VERZEO MINOR PROJECT

• Project Name:

Azure Cloud Computing June Minor Project

• Project Description:

TASK 2:

Create an azure storage account using the azure portal and create a BLOB storage(Hot

tier) inside a container.

Upload one image as well as a short video and set different access permissions

(private and public). ENABLE ACCESS TRACKING and add a rule in the lifecycle

management policies telling that

i. if the page blob which we created is not accessed for 10 days then change its

access tier to cool.

ii. If the blob is not modified for 45 days, delete the blob.

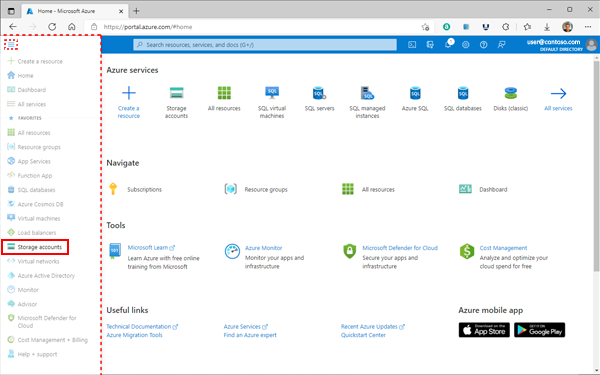
**Create a storage account**

A storage account is an Azure Resource Manager resource. Resource Manager is the deployment and management service for Azure.

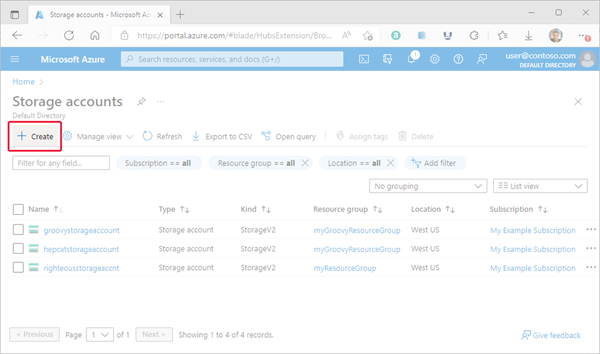
Every Resource Manager resource, including an Azure storage account, must belong to an Azure resource group. A resource group is a logical container for grouping your Azure services. When you create a storage account, you have the option to either create a new resource group, or use an existing resource group. This how-to shows how to create a new resource group.

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

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

[](https://learn.microsoft.com/en-us/azure/storage/common/media/storage-account-create/menu-expand-lrg.png#lightbox)

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

[](https://learn.microsoft.com/en-us/azure/storage/common/media/storage-account-create/create-button-lrg.png#lightbox)

Options for your new storage account are organized into tabs in the **Create a storage account** page. The following sections describe each of the tabs and their options.

**Basics tab**

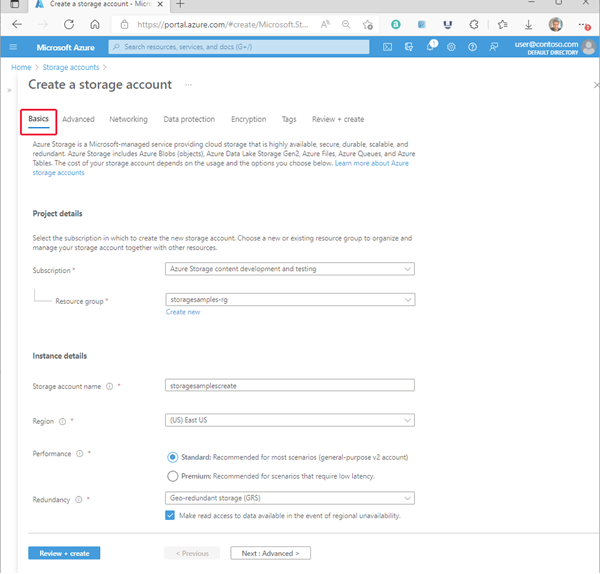
On the **Basics** tab, provide the essential information for your storage account. After you complete the **Basics** tab, you can choose to further customize your new storage account by setting options on the other tabs, or you can select **Review + create** to accept the default options and proceed to validate and create the account.

The following table describes the fields on the **Basics** tab.

Expand table

| **Section** | **Field** | **Required or optional** | **Description** |
| --- | --- | --- | --- |
| Project details | Subscription | Required | Select the subscription for the new storage account. |
| Project details | Resource group | Required | Create a new resource group for this storage account, or select an existing one. For more information, see [Resource groups](https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview#resource-groups). |
| Instance details | Storage account name | Required | Choose a unique name for your storage account. Storage account names must be between 3 and 24 characters in length and might contain numbers and lowercase letters only. |
| Instance details | Region | Required | Select the appropriate region for your storage account. For more information, see [Regions and Availability Zones in Azure](https://learn.microsoft.com/en-us/azure/availability-zones/az-overview).  Not all regions are supported for all types of storage accounts or redundancy configurations. For more information, see [Azure Storage redundancy](https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy).  The choice of region can have a billing impact. For more information, see [Storage account billing](https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview#storage-account-billing).  If your subscription supports Azure public multi-access edge zones (Azure MEC), you can deploy your storage account to an edge zone. For more information about edge zones, see [What is Azure public MEC?](https://learn.microsoft.com/en-us/azure/public-multi-access-edge-compute-mec/overview). |
| Instance details | Performance | Required | Select **Standard** performance for general-purpose v2 storage accounts (default). This type of account is recommended by Microsoft for most scenarios. For more information, see [Types of storage accounts](https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview#types-of-storage-accounts).  Select **Premium** for scenarios requiring low latency. After selecting **Premium**, select the type of premium storage account to create. The following types of premium storage accounts are available:   * [Block blobs](https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview) * [File shares](https://learn.microsoft.com/en-us/azure/storage/files/storage-files-planning#management-concepts) * [Page blobs](https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blob-pageblob-overview) |
| Instance details | Redundancy | Required | Select your desired redundancy configuration. Not all redundancy options are available for all types of storage accounts in all regions. For more information about redundancy configurations, see [Azure Storage redundancy](https://learn.microsoft.com/en-us/azure/storage/common/storage-redundancy).  If you select a geo-redundant configuration (GRS or GZRS), your data is replicated to a data center in a different region. For read access to data in the secondary region, select **Make read access to data available in the event of regional unavailability**. |

