Lab #4: **Azure Active Directory (Users, Groups, and Access Management)**

Purpose:

- We'll test permissions of roles and groups in Microsoft's Azure Active Directory (AD), which is now known as **Entra ID**. IAM is a crucial part of cybersecurity.

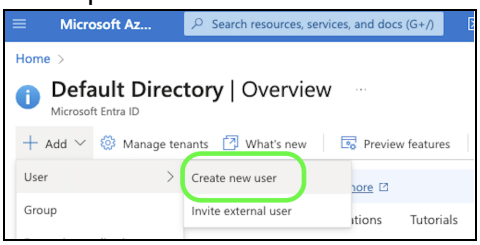
Tasks:

1. **Configure permissions #1: Tenant-Level Global Reader**
2. **Configure permissions #2: Subscription-Level Reader**
3. **Configure permissions #3: Resource Group-Level Contributor**

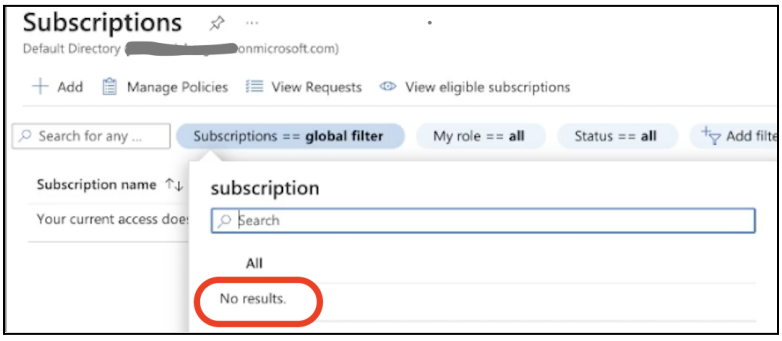
Task 1: **Configure permissions #1: Tenant-Level Global Reader**

***Note**: The **Tenant** level is the highest hierarchical level in Entra ID. The **Global Reader** role can read everything that a Global Admin can, but isn't able to update anything.*

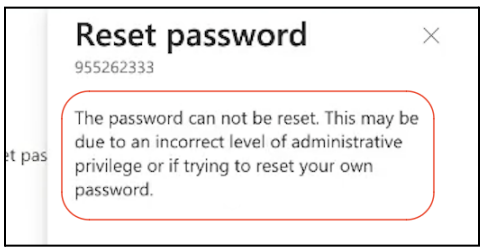
1. **Azure** portal > **Entra ID** > **Users** > create a new user account (**test1**).



   a. Select the **test1** user account > select **Assigned Roles** (under **Manage**) > select **Add Assignments** > select the **Global Reader** role.
2. Open a new incognito window > portal.azure.com > Log in as **test1**
3. Observe the result of being a Tenant-level "Global Reader".
   a. In **Subscriptions** → Unable to view anything (no "Subscriptions" access)



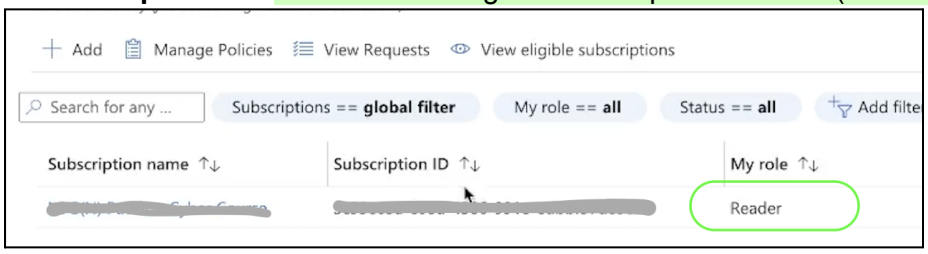
   b. In **Entra ID** → Able to view all users, but unable to change anything (e.g., passwords)



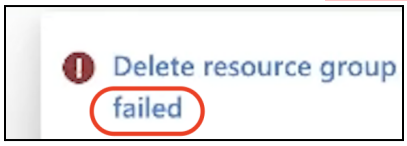
Task 2: Configure permissions #2: Subscription-Level Reader

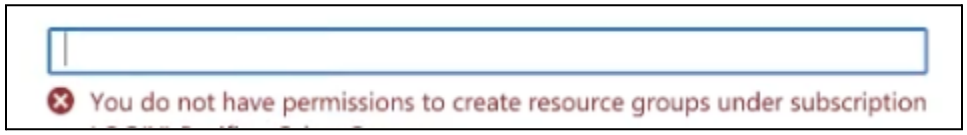
***Note**: The **Subscription** level is a middle hierarchical level in Entra ID used to manage access and organize billing. The **Subscription Reader** role can only read subscription-related areas.*

1. **Azure** portal > **Entra ID** > create a new user account (**test2**).
2. In **Subscriptions** > select my subscription > **IAM**
    a. Add a new role assignment > select the **Reader** role > assign the **test2** user account > the role is now assigned this permission.
3. Open a new incognito window > portal.azure.com > Log in as **test2**
4. Observe the result of being a Subscription-level "Reader".
    a. In **Subscriptions** → We see our assigned subscription and role ("Reader")



    b. In **Resource Groups** → Able to view our resource groups, but unable to change anything (e.g., delete or create groups)





Task 3: Configure permissions #3: Resource Group-Level Contributor

***Note**: After creating this test user account, we'll be providing them with **Contributor** permissions to a specific resource group (grants full access to manage resources in that group).*

1. **Azure** portal > **Entra ID** > create a new user account (**test3**).
2. In **Resource Groups** > create a new resource group > open this new resource group.
    a. In **IAM** > select **Add Resource Assignment** > assign Resource Group-level Contributor > assign the **test3** user account > the role is now assigned this permission.
3. Open a new incognito window > portal.azure.com > Log in as **test3**
4. Observe the result of being a Resource Groupt-level "Global Reader".
    a. In **Resource Groups** → Able to view and edit the one resource group, but unable to view and edit any other resource groups.

***Note**: We are able to create VMs and storage accounts, but only for resource groups that we have access to. If you try to assign an unauthorized group when creating a VM (e.g.) you'll receive a permission error.*

End:

- Go back to your Azure account and delete accounts and groups created for this lab.