 'hold'. A success message at the top right says 'Successfully created storage container' and 'Successfully created storage container 'hold''. A note below it states 'Container 'hold' has been successfully created.' A 'Create container' button is visible at the bottom of the blade.

Upload a file to the container

The screenshot shows the Azure Storage Explorer interface for a container named 'hold'. In the top right corner, a success message box displays: 'Successfully uploaded blob(s)' and 'Successfully uploaded 1 blob(s.)'. The main pane shows a table of blobs with one entry: 'UserCreateTemplate.csv' (blob type: Block blob, size: 574 B, lease state: Available). The left sidebar has sections for Overview, Diagnose and solve problems, Access Control (IAM), Settings (Shared access tokens, Access policy, Properties, Metadata), and a search bar.

In the **Settings** section, select the **Access policy** blade

In the **Immutable blob storage** section, select **+ Add policy**

The screenshot shows the 'Access policy' blade for the 'hold' container. On the left, under 'Settings', 'Access policy' is selected. On the right, the 'Immutable Storage policy' blade is open. It shows a 'Policy type' dropdown set to 'Legal hold'. A note indicates that each legal hold policy needs to be associated with 1 or more tags. Below this, there's a 'Tag' input field with 'Add tag' and a 'Save' button at the bottom.

For the **Policy type**, select **time-based retention** & Set the **Retention period** to **5 days**

See image next

The screenshot shows the Azure Storage Explorer interface. On the left, the navigation pane includes 'Overview', 'Diagnose and solve problems', 'Access Control (IAM)', 'Properties', and 'Metadata'. The 'Access policy' section is selected. On the right, there's a list of 'Stored access policies' with a 'No results' message. A modal window titled 'Immutable Storage policy' is displayed, containing the following fields:

- Policy type:** Time-based retention
- Set retention period for ***: 5 days
- Enable version-level immutability**: Unchecked
- In order to enable version-level immutability support, your storage account must have versioning turned on.**
- Allow protected append writes to**:
 - None**: Selected (radio button)
 - Append blobs
 - Block and append blobs

At the bottom of the modal are 'Save' and 'Cancel' buttons.

Click on save

The screenshot shows the Azure Storage Explorer interface after saving the policy. The 'Access policy' section in the navigation pane is still selected. On the right, the 'Stored access policies' table is populated with one row:

Identifier	Start time	Expiry time	Permissions
Immutable blob storage	+ Add policy		

The table details the policy:

- Identifier:** Immutable blob storage
- Scope:** Container
- Retention interval:** 5 days
- State:** Unlocked

To test Try to delete the file in the container

The screenshot shows the Azure Storage Explorer interface. On the left, a sidebar lists options like Overview, Diagnosis and solve problems, Access Control (IAM), Properties, and Metadata. The main area shows a table with columns Name, Modified, Access tier, and Archive stat. One row is selected, showing 'UserCreateTemplate.csv' was modified on 21/01/2024, 02:13:50 with a Hot (Inferred) access tier. To the right, a 'Notifications' sidebar displays several log entries:

- Failed to delete blobs**: Failed to delete 1 out of 1 blobs: UserCreateTemplate.csv. This operation is not permitted as the blob is immutable due to a policy. RequestId:db1acb085-001e-0063-2210-4c797f000000 Time:2024-01-21T02:17:53.1845044Z (a few seconds ago)
- Successfully updated retention policy**: Successfully updated retention policy for container 'hold'. (2 minutes ago)
- Successfully uploaded blob(s)**: Successfully uploaded 1 blob(s). (5 minutes ago)
- Successfully created storage container**: Successfully created storage container 'hold'. (6 minutes ago)

Verify you are notified **failed to delete blobs** due to policy

Step 9 - The developers require an encryption scope that enables infrastructure encryption
Navigate back to the storage account **storagefordevs01**

The screenshot shows the Azure Storage account settings page for 'storagefordevs01'. The left sidebar lists categories such as Overview, Activity log, Tags, Diagnosis and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Data storage (Containers, File shares, Queues, Tables), Security + networking (Networking, Front Door and CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud), Data management (Redundancy, Data protection, Object replication, Blob inventory), and a JSON View button.

The main content area displays the following service configurations:

- Blob service**: Hierarchical namespace: Disabled; Default access tier: Hot; Blob anonymous access: Disabled; Blob soft delete: Disabled; Container soft delete: Disabled; Versioning: Disabled; Change feed: Disabled; NFS v3: Disabled; Allow cross-tenant replication: Disabled.
- File service**: Large file share: Disabled; Identity-based access: Not configured; Default share-level permissions: Disabled; Soft delete: Disabled; Share capacity: 5 TiB.
- Queue service**: (No specific configuration shown)
- Security**: Require secure transfer for REST API operations: Enabled; Storage account key access: Enabled; Minimum TLS version: Version 1.2; Infrastructure encryption: Disabled.
- Networking**: Allow access from: All networks; Number of private endpoint connections: 0; Network routing: Microsoft network routing; Access for trusted Microsoft services: Yes; Endpoint type: Standard.

In the **Security + networking** blade, select **Encryption**

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

In the **Encryption scopes** tab, select **Add**

Give your encryption scope a **name**

The **Encryption type** is **Microsoft-managed key**

Set **Infrastructure encryption** to **Enable**

Notice the warning that enabling infrastructure encryption can not be changed after the scope is created

Create the encryption scope

Encryption scope name *

Encryption type Microsoft-managed keys Customer-managed keys

Infrastructure encryption Enabled Disabled

⚠️ This option cannot be changed after this encryption scope is created.

Create

Encryption Scope created

The screenshot shows the 'Encryption scopes' blade for the storage account 'storagefordevs01'. On the left, there's a navigation menu with sections like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Data storage (Containers, File shares, Queues, Tables), Security + networking (Networking, Front Door and CDN, Access keys, Shared access signature, Encryption, Microsoft Defender for Cloud), and Data management (Redundancy, Data protection, Object replication, Blob inventory). The 'Encryption' section is currently selected. The main area shows a table with one row for the 'devscope'. The columns are Name, Status, Encryption type, Key, and Automated key rotation. The 'devscope' is listed with Status 'Enabled', Encryption type 'Microsoft-managed keys', and Key '-'. There's also a toggle switch for 'Only show enabled scopes'.

Return to your storage account and create a new container

Notice on the **New container** page, there is the **Name** and **Public access level**

Notice in the **Advanced** section you can select the **Encryption scope** you created and apply it to all blobs in the container

The screenshot shows the 'Containers' blade for the storage account 'storagefordevs01'. The left sidebar has the same navigation as the previous screenshot. The main area lists two containers: '\$logs' and 'hold'. On the right, a 'New container' dialog is open. It has fields for 'Name' (set to 'devops') and 'Anonymous access level' (set to 'Private (no anonymous access)'). Below these, a note says 'The access level is set to private because anonymous access is disabled on this storage account.' Under the 'Advanced' section, there's a dropdown for 'Encryption scope' (set to 'devscope') and a checked checkbox for 'Use this encryption scope for all blobs in the container'. There are also options for 'Enable version-level immutability support' (unchecked) and a note about enabling it. At the bottom of the dialog are 'Create' and 'Give feedback' buttons.