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

[](https://learn.microsoft.com/en-us/azure/storage/common/media/storage-account-create/create-account-basics-tab-lrg.png#lightbox)

**Advanced tab**

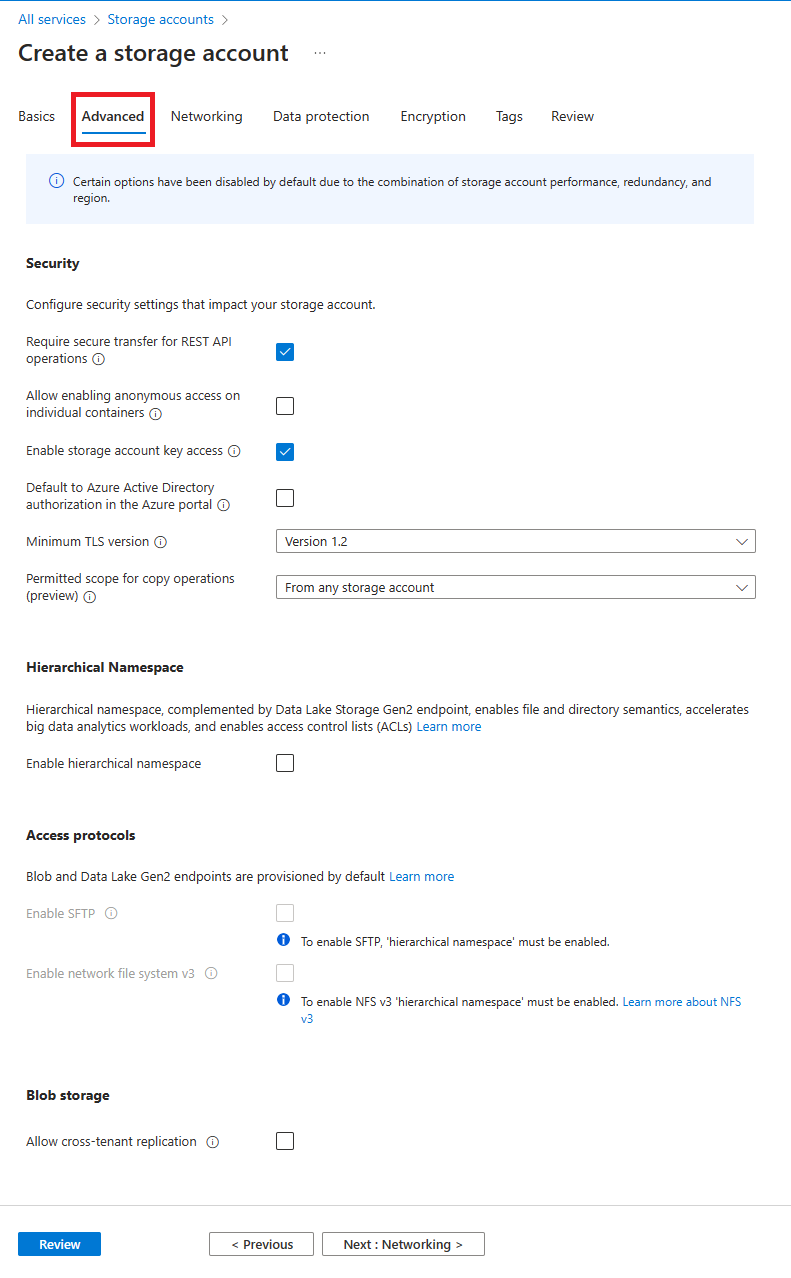
On the **Advanced** tab, you can configure additional options and modify default settings for your new storage account. Some of these options can also be configured after the storage account is created, while others must be configured at the time of creation.

The following table describes the fields on the **Advanced** tab.

