

Objective

The objective of this lab is to understand how Azure subscriptions are managed and how **Role-Based Access Control (RBAC)** is used to control access to Azure resources by assigning roles to users.

Step no 1

The screenshot shows the Microsoft Azure portal with the title 'Create a resource group'. The 'Basics' tab is selected. The form fields are as follows:

- Subscription: Azure subscription 1
- Resource group name: Lab-RG
- Region: (US) East US

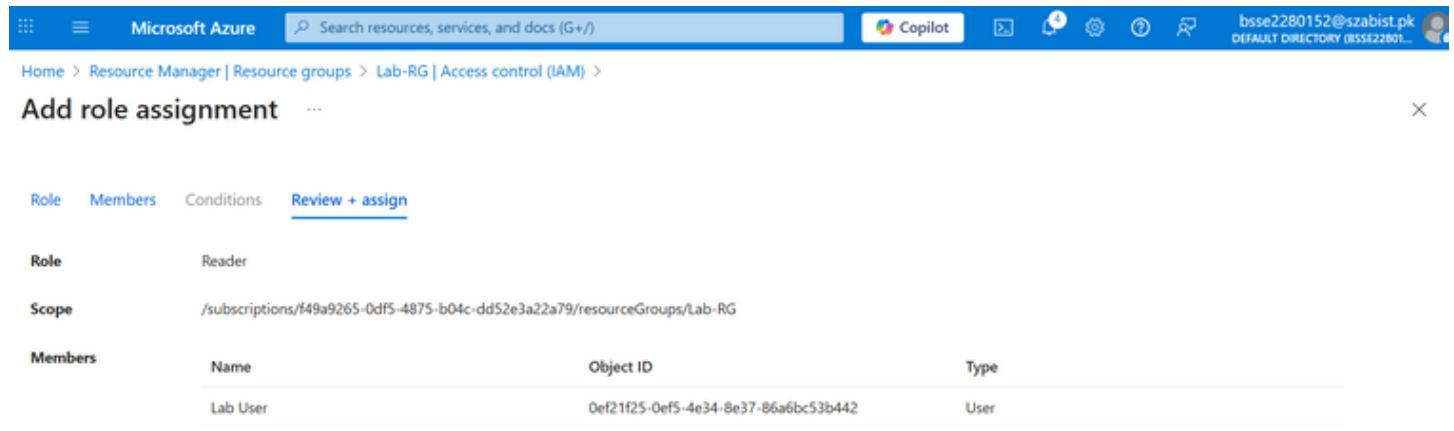
Step no 2

The screenshot shows the Microsoft Azure portal with the title 'Add role assignment'. The 'Selected role' is set to 'Reader'. The 'Assign access to' section has 'User, group, or service principal' selected. The 'Members' section shows a table with one row:

Name	Object ID	Type
Lab User	0ef21f25-0ef5-4e34-8e37-86a6bc53b442	User

The 'Description' field is empty. At the bottom, there are buttons for 'Review + assign', 'Previous', and 'Next'.

Step 03



The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with icons for Home, Search resources, services, and docs (G+/-), Copilot, and user information (bsse2280152@szabist.pk). Below the navigation bar, the URL path is visible: Home > Resource Manager | Resource groups > Lab-RG | Access control (IAM) > Add role assignment.

The main content area is titled "Add role assignment". It has tabs at the top: Role, Members, Conditions, and Review + assign. The "Review + assign" tab is currently selected. The "Role" section shows "Reader" assigned to the scope "/subscriptions/f49a9265-0df5-4875-b04c-dd52e3a22a79/resourceGroups/Lab-RG". The "Members" section lists a single member: "Lab User" with Object ID 0ef21f25-0ef5-4e34-8e37-86a6bc53b442, categorized as "User".

Result

Successfully managed Azure subscription access by creating a resource group and assigning RBAC roles. This lab demonstrated how Azure ensures secure access control using Role-Based Access Control.