About Azure storage accounts

**Overview**

An Azure storage account provides a unique namespace to store and access your Azure Storage data objects. All objects in a storage account are billed together as a group. By default, the data in your account is available only to you, the account owner.

There are two types of storage accounts:

**General-purpose Storage Accounts**

A general-purpose storage account gives you access to Azure Storage services such as Tables, Queues, Files, Blobs and Azure virtual machine disks under a single account. This type of storage account has two performance tiers:

* A standard storage performance tier which allows you to store Tables, Queues, Files, Blobs and Azure virtual machine disks.
* A premium storage performance tier which currently only supports Azure virtual machine disks. See [Premium Storage: High-Performance Storage for Azure Virtual Machine Workloads](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/premium-storage) for an in-depth overview of Premium storage.

**Blob Storage Accounts**

A Blob storage account is a specialized storage account for storing your unstructured data as blobs (objects) in Azure Storage. Blob storage accounts are similar to your existing general-purpose storage accounts and share all the great durability, availability, scalability, and performance features that you use today including 100% API consistency for block blobs and append blobs. For applications requiring only block or append blob storage, we recommend using Blob storage accounts.

Note

Blob storage accounts support only block and append blobs, and not page blobs.

Blob storage accounts expose the **Access Tier** attribute which can be specified during account creation and modified later as needed. There are two types of access tiers that can be specified based on your data access pattern:

* A **Hot** access tier which indicates that the objects in the storage account will be more frequently accessed. This allows you to store data at a lower access cost.
* A **Cool** access tier which indicates that the objects in the storage account will be less frequently accessed. This allows you to store data at a lower data storage cost.

If there is a change in the usage pattern of your data, you can also switch between these access tiers at any time. Changing the access tier may result in additional charges. Please see [Pricing and billing for Blob storage accounts](https://docs.microsoft.com/en-in/azure/storage/blobs/storage-account-options#pricing-and-billing) for more details.

For more details on Blob storage accounts, see [Azure Blob Storage: Cool and Hot tiers](https://docs.microsoft.com/en-in/azure/storage/blobs/storage-blob-storage-tiers).

Before you can create a storage account, you must have an Azure subscription, which is a plan that gives you access to a variety of Azure services. You can get started with Azure with a [free account](https://azure.microsoft.com/pricing/free-trial/). Once you decide to purchase a subscription plan, you can choose from a variety of [purchase options](https://azure.microsoft.com/pricing/purchase-options/). If you’re an [MSDN subscriber](https://azure.microsoft.com/pricing/member-offers/msdn-benefits-details/), you get free monthly credits that you can use with Azure services, including Azure Storage. See [Azure Storage Pricing](https://azure.microsoft.com/pricing/details/storage/)for information on volume pricing.

To learn how to create a storage account, see [Create a storage account](https://docs.microsoft.com/en-in/azure/storage/common/storage-create-storage-account#create-a-storage-account) for more details. You can create up to 200 uniquely named storage accounts with a single subscription. See [Azure Storage Scalability and Performance Targets](https://docs.microsoft.com/en-in/azure/storage/common/storage-scalability-targets) for details about storage account limits.

**Storage account billing**

You are billed for Azure Storage usage based on your storage account. Storage costs are based on the following factors: region/location, account type, storage capacity, replication scheme, storage transactions, and data egress.

* Region refers to the geographical region in which your account is based.
* Account type refers to whether you are using a general-purpose storage account or a Blob storage account. With a Blob storage account, the access tier also determines the billing model for the account.
* Storage capacity refers to how much of your storage account allotment you are using to store data.
* Replication determines how many copies of your data are maintained at one time, and in what locations.
* Transactions refer to all read and write operations to Azure Storage.
* Data egress refers to data transferred out of an Azure region. When the data in your storage account is accessed by an application that is not running in the same region, you are charged for data egress. (For Azure services, you can take steps to group your data and services in the same data centers to reduce or eliminate data egress charges.)

