Lab Report: Azure AD User Management and Access Control

Course Name: CST8912 – Cloud Solution Architecture
Lab Number: Graded Lab Activity #5
Lab Date: 2025-02-13
Submitted to: Prof. Tanishq Bansal
Student Name: ZheZhang
Student ID: 041109657

Title

Azure Active Directory (Microsoft Entra ID) User Management, Group Management, and Role-Based Access Control (RBAC).

Introduction or Purpose

The objective of this lab is to explore **Microsoft Entra ID (Azure AD)** by creating and managing **users, groups, and management groups**, and configuring **Role-Based Access Control (RBAC)**. Through this lab, we will:

- Create and configure **Azure AD users** (both internal and external users).
- Set up **static and dynamic security groups**.
- Create a **Management Group** for logical resource segmentation.
- Assign the **Virtual Machine Contributor** role to the **Help Desk group**.
- Clean up resources at the end of the experiment.

This hands-on activity helps simulate real-world **cloud identity and access management** scenarios applicable to any cloud provider.

Steps Covered in the Lab

Task 1: Create and Configure Azure AD Users

Step 1.1: Access Azure AD

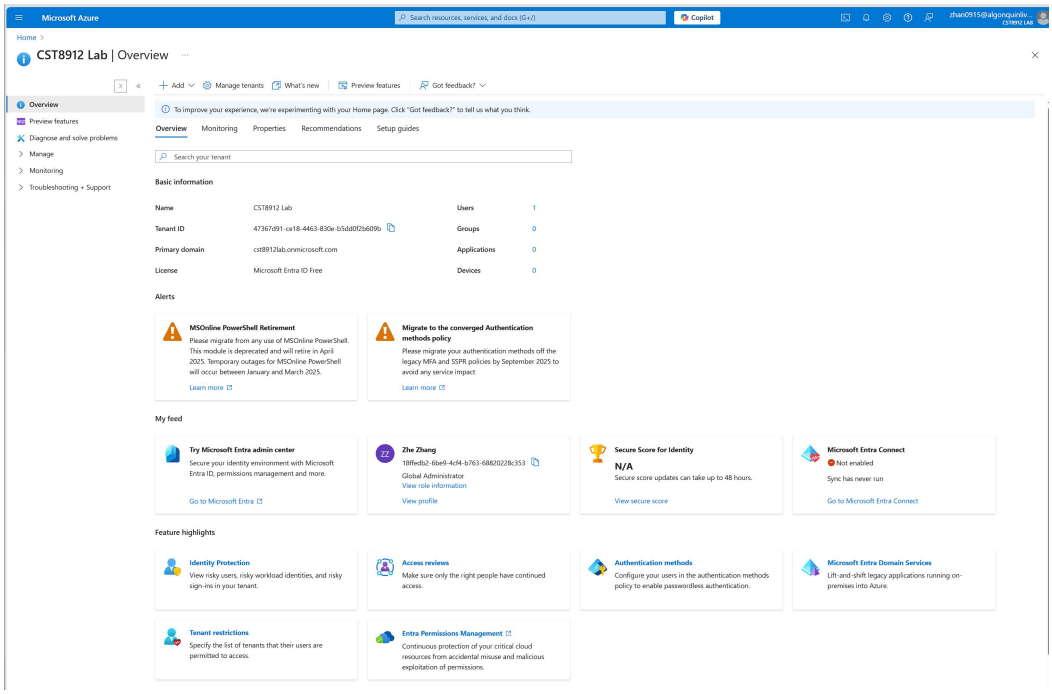
- Log in to **Azure Portal** (https://portal.azure.com).
- Search for **"Azure Active Directory"** and open **Microsoft Entra ID**.

Step 1.2: Create an Azure AD Tenant

- Navigate to **Manage > Create a tenant**.
- Choose **Microsoft Entra ID** as the tenant type.
- Enter the following details:

- **Organization name**: CST8912 Lab
- **Initial domain name**: cst8912org.onmicrosoft.com
- **Location**: Canada

- Click **Review + Create**, then **Create**, and wait for the tenant to be created.