Expand table

| **Section** | **Field** | **Required or optional** | **Description** |
| --- | --- | --- | --- |
| Security | Require secure transfer for REST API operations | Optional | Require secure transfer to ensure that incoming requests to this storage account are made only via HTTPS (default). Recommended for optimal security. For more information, see [Require secure transfer to ensure secure connections](https://learn.microsoft.com/en-us/azure/storage/common/storage-require-secure-transfer). |
| Security | Allow enabling anonymous access on individual containers | Optional | When enabled, this setting allows a user with the appropriate permissions to enable anonymous access to a container in the storage account (default). Disabling this setting prevents all anonymous access to the storage account. Microsoft recommends disabling this setting for optimal security.  For more information, see [Prevent anonymous read access to containers and blobs](https://learn.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent).  Enabling anonymous access does not make blob data available for anonymous access unless the user takes the additional step to explicitly configure the container's anonymous access setting. |
| Security | Enable storage account key access | Optional | When enabled, this setting allows clients to authorize requests to the storage account using either the account access keys or a Microsoft Entra account (default). Disabling this setting prevents authorization with the account access keys. For more information, see [Prevent Shared Key authorization for an Azure Storage account](https://learn.microsoft.com/en-us/azure/storage/common/shared-key-authorization-prevent). |
| Security | Default to Microsoft Entra authorization in the Azure portal | Optional | When enabled, the Azure portal authorizes data operations with the user's Microsoft Entra credentials by default. If the user does not have the appropriate permissions assigned via Azure role-based access control (Azure RBAC) to perform data operations, then the portal will use the account access keys for data access instead. The user can also choose to switch to using the account access keys. For more information, see [Default to Microsoft Entra authorization in the Azure portal](https://learn.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal#default-to-azure-ad-authorization-in-the-azure-portal). |
| Security | Minimum TLS version | Required | Select the minimum version of Transport Layer Security (TLS) for incoming requests to the storage account. The default value is TLS version 1.2. When set to the default value, incoming requests made using TLS 1.0 or TLS 1.1 are rejected. For more information, see [Enforce a minimum required version of Transport Layer Security (TLS) for requests to a storage account](https://learn.microsoft.com/en-us/azure/storage/common/transport-layer-security-configure-minimum-version). |
| Security | Permitted scope for copy operations (preview) | Required | Select the scope of storage accounts from which data can be copied to the new account. The default value is From any storage account. When set to the default value, users with the appropriate permissions can copy data from any storage account to the new account.  Select From storage accounts in the same Azure AD tenant to only allow copy operations from storage accounts within the same Microsoft Entra tenant. Select From storage accounts that have a private endpoint to the same virtual network to only allow copy operations from storage accounts with private endpoints on the same virtual network.  For more information, see [Restrict the source of copy operations to a storage account](https://learn.microsoft.com/en-us/azure/storage/common/security-restrict-copy-operations). |
| Data Lake Storage Gen2 | Enable hierarchical namespace | Optional | To use this storage account for Azure Data Lake Storage Gen2 workloads, configure a hierarchical namespace. For more information, see [Introduction to Azure Data Lake Storage Gen2](https://learn.microsoft.com/en-us/azure/storage/blobs/data-lake-storage-introduction). |
| Blob storage | Enable SFTP | Optional | Enable the use of Secure File Transfer Protocol (SFTP) to securely transfer of data over the internet. For more information, see [Secure File Transfer (SFTP) protocol support in Azure Blob Storage](https://learn.microsoft.com/en-us/azure/storage/blobs/secure-file-transfer-protocol-support). |
| Blob storage | Enable network file system (NFS) v3 | Optional | NFS v3 provides Linux file system compatibility at object storage scale enables Linux clients to mount a container in Blob storage from an Azure Virtual Machine (VM) or a computer on-premises. For more information, see [Network File System (NFS) 3.0 protocol support in Azure Blob Storage](https://learn.microsoft.com/en-us/azure/storage/blobs/network-file-system-protocol-support). |
| Blob storage | Allow cross-tenant replication | Required | By default, users with appropriate permissions can configure object replication across Microsoft Entra tenants. To prevent replication across tenants, deselect this option. For more information, see [Prevent replication across Microsoft Entra tenants](https://learn.microsoft.com/en-us/azure/storage/blobs/object-replication-overview#prevent-replication-across-azure-ad-tenants). |
| Blob storage | Access tier | Required | Blob access tiers enable you to store blob data in the most cost-effective manner, based on usage. Select the hot tier (default) for frequently accessed data. Select the cool tier for infrequently accessed data. For more information, see [Hot, Cool, and Archive access tiers for blob data](https://learn.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview). |
| Azure Files | Enable large file shares | Optional | Available only for standard file shares with the LRS or ZRS redundancies. |

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

[](https://learn.microsoft.com/en-us/azure/storage/common/media/storage-account-create/create-account-advanced-tab.png#lightbox)

**Networking tab**

On the **Networking** tab, you can configure network connectivity and routing preference settings for your new storage account. These options can also be configured after the storage account is created.

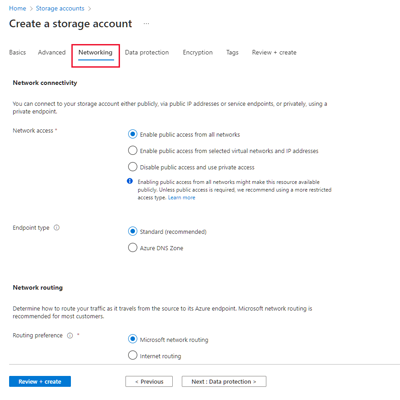
The following table describes the fields on the **Networking** tab.

Expand table

| **Section** | **Field** | **Required or optional** | **Description** |
| --- | --- | --- | --- |
| Network connectivity | Network access | Required | By default, incoming network traffic is routed to the public endpoint for your storage account. You can specify that traffic must be routed to the public endpoint through an Azure virtual network. You can also configure private endpoints for your storage account. For more information, see [Use private endpoints for Azure Storage](https://learn.microsoft.com/en-us/azure/storage/common/storage-private-endpoints). |
| Network connectivity | Endpoint type | Required | Azure Storage supports two types of endpoints: [standard endpoints](https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview#standard-endpoints) (the default) and [Azure DNS zone endpoints](https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview#azure-dns-zone-endpoints-preview) (preview). Within a given subscription, you can create up to 2501 accounts with standard endpoints per region, and up to 5000 accounts with Azure DNS zone endpoints per region, for a total of 5250 storage accounts. To register for the preview, see [About the preview](https://learn.microsoft.com/en-us/azure/storage/common/storage-account-overview#about-the-preview). |
| Network routing | Routing preference | Required | The network routing preference specifies how network traffic is routed to the public endpoint of your storage account from clients over the internet. By default, a new storage account uses Microsoft network routing. You can also choose to route network traffic through the POP closest to the storage account, which might lower networking costs. For more information, see [Network routing preference for Azure Storage](https://learn.microsoft.com/en-us/azure/storage/common/network-routing-preference). |

1With a quota increase, you can create up to 500 storage accounts with standard endpoints per region in a given subscription, for a total of 5500 storage accounts per region. For more information, see [Increase Azure Storage account quotas](https://learn.microsoft.com/en-us/azure/quotas/storage-account-quota-requests).