The [Azure Storage Pricing](https://azure.microsoft.com/pricing/details/storage/) page provides detailed pricing information based on account type, storage capacity, replication, and transactions. The [Data Transfers Pricing Details](https://azure.microsoft.com/pricing/details/data-transfers/) provides detailed pricing information for data egress. You can use the [Azure Storage Pricing Calculator](https://azure.microsoft.com/pricing/calculator/?scenario=data-management) to help estimate your costs.

Note

When you create an Azure virtual machine, a storage account is created for you automatically in the deployment location if you do not already have a storage account in that location. So it's not necessary to follow the steps below to create a storage account for your virtual machine disks. The storage account name will be based on the virtual machine name. See the [Azure Virtual Machines documentation](https://azure.microsoft.com/documentation/services/virtual-machines/) for more details.

Storage account endpoints

Every object that you store in Azure Storage has a unique URL address. The storage account name forms the subdomain of that address. The combination of subdomain and domain name, which is specific to each service, forms an *endpoint* for your storage account.

For example, if your storage account is named *mystorageaccount*, then the default endpoints for your storage account are:

* Blob service: http://*mystorageaccount*.blob.core.windows.net
* Table service: http://*mystorageaccount*.table.core.windows.net
* Queue service: http://*mystorageaccount*.queue.core.windows.net
* File service: http://*mystorageaccount*.file.core.windows.net

Note

A Blob storage account only exposes the Blob service endpoint.

The URL for accessing an object in a storage account is built by appending the object's location in the storage account to the endpoint. For example, a blob address might have this format: http://*mystorageaccount*.blob.core.windows.net/*mycontainer*/*myblob*.

You can also configure a custom domain name to use with your storage account. For more information, see [Configure a custom domain Name for your Blob Storage Endpoint](https://docs.microsoft.com/en-in/azure/storage/blobs/storage-custom-domain-name). You can also configure it with PowerShell. For more information, see the [Set-AzureRmStorageAccount](https://docs.microsoft.com/en-us/powershell/module/azurerm.storage/set-azurermstorageaccount) cmdlet.

**Create a storage account**

1. Sign in to the [Azure portal](https://portal.azure.com/).
2. In the Azure portal, expand the menu on the left side to open the menu of services, and choose **More Services**. Then, scroll down to **Storage**, and choose **Storage accounts**. On the **Storage Accounts** window that appears, choose **Add**.
3. Enter a name for your storage account. See [Storage account endpoints](https://docs.microsoft.com/en-in/azure/storage/common/storage-create-storage-account?toc=%2fazure%2fstorage%2fqueues%2ftoc.json#storage-account-endpoints) for details about how the storage account name will be used to address your objects in Azure Storage.

Note

Storage account names must be between 3 and 24 characters in length and may contain numbers and lowercase letters only.

Your storage account name must be unique within Azure. The Azure portal will indicate if the storage account name you select is already in use.

1. Specify the deployment model to be used: **Resource Manager** or **Classic**. **Resource Manager** is the recommended deployment model. For more information, see [Understanding Resource Manager deployment and classic deployment](https://docs.microsoft.com/en-in/azure/azure-resource-manager/resource-manager-deployment-model).

Note

Blob storage accounts can only be created using the Resource Manager deployment model.

1. Select the type of storage account: **General purpose** or **Blob storage**. **General purpose**is the default.

If **General purpose** was selected, then specify the performance tier: **Standard** or **Premium**. The default is **Standard**. For more details on standard and premium storage accounts, see [Introduction to Microsoft Azure Storage](https://docs.microsoft.com/en-in/azure/storage/common/storage-introduction) and [Premium Storage: High-Performance Storage for Azure Virtual Machine Workloads](https://docs.microsoft.com/en-in/azure/virtual-machines/windows/premium-storage).

If **Blob Storage** was selected, then specify the access tier: **Hot** or **Cool**. The default is **Hot**. See [Azure Blob Storage: Cool and Hot tiers](https://docs.microsoft.com/en-in/azure/storage/blobs/storage-blob-storage-tiers) for more details.