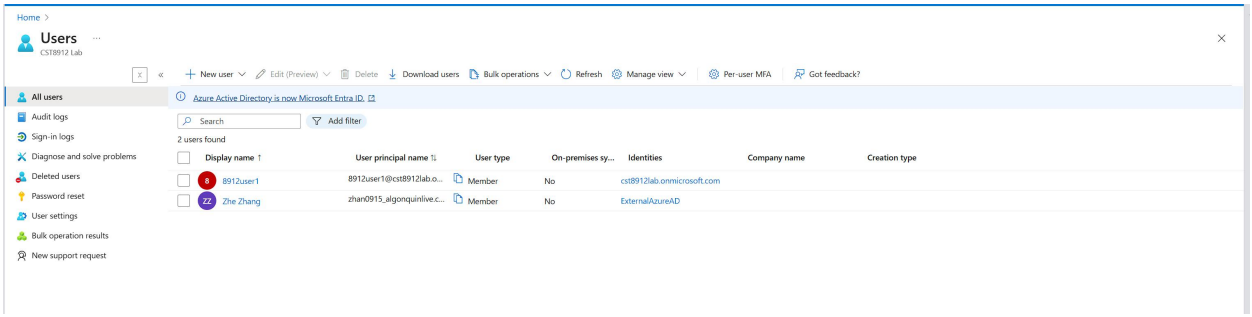


Step 1.3: Create a User

- Go to **Microsoft Entra ID > Users**.
- Click **+ New user**.
- Fill in the following details:

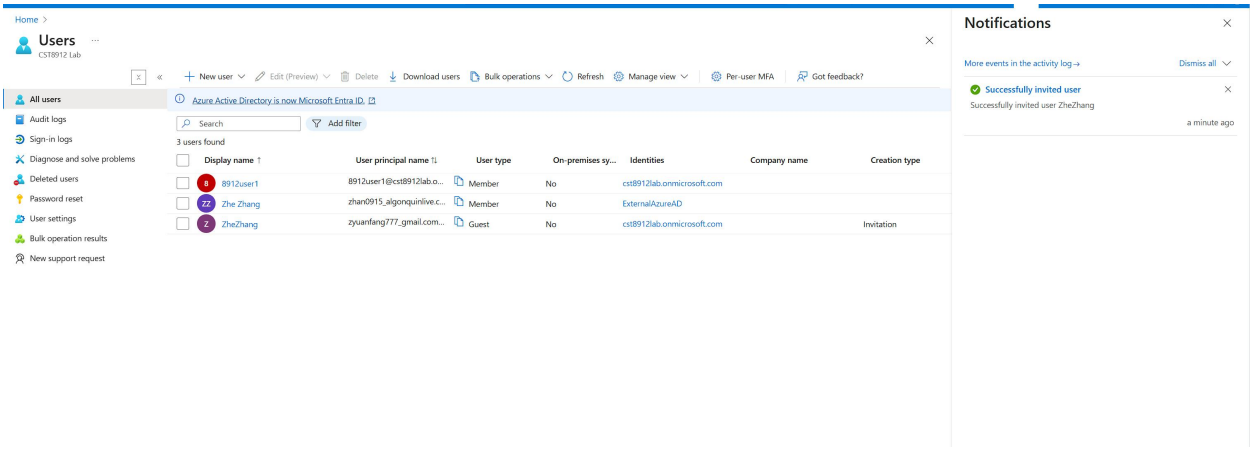
  - **User principal name**: 8912user1
  - **Display name**: 8912user1
  - **Auto-generate password** (checked)
  - **Account enabled** (checked)
  - **Job title**: IT Administrator
  - **Department**: IT
  - **Usage location**: Canada

- Click **Create**.



Step 1.4: Invite an External User

- In **Users**, click **+ New user > Invite an external user**.
- Fill in the following details:
    - **Email**: (Use a valid external email)
    - **Display name**: (Enter name)
    - **Send invite message** (checked)
    - **Message**: Welcome to Azure and our group project
- Click **Review + Invite**, then click **Invite**.