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

[](https://learn.microsoft.com/en-us/azure/storage/common/media/storage-account-create/create-account-networking-tab-lrg.png#lightbox)

**Data protection tab**

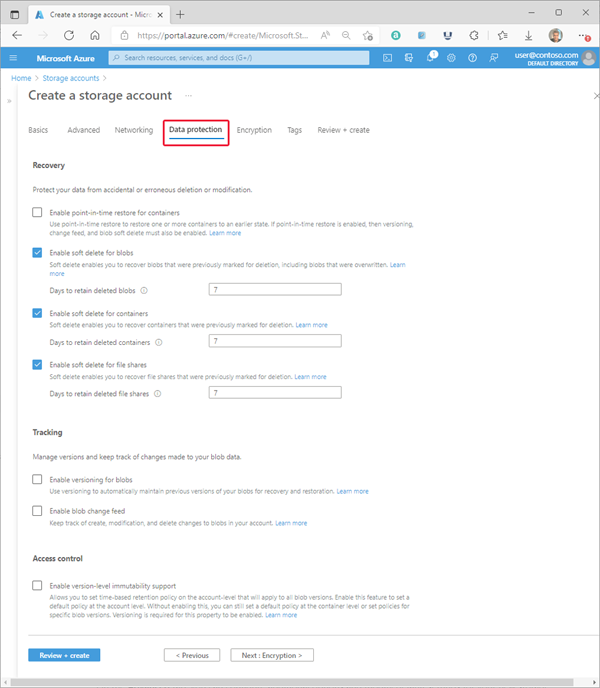
On the **Data protection** tab, you can configure data protection options for blob data in your new storage account. These options can also be configured after the storage account is created. For an overview of data protection options in Azure Storage, see [Data protection overview](https://learn.microsoft.com/en-us/azure/storage/blobs/data-protection-overview).

The following table describes the fields on the **Data protection** tab.

Expand table

| **Section** | **Field** | **Required or optional** | **Description** |
| --- | --- | --- | --- |
| Recovery | Enable point-in-time restore for containers | Optional | Point-in-time restore provides protection against accidental deletion or corruption by enabling you to restore block blob data to an earlier state. For more information, see [Point-in-time restore for block blobs](https://learn.microsoft.com/en-us/azure/storage/blobs/point-in-time-restore-overview).  Enabling point-in-time restore also enables blob versioning, blob soft delete, and blob change feed. These prerequisite features might have a cost impact. For more information, see [Pricing and billing](https://learn.microsoft.com/en-us/azure/storage/blobs/point-in-time-restore-overview#pricing-and-billing) for point-in-time restore. |
| Recovery | Enable soft delete for blobs | Optional | Blob soft delete protects an individual blob, snapshot, or version from accidental deletes or overwrites by maintaining the deleted data in the system for a specified retention period. During the retention period, you can restore a soft-deleted object to its state at the time it was deleted. For more information, see [Soft delete for blobs](https://learn.microsoft.com/en-us/azure/storage/blobs/soft-delete-blob-overview).  Microsoft recommends enabling blob soft delete for your storage accounts and setting a minimum retention period of seven days. |
| Recovery | Enable soft delete for containers | Optional | Container soft delete protects a container and its contents from accidental deletes by maintaining the deleted data in the system for a specified retention period. During the retention period, you can restore a soft-deleted container to its state at the time it was deleted. For more information, see [Soft delete for containers](https://learn.microsoft.com/en-us/azure/storage/blobs/soft-delete-container-overview).  Microsoft recommends enabling container soft delete for your storage accounts and setting a minimum retention period of seven days. |
| Recovery | Enable soft delete for file shares | Optional | Soft delete for file shares protects a file share and its contents from accidental deletes by maintaining the deleted data in the system for a specified retention period. During the retention period, you can restore a soft-deleted file share to its state at the time it was deleted. For more information, see [Prevent accidental deletion of Azure file shares](https://learn.microsoft.com/en-us/azure/storage/files/storage-files-prevent-file-share-deletion).  Microsoft recommends enabling soft delete for file shares for Azure Files workloads and setting a minimum retention period of seven days. |
| Tracking | Enable versioning for blobs | Optional | Blob versioning automatically saves the state of a blob in a previous version when the blob is overwritten. For more information, see [Blob versioning](https://learn.microsoft.com/en-us/azure/storage/blobs/versioning-overview).  Microsoft recommends enabling blob versioning for optimal data protection for the storage account. |
| Tracking | Enable blob change feed | Optional | The blob change feed provides transaction logs of all changes to all blobs in your storage account, as well as to their metadata. For more information, see [Change feed support in Azure Blob Storage](https://learn.microsoft.com/en-us/azure/storage/blobs/storage-blob-change-feed). |
| Access control | Enable version-level immutability support | Optional | Enable support for immutability policies that are scoped to the blob version. If this option is selected, then after you create the storage account, you can configure a default time-based retention policy for the account or for the container, which blob versions within the account or container will inherit by default. For more information, see [Enable version-level immutability support on a storage account](https://learn.microsoft.com/en-us/azure/storage/blobs/immutable-policy-configure-version-scope#enable-version-level-immutability-support-on-a-storage-account). |

The following image shows a standard configuration of the data protection properties for a new storage account.

[](https://learn.microsoft.com/en-us/azure/storage/common/media/storage-account-create/create-account-protection-tab-lrg.png#lightbox)

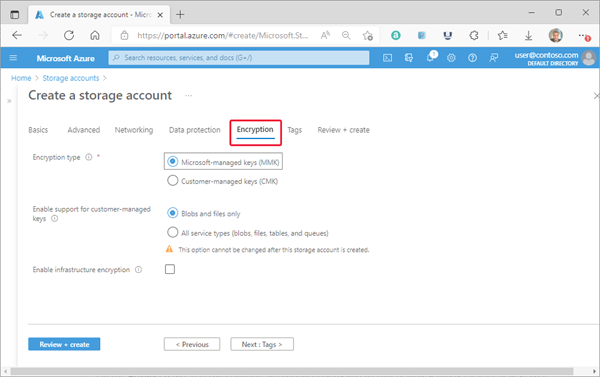
**Encryption tab**

On the **Encryption** tab, you can configure options that relate to how your data is encrypted when it is persisted to the cloud. Some of these options can be configured only when you create the storage account.

