1. Objective – Implement and set tagging on resource groups

1. Select **Home > Resource groups**, then choose your resource group, such as *oreilly-az104*
2. Select **Tags** from the menu on the left-hand side. Tags are name/value pairs. Enter the following tag information:

   Name: *dept*
   Value: *training*

3. Choose **Save**. This is a common approach to assigning tags based on department, or cost center. Other values could be *finance, hr,* or *research.*
   You can then search for resources based on tags, and billing reports will report tags to let you analyze in Excel, or similar.

2. Objective – Configure resource locks

1. Select **Home > Resource groups**, then choose your resource group, such as *oreilly-az104*
2. Select **Locks** from the menu on the left-hand side, then **+ Add**

   Lock name: *NoDelete*

   Lock type: Delete

3. When ready, select **OK.** Take care with *Read-Only* resource locks as this may have unexpected consequences on resources that need storage writes, for example.
4. In the next exercise, you try to delete the resource group to see this lock in action.

3. Objective – Remove resource groups

1. Select **Home > Resource groups**, then choose your resource group, such as *oreilly-az104*
2. At the top of the **Overview** page, select **Delete resource group**
3. In the confirmation window, enter the name of the resource group, such as *oreilly-az104*, then select **Delete**
4. The notification bell in the top right-hand corner shows that the resource is locked and can't be deleted. It's good practice to lock critical resource groups from accidental, or malicious, deletion. But, it's also good practice to keep your Azure environment clean and delete resource groups when you're done with them. Doing so keeps your Azure costs low, especially for training and studying.
5. Select **Locks**, then select **Delete** on the right-hand side of the your *NoDelete* lock in the list. Don't try to delete your resource group just yet, as you still have one more exercise to do!

4. Objective – Assign RBAC roles and access to Azure resources

1. Select **Home > Resource groups**, then choose your resource group, such as *oreilly-az104*
2. Select your VM, such as *winvm01*, then select **Access control (IAM)** from the menu on the left-hand side.

3. Choose **Role assignments**. A list of existing assignments is shown. Select **+ Add**, then **Add role assignment**
4. There are dozens of built-in roles you can use for resources. Select *Virtual Machine Contributor.*
5. You want to **Assign access to** an *Azure AD user, group, or service principal*, then select your *Azure User* from previous labs.
   When ready, select **Save**
6. Open an InPrivate or Incognito window in your web browser to https://portal.azure.com. When prompted to sign in, enter the credentials you copied to a text editor in the previous labs, such as for *azureuser@<yourtenant>.onmicrosoft.com*
7. Enter and confirm a new password after you sign in with the temporary password created for the user. Once signed in to the Azure portal, select **Home > All resources**
8. The VM, such as *winvm01*, should be listed. No other resources from your Azure subscription are shown. You only assigned RBAC roles to this one VM. Select the VM from the list.
9. You can review overview information and perform some basic VM tasks. The *Virtual Machine Contributor* role doesn't let you configure settings beyond the basic VM.
   Try to select **Networking** or **Disks**. Errors are shown that you don't have permissions to view or configure some settings.

   RBAC permissions can be very granular when applied, so plan out your business requirements carefully. Follow the principal of least access. Only assign the permissions required. You can create and assign custom RBAC roles if needed.