1. Objective – Create and configure storage account

1. Select **Home > Resource groups**, then choose your resource group, such as *oreilly-az104*
2. At the top of the resource group window select **+ Add**, search for and select "*storage account*", then choose **Create**. Enter the following configuration information. If not noted below, use the defaults:

   Resource group: *oreilly-az104*

   Name: *az104<yourinitials-or-random-value> (must be all lowercase, no special chars)*

   Location: *West US*

   Performance: *Standard*

   Account kind: *StorageV2 (general purpose v2)*

   Replication: *Read-access geo-redundant storage (RA-GRS)*

   Access tier (default): *Hot*

3. When ready, select **Review + create**, then **Create**
4. If needed, select the notification bell in the top right-hand corner to view deployment progress as the storage account is created. It takes a minute or two to create the resource. When ready, select **Go to resource**.

2. Objective – Manage access keys

1. From your storage account, select **Access keys** from the menu on the left-hand side.
2. Two keys are available. One of these keys should be used for your applications to access the storage account. Ideally, store these keys in a central digital store like Azure Key Vault, not hard-coded into the applications.

   When needed, rotate the keys. Update the digital vault or application code to switch from using *key1* to using *key2*. Then, generate a new *key1.*

   Select the *Regenerate* circular icon next to *key1*, then **Yes** to regenerate the access key.
3. In time, you'd repeat the process to move applications from using *key2* to using *key1* and this time regenerate *key2*. This two-key approach means your applications can continue to work using the alternate key while you regenerate and invalid the previous key.

3. Objective – Generate shared access signature

1. From your storage account, select **Shared access signature** from the menu on the left-hand side.
2. Use the check boxes to allow only access to *Blob* storage across the whole *Service*, but only with *Read* permissions.

   Set the SAS to expire one week from today. Only allow *HTTPS*, and sign using *key1*

3. Select **Generate SAS and connection string**. The connection string and SAS token would be given to developers to partners to use as needed in their application connections. The Azure portal doesn't let you retrieve a SAS once you close out this window.

4. Objective – Configure network access to the storage account

1. From your storage account, select **Firewalls and virtual networks** from the menu on the left-hand side.
2. By default, *All networks* are allowed to connect. Instead, choose *Selected networks*
3. Select **+ Add existing virtual network**, then choose the *vnet-westus* virtual network. Select the *backend-subnet.*
4. Note that you can also add your own client to access the storage account, or an IP address range like an on-premises office location.

   Exceptions for other Azure services to access the storage account can also be added, including ingesting storage logs or metrics, such as for Azure Monitor.