Expand table

| **Field** | **Required or optional** | **Description** |
| --- | --- | --- |
| Encryption type | Required | By default, data in the storage account is encrypted by using Microsoft-managed keys. You can rely on Microsoft-managed keys for the encryption of your data, or you can manage encryption with your own keys. For more information, see [Azure Storage encryption for data at rest](https://learn.microsoft.com/en-us/azure/storage/common/storage-service-encryption). |
| Enable support for customer-managed keys | Required | By default, customer managed keys can be used to encrypt only blobs and files. Set this option to **All service types (blobs, files, tables, and queues)** to enable support for customer-managed keys for all services. You are not required to use customer-managed keys if you choose this option. For more information, see [Customer-managed keys for Azure Storage encryption](https://learn.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview). |
| Encryption key | Required if **Encryption type** field is set to **Customer-managed keys**. | If you choose **Select a key vault and key**, you are presented with the option to navigate to the key vault and key that you wish to use. If you choose **Enter key from URI**, then you are presented with a field to enter the key URI and the subscription. |
| User-assigned identity | Required if **Encryption type** field is set to **Customer-managed keys**. | If you are configuring customer-managed keys at create time for the storage account, you must provide a user-assigned identity to use for authorizing access to the key vault. |
| Enable infrastructure encryption | Optional | By default, infrastructure encryption is not enabled. Enable infrastructure encryption to encrypt your data at both the service level and the infrastructure level. For more information, see [Create a storage account with infrastructure encryption enabled for double encryption of data](https://learn.microsoft.com/en-us/azure/storage/common/infrastructure-encryption-enable). |

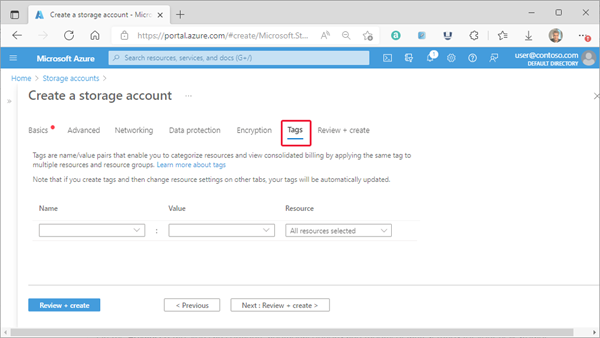
The following image shows a standard configuration of the encryption properties for a new storage account.

[](https://learn.microsoft.com/en-us/azure/storage/common/media/storage-account-create/create-account-encryption-tab-lrg.png#lightbox)

**Tags tab**

On the **Tags** tab, you can specify Resource Manager tags to help organize your Azure resources. For more information, see [Tag resources, resource groups, and subscriptions for logical organization](https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/tag-resources).

The following image shows a standard configuration of the index tag properties for a new storage account.

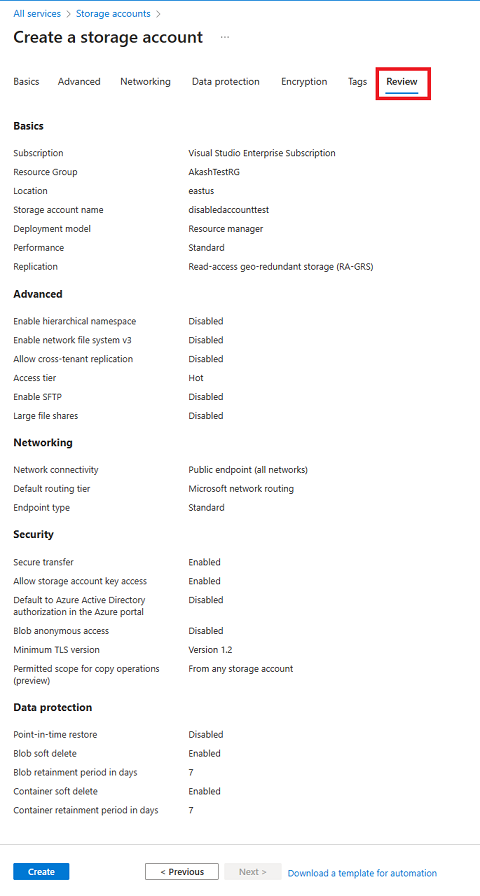
[](https://learn.microsoft.com/en-us/azure/storage/common/media/storage-account-create/create-account-tags-tab-lrg.png#lightbox)

**Review + create tab**

When you navigate to the **Review + create** tab, Azure runs validation on the storage account settings that you have chosen. If validation passes, you can proceed to create the storage account.

If validation fails, then the portal indicates which settings need to be modified.

