**Lab 12: Azure Custom Role Assignments**

**Step 1: Access the Azure Portal**

1. **Explanation**: The Azure portal is where you manage all your Azure resources.
2. **How to Do It**: Open your web browser and go to [portal.azure.com](https://portal.azure.com/). Log in with your Azure credentials.

**Step 2: Navigate to the Azure Subscription**

1. **Explanation**: Subscriptions are like containers that hold all your Azure resources and settings. To create a custom role, you need to decide where it will be used, and the subscription level is the top of the hierarchy.
2. **How to Do It**: In the Azure Portal, click on "Subscriptions" in the left-hand sidebar. If it's not visible, use the search bar at the top to find it. Click on the subscription where you want to add the custom role.

**Step 3: Access Access Control (IAM)**

1. **Explanation**: Access control (IAM) is where you manage who has permission to do what with your resources. You can assign predefined roles or create custom ones.
2. **How to Do It**: Once you're on the subscription's overview page, find and click on "Access control (IAM)" in the left-hand menu. This will open a new page with all the access settings.

**Step 4: Add a Custom Role**

1. **Explanation**: Adding a custom role allows you to precisely control what permissions are granted to users or groups, based on your specific requirements.
2. **How to Do It**: In the "Access control (IAM)" page, click the "Add" button, then choose "Add custom role" from the dropdown. A wizard will open to guide you through the creation process.

**Step 5: Define the Basics**

1. **Explanation**: This is where you define basic information about your custom role, like its name and description.
2. **How to Do It**:
   * In the "Basics" tab of the wizard, type a name for the role, like "AzureML Data Scientist Extended."
   * Write a description that clarifies the role's purpose, such as "Extended Data Scientist role for Azure Machine Learning."
   * Click "Next: Permissions."

**Step 6: Set Permissions**

1. **Explanation**: Permissions define what actions the role can and cannot perform on specific resources.
2. **How to Do It**:
   * Click "+ Add permissions" to open a pane where you can select services and permissions.
   * Filter by "Machine Learning" to narrow down the list.
   * Choose permissions relevant to data scientists, such as "Microsoft.MachineLearningServices/workspaces" for reading, writing, and deleting workspaces.
   * Make sure the actions you want aren't blocked by "NotActions." If they are, remove them from the "NotActions" list.
   * Click "Next: Assignable scopes."

**Step 7: Set the Assignable Scope**

1. **Explanation**: Assignable scopes determine where this role can be assigned. For example, at the subscription level, anyone with the role can manage any resource within that subscription.
2. **How to Do It**:
   * Click "+ Add assignable scope."
   * Select the scope you want: subscription, resource group, or resource level. For broader permissions, use the subscription level.
   * Click "Next: Review + create."

**Step 8: Review and Create the Role**

1. **Explanation**: This is where you double-check all your settings before finalizing the role.
2. **How to Do It**:
   * Review the role name, description, permissions, and assignable scopes to make sure everything is as you intended.
   * Click "Create" to finish creating the custom role.

**Step 9: Assign the Custom Role**

1. **Explanation**: Now that the role is created, assign it to users or groups who need these specific permissions.
2. **How to Do It**:
   * Go back to the "Access control (IAM)" page.
   * Click "Add," then "Add role assignment."
   * In the role dropdown, find and select the custom role you just created.
   * Click "Next."
   * Add the users or groups that should have this custom role.
   * Click "Next," then "Review + assign."

**Step 10: Verify the Custom Role Assignment**

1. **Explanation**: After assigning the role, it's important to confirm that the assignment was successful.
2. **How to Do It**:
   * Go back to the "Access control (IAM)" page.
   * Click on the "Role assignments" tab.
   * Look through the list to verify that the custom role is assigned to the intended users or groups.