1. Select the replication option for the storage account: **LRS**, **GRS**, **RA-GRS**, or **ZRS**. The default is **RA-GRS**. For more details on Azure Storage replication options, see [Azure Storage replication](https://docs.microsoft.com/en-in/azure/storage/common/storage-redundancy).
2. Select the subscription in which you want to create the new storage account.
3. Specify a new resource group or select an existing resource group. For more information on resource groups, see [Azure Resource Manager overview](https://docs.microsoft.com/en-in/azure/azure-resource-manager/resource-group-overview).
4. Select the geographic location for your storage account. See [Azure Regions](https://azure.microsoft.com/regions/#services) for more information about what services are available in which region.
5. Click **Create** to create the storage account.

**Manage your storage account**

**Change your account configuration**

After you create your storage account, you can modify its configuration, such as changing the replication option used for the account or changing the access tier for a Blob storage account. In the [Azure portal](https://portal.azure.com/), navigate to your storage account, find and click **Configuration** under **SETTINGS**to view and/or change the account configuration.

Note

Depending on the performance tier you chose when creating the storage account, some replication options may not be available.

Changing the replication option will change your pricing. For more details, see [Azure Storage Pricing](https://azure.microsoft.com/pricing/details/storage/) page.

For Blob storage accounts, changing the access tier may incur charges for the change in addition to changing your pricing. Please see the [Blob storage accounts - Pricing and Billing](https://docs.microsoft.com/en-in/azure/storage/blobs/storage-account-options#pricing-and-billing) for more details.

**Manage your storage access keys**

When you create a storage account, Azure generates two 512-bit storage access keys, which are used for authentication when the storage account is accessed. By providing two storage access keys, Azure enables you to regenerate the keys with no interruption to your storage service or access to that service.

Note

We recommend that you avoid sharing your storage access keys with anyone else. To permit access to storage resources without giving out your access keys, you can use a *shared access signature*. A shared access signature provides access to a resource in your account for an interval that you define and with the permissions that you specify. See [Using Shared Access Signatures (SAS)](https://docs.microsoft.com/en-in/azure/storage/common/storage-dotnet-shared-access-signature-part-1) for more information.

View and copy storage access keys

In the [Azure portal](https://portal.azure.com/), navigate to your storage account, click **All settings** and then click **Access keys** to view, copy, and regenerate your account access keys. The **Access Keys**blade also includes pre-configured connection strings using your primary and secondary keys that you can copy to use in your applications.

**Regenerate storage access keys**

We recommend that you change the access keys to your storage account periodically to help keep your storage connections secure. Two access keys are assigned so that you can maintain connections to the storage account by using one access key while you regenerate the other access key.

Warning

Regenerating your access keys can affect services in Azure as well as your own applications that are dependent on the storage account. All clients that use the access key to access the storage account must be updated to use the new key.

**Media services** - If you have media services that are dependent on your storage account, you must re-sync the access keys with your media service after you regenerate the keys.

**Applications** - If you have web applications or cloud services that use the storage account, you will lose the connections if you regenerate keys, unless you roll your keys.

**Storage Explorers** - If you are using any [storage explorer applications](https://docs.microsoft.com/en-in/azure/storage/common/storage-explorers), you will probably need to update the storage key used by those applications.

Here is the process for rotating your storage access keys:

1. Update the connection strings in your application code to reference the secondary access key of the storage account.
2. Regenerate the primary access key for your storage account. On the **Access Keys** blade, click **Regenerate Key1**, and then click **Yes** to confirm that you want to generate a new key.
3. Update the connection strings in your code to reference the new primary access key.
4. Regenerate the secondary access key in the same manner.

**Delete a storage account**

To remove a storage account that you are no longer using, navigate to the storage account in the [Azure portal](https://portal.azure.com/), and click **Delete**. Deleting a storage account deletes the entire account, including all data in the account.

Warning

It's not possible to restore a deleted storage account or retrieve any of the content that it contained before deletion. Be sure to back up anything you want to save before you delete the account. This also holds true for any resources in the account—once you delete a blob, table, queue, or file, it is permanently deleted.

If you try to delete a storage account associated with an Azure virtual machine, you may get an error about the storage account still being in use. For help troubleshooting this error, please see [Troubleshoot errors when you delete storage accounts](https://docs.microsoft.com/en-in/azure/storage/common/storage-resource-manager-cannot-delete-storage-account-container-vhd).+