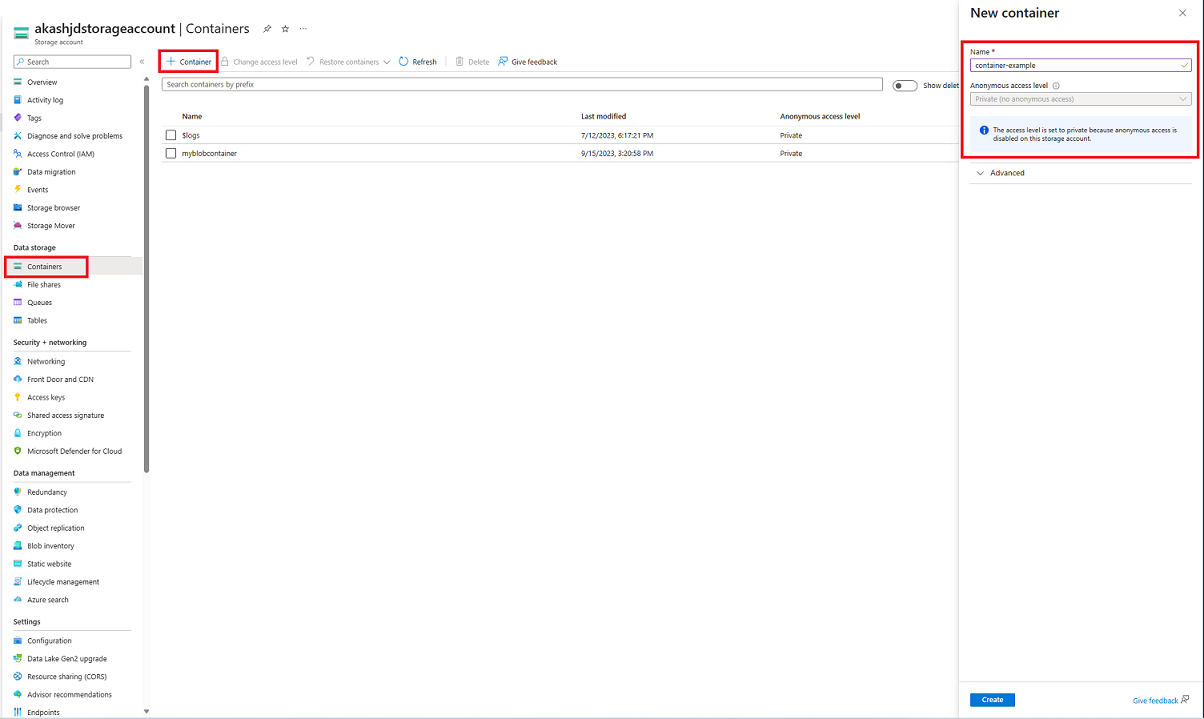
The following image shows the **Review** tab data prior to the creation of a new storage account.

[](https://learn.microsoft.com/en-us/azure/storage/common/media/storage-account-create/create-account-review-tab-lrg.png#lightbox)

## Create a container

To create a container in the Azure portal, follow these steps:

1. Navigate to your new storage account in the Azure portal.
2. In the left menu for the storage account, scroll to the **Data storage** section, then select **Containers**.
3. Select the **+ Container** button.
4. Type a name for your new container. The container name must be lowercase, must start with a letter or number, and can include only letters, numbers, and the dash (-) character. For more information about container and blob names, see [Naming and referencing containers, blobs, and metadata](https://learn.microsoft.com/en-us/rest/api/storageservices/naming-and-referencing-containers--blobs--and-metadata).
5. Set the level of anonymous access to the container. The default level is **Private (no anonymous access)**.
6. Select **Create** to create the container.

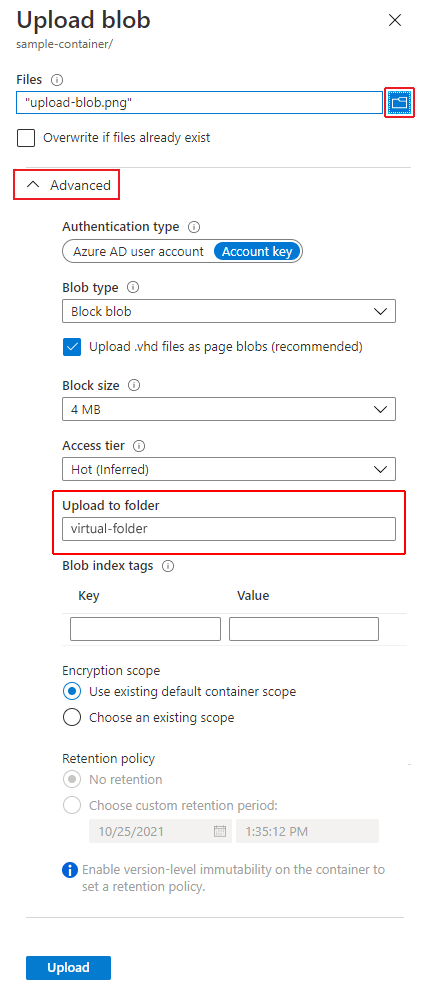
[](https://learn.microsoft.com/en-us/azure/storage/blobs/media/storage-quickstart-blobs-portal/create-container-lrg.png#lightbox)

## Upload a block blob

Block blobs consist of blocks of data assembled to make a blob. Most scenarios using Blob storage employ block blobs. Block blobs are ideal for storing text and binary data in the cloud, like files, images, and videos. This quickstart shows how to work with block blobs.

To upload a block blob to your new container in the Azure portal, follow these steps:

1. In the Azure portal, navigate to the container you created in the previous section.
2. Select the container to show a list of blobs it contains. This container is new, so it won't yet contain any blobs.
3. Select the **Upload** button to open the upload blade and browse your local file system to find a file to upload as a block blob. You can optionally expand the **Advanced** section to configure other settings for the upload operation. You can, for example, upload a blob into a new or existing virtual folder or by supplying a value in the **Upload to folder** field.



1. Select the **Upload** button to upload the blob.
2. Upload as many blobs as you like in this way. You'll see that the new blobs are now listed within the container.

# Configure a lifecycle management policy

Azure Storage lifecycle management offers a rule-based policy that you can use to transition blob data to the appropriate access tiers or to expire data at the end of the data lifecycle. A lifecycle policy acts on a base blob, and optionally on the blob's versions or snapshots. For more information about lifecycle management policies, see [Optimize costs by automatically managing the data lifecycle](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview).

A lifecycle management policy is composed of one or more rules that define a set of actions to take based on a condition being met. For a base blob, you can choose to check one of the following conditions:

* The number of days since the blob was created.
* The number of days since the blob was last modified.
* The number of days since the blob was last accessed. To use this condition in an action, you should first [optionally enable last access time tracking](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal#optionally-enable-access-time-tracking).