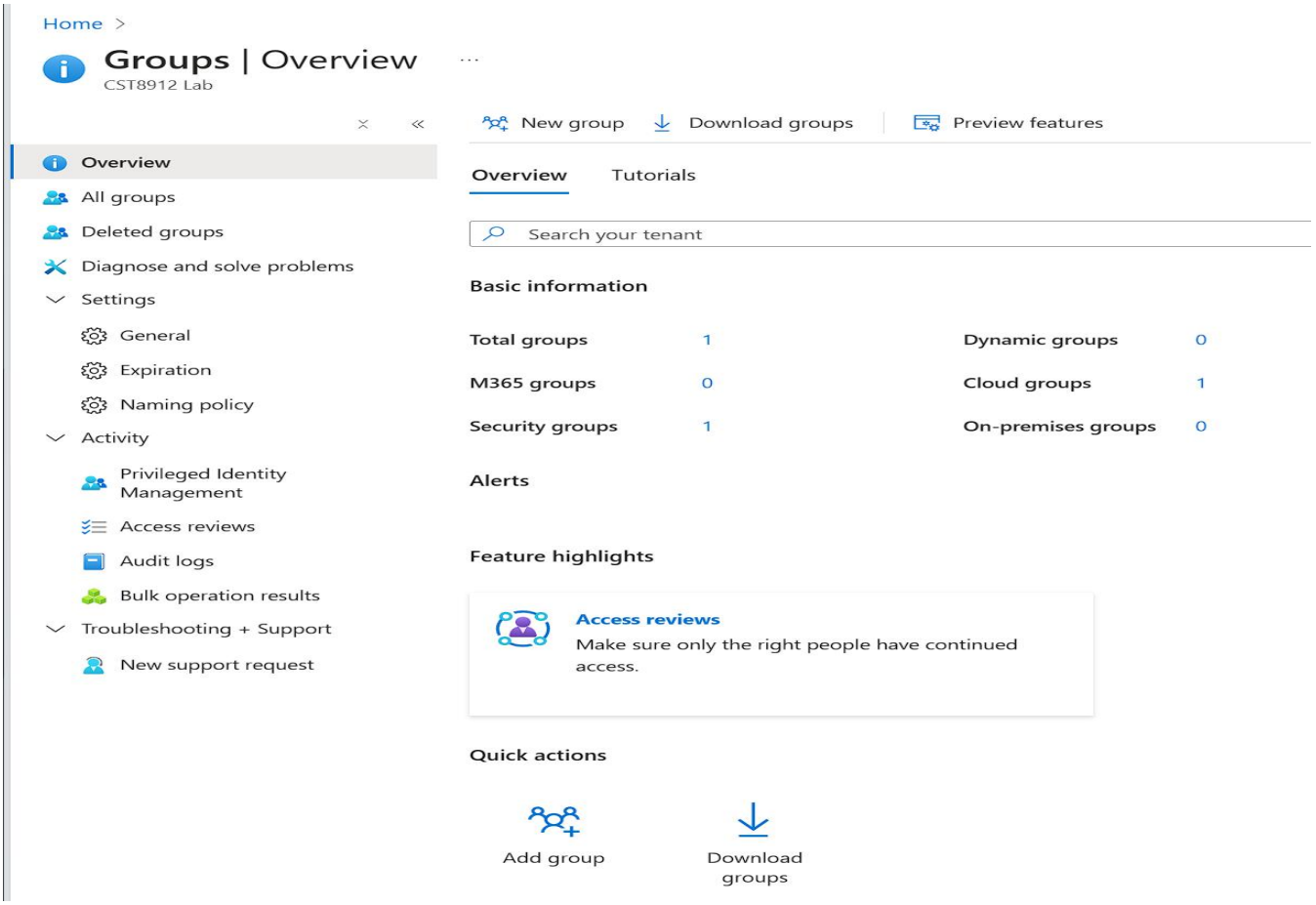
Task 2: Create Groups and Add Members

Step 2.1: Create a Group

- Search for **"Groups"** and navigate to **Groups**.
- Click **+ New group** and enter:
    - **Group type**: Security
    - **Group name**: IT Administrator
    - **Description**: Administrators that manage the IT lab

- **Membership type**: Assigned

- Click **Create**.



