**Create a storage account using Azure portal**

1. Sign into the [Azure portal](https://portal.azure.com/learn.docs.microsoft.com) using the same account
2. On the Azure portal menu, or from the **Home** page, under **Azure services**, select **Create a resource**. The **Create a resource** pane appears.
3. In the left menu pane, select **Storage**, and then search for and select **Storage account**. The **Storage account** pane appears.
4. Select **Create.** The **Create a storage account** pane appears.
5. On the **Basics** tab, enter the following values for each setting.

| **TABLE 1** | |
| --- | --- |
| **Setting** | **Value** |
| **Project details** |  |
| Subscription | Concierge Subscription |
| Resource group | ("[sandbox resource group name]") from the dropdown list. |
| **Instance details** |  |
| Storage account name | The name will be used to generate the public URL used to access the data in the account. The name must be unique across all existing storage account names in Azure. Names must be 3 to 24 characters long and can contain only lowercase letters and numbers. |
| Region | Select a location near to you in the dropdown list. |
| Performance | Standard. This option decides the type of disk storage used to hold the data in the Storage account. Standard uses traditional hard disks, and Premium uses solid-state drives (SSD) for faster access. |
| Redundancy | Select *Locally redundant storage (LRS)* from the dropdown list. In our case, the images and videos quickly become out-of-date and are removed from the site. As a result, there's little value to paying extra for global redundancy. If a catastrophic event results in data loss, you can restart the site with fresh content from your users. |

1. The free sandbox allows you to create resources in a subset of the Azure global regions. Select a region from the following list when you create resources:
   * West US 2
   * South Central US
   * Central US
   * East US
   * West Europe
   * Southeast Asia
   * Japan East
   * Brazil South
   * Australia Southeast
   * Central India
2. Select **Next : Advanced**. Enter the following values for each setting.

| **TABLE 2** | |
| --- | --- |
| **Setting** | **Value** |
| **Security** |  |
| Require secure transfer for REST API operations | *Check*. This setting controls whether **HTTP** can be used for the REST APIs that access data in the storage account. Setting this option to *enable* forces all clients to use SSL (**HTTPS**). Most of the time, you'll want to set this to *enable* as using HTTPS over the network is considered a best practice. |
| Enable blob public access | *Check*. We'll allow clients to read data in that container without authorizing the request. |
| Minimum TLS version | Select *Version 1.2* from dropdown list. TLS 1.2 is the most secure version of TLS and is used by Azure Storage on public HTTPS endpoints. TLS 1.1 and 1.0 is supported for backwards compatibility. See *Warning* at end of table. |
| **Data Lake Storage Gen 2** |  |
| Enable hierarchical namespace | *Uncheck*. This is for big-data applications that aren't relevant to this module. |
| **Blob storage** |  |
| Access tier | *Hot*. This setting is only used for Blob storage. The *Hot* access tier is ideal for frequently accessed data; the *Cool* access tier is better for infrequently accessed data. This setting only sets the *default* value. When you create a Blob, you can set a different value for the data. In our case, we want the videos to load quickly, so we'll use the high-performance option for our blobs. |
| **Azure Files** |  |
| Enable large file shares | *Uncheck*. Large file shares provide support up to a 100 TiB, however this type of storage account can't convert to a Geo-redundant storage offering, and upgrades are permanent. |

1. **Warning**
2. If this option is enabled, it will enforce some additional restrictions. Azure files service connections without encryption will fail, including scenarios using SMB 2.1 or 3.0 on Linux. Because Azure storage doesn't support SSL for custom domain names, this option cannot be used with a custom domain name.
3. Select **Next : Networking**. Enter the following values for each setting.

| **TABLE 3** | |
| --- | --- |
| **Setting** | **Value** |
| **Network connectivity** |  |
| Connectivity method | *Public endpoint (all networks)*. We want to allow public Internet access. Our content is public facing, and we need to allow access from public clients. |
| **Network routing** |  |
| Routing preference | *Microsoft network routing*. We want to make use of the Microsoft global network that is optimized for low-latency path selection. |

1. Select **Next : Data protection**. Enter the following value for the setting.

| **TABLE 4** | |
| --- | --- |
| **Setting** | **Value** |
| **Recovery** |  |
| Enable soft delete for blobs | *Uncheck*. Soft delete lets you recover your blob data in many cases where blobs or blob snapshots are deleted accidentally or overwritten. |
| Enable soft delete for file shares | *Uncheck*. File share soft delete lets you recover your blob data more easily at the folder level. |

1. Select **Next : Tags**. Here, you associate key/value pairs to the account for your categorization and determine if a feature is available to any Azure resource.
2. Select **Review + create** to review the settings. This will do a quick validation of your options to make sure all the required fields are selected. If there are issues, they'll be reported here.
3. After validation passes, select **Create** to provision the storage account.

It may take two minutes to deploy the account.

1. After validation succeeds, select **Go to resource** to view your newly-created storage account.

You created a storage account with settings driven by your business requirements. For example, you might have selected a West US datacenter because your customers were primarily located in southern California. This is a typical flow: first analyze your data and goals, and then configure the storage account options to match.