When the selected condition is true, then the management policy performs the specified action. For example, if you have defined an action to move a blob from the hot tier to the cool tier if it has not been modified for 30 days, then the lifecycle management policy will move the blob 30 days after the last write operation to that blob.

For a blob snapshot or version, the condition that is checked is the number of days since the snapshot or version was created.

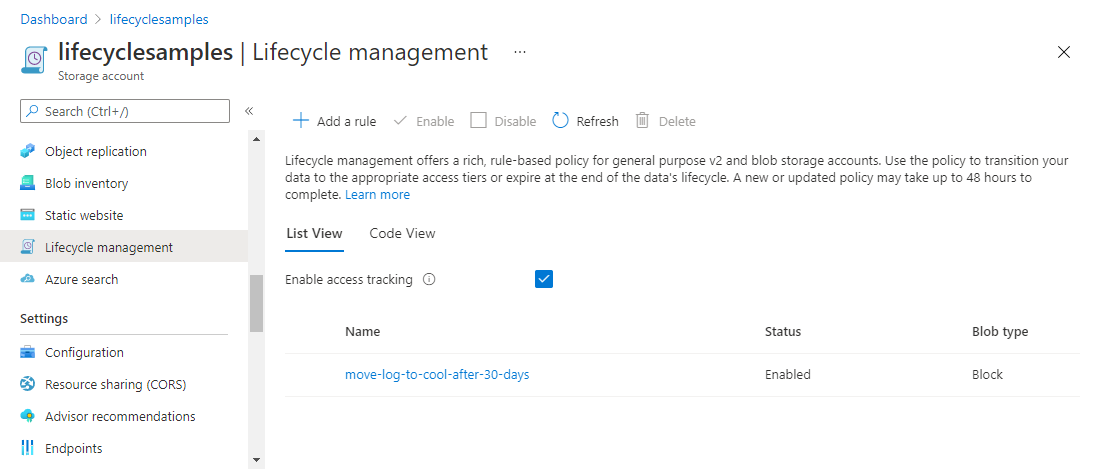
## Optionally enable access time tracking

Before you configure a lifecycle management policy, you can choose to enable blob access time tracking. When access time tracking is enabled, a lifecycle management policy can include an action based on the time that the blob was last accessed with a read or write operation. To minimize the effect on read access latency, only the first read of the last 24 hours updates the last access time. Subsequent reads in the same 24-hour period don't update the last access time. If a blob is modified between reads, the last access time is the more recent of the two values.

If [last access time tracking](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview#move-data-based-on-last-accessed-time) is not enabled, **daysAfterLastAccessTimeGreaterThan** uses the date the lifecycle policy was enabled instead of the LastAccessTime property of the blob. This date is also used when the LastAccessTime property is a null value. For more information about using last access time tracking, see [Move data based on last accessed time](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-overview#move-data-based-on-last-accessed-time).

To enable last access time tracking with the Azure portal, follow these steps:

1. Navigate to your storage account in the Azure portal.
2. In the **Data management** section, select **Lifecycle management**.
3. Check the checkbox "Enable access tracking"



Use the **daysAfterLastAccessTimeGreaterThan** property to specify the number of days from last access after which an action should be taken on a blob.

## Create or manage a policy

You can add, edit, or remove a lifecycle management policy with the Azure portal, PowerShell, Azure CLI, or an Azure Resource Manager template.

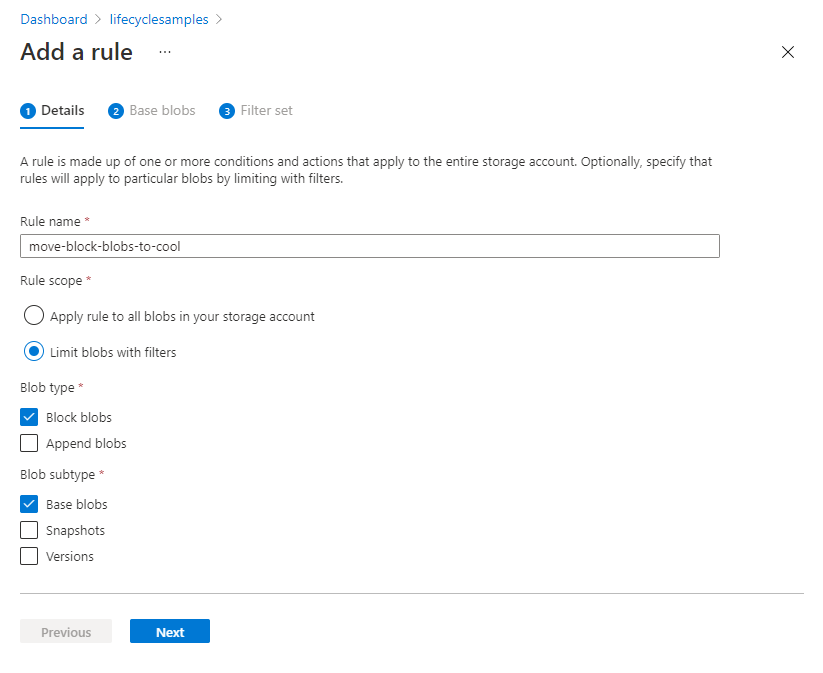
* [Portal](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal#tabpanel_2_azure-portal)
* [PowerShell](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal#tabpanel_2_azure-powershell)
* [Azure CLI](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal#tabpanel_2_azure-cli)
* [Template](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal#tabpanel_2_template)

There are two ways to add a policy through the Azure portal.

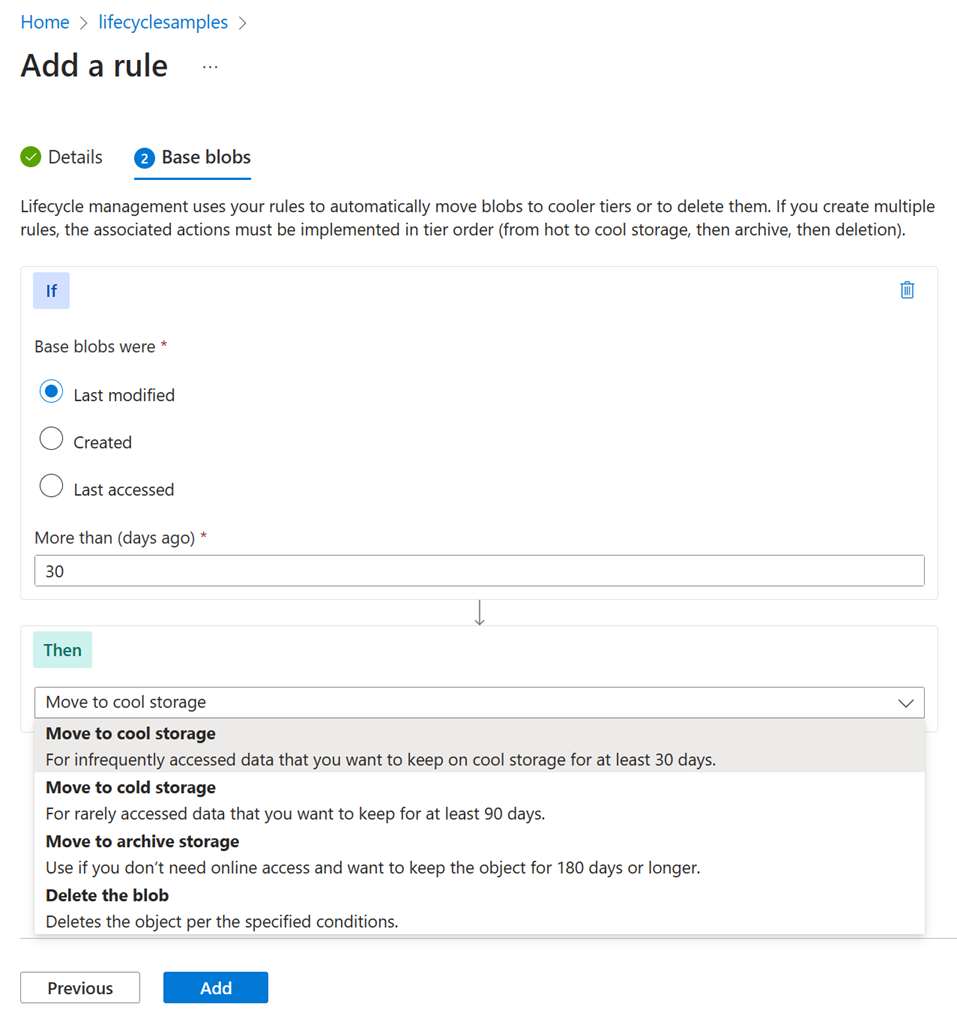
* [List view](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal#list-view)
* [Code view](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal#code-view)

#### List view

1. In the Azure portal, navigate to your storage account.
2. Under **Data management**, select **Lifecycle Management** to view or change lifecycle management policies.
3. Select the **List View** tab.
4. Select **Add a rule** and name your rule on the **Details** form. You can also set the **Rule scope**, **Blob type**, and **Blob subtype** values. The following example sets the scope to filter blobs. This causes the **Filter set** tab to be added.

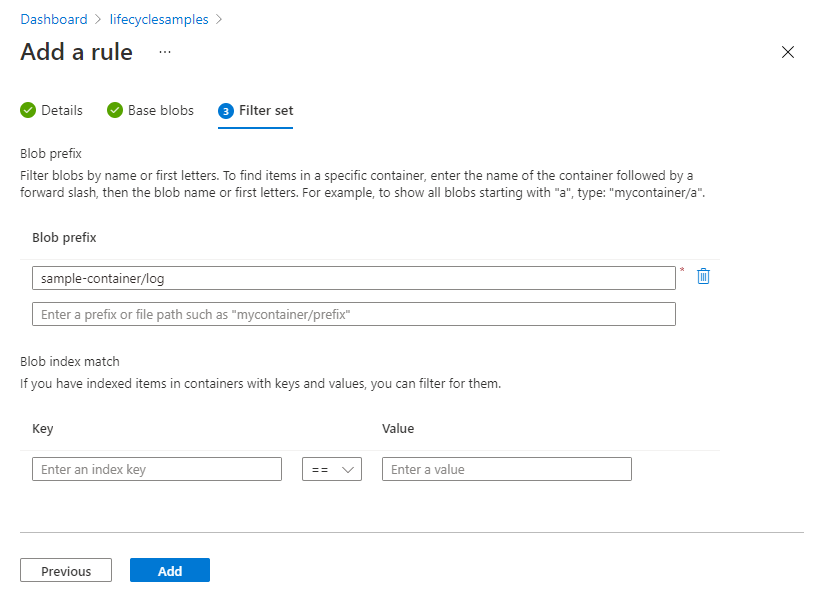


1. Select **Base blobs** to set the conditions for your rule. In the following example, blobs are moved to cool storage if they haven't been modified for 30 days.



The **Last accessed** option is available only if you have enabled access time tracking and you've selected **Block blobs** as the blob type. To learn how to enable access tracking, see [Optionally enable access time tracking](https://learn.microsoft.com/en-us/azure/storage/blobs/lifecycle-management-policy-configure?tabs=azure-portal#optionally-enable-access-time-tracking).

1. If you selected **Limit blobs with filters** on the **Details** page, select **Filter set** to add an optional filter. The following example filters on blobs whose name begins with log in a container called sample-container.



1. Select **Add** to add the new policy.

Keep in mind that a lifecycle management policy will not delete the current version of a blob until any previous versions or snapshots associated with that blob have been deleted. If blobs in your storage account have previous versions or snapshots, then you should select **Base blobs**, **Snapshots**, and **Versions** in the **Blob Subtype** section when you are specifying a delete action as part of the policy.