Step 2.2: Add an Owner

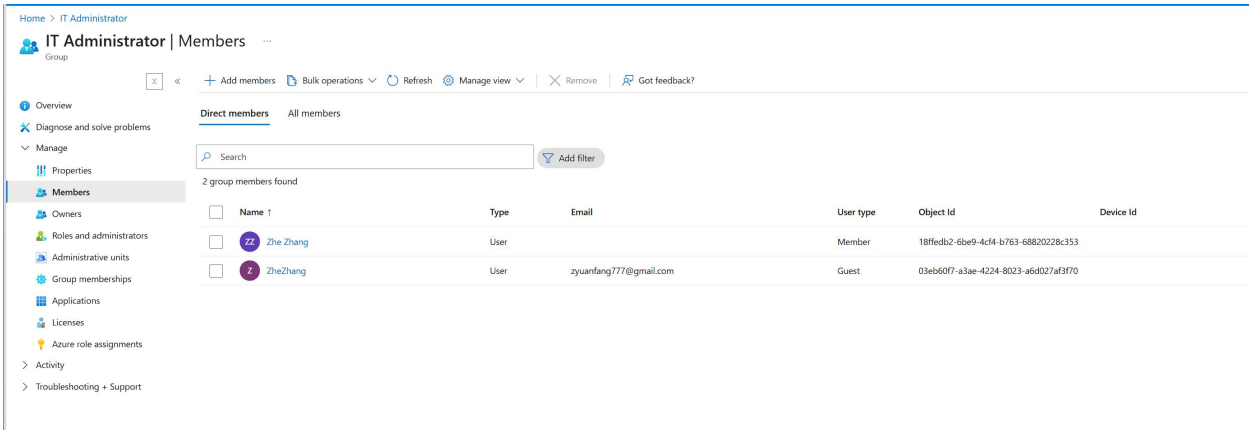
- Open the **IT Administrator** group.
- Click **Owners** > **Add owners**.
- Search for and select **your account**, then click **Select** and **Save**.

Step 2.3: Add Members

- Open the **IT Administrator** group.
- Click **Members** > **Add members**.
- Search for and add:

    - 8912user1
    - The external user invited in **Task 1.4**

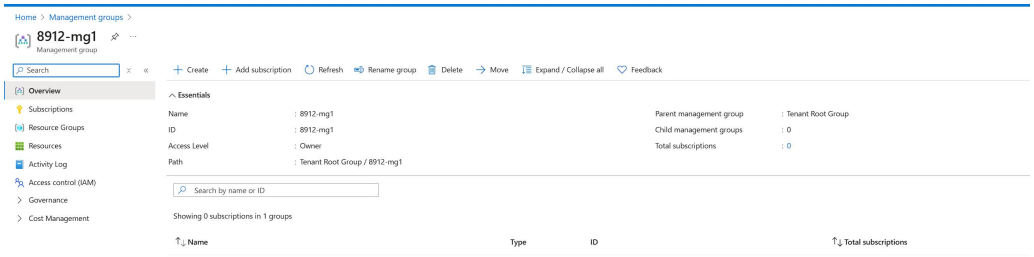
- Click **Save**.



Task 3: Implement Management Groups

Step 3.1: Create a Management Group

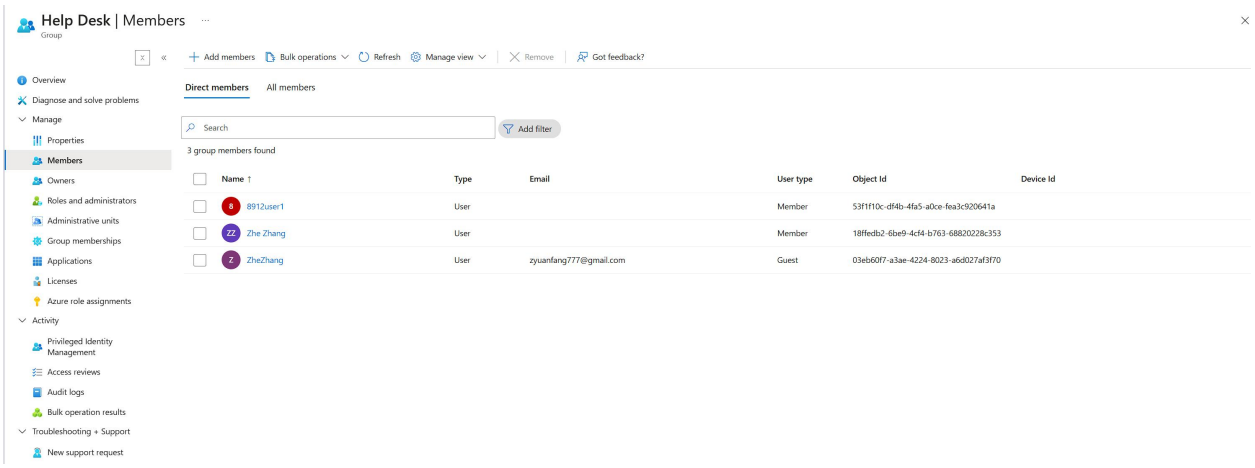
- Search for **"Management Groups"** and click **Management Groups**.
- Click **+ Create**.
- Enter:
    - **Management group ID**: 8912-mg1
    - **Display name**: 8912-mg1
- Click **Submit**



Task 4: Assign a Built-in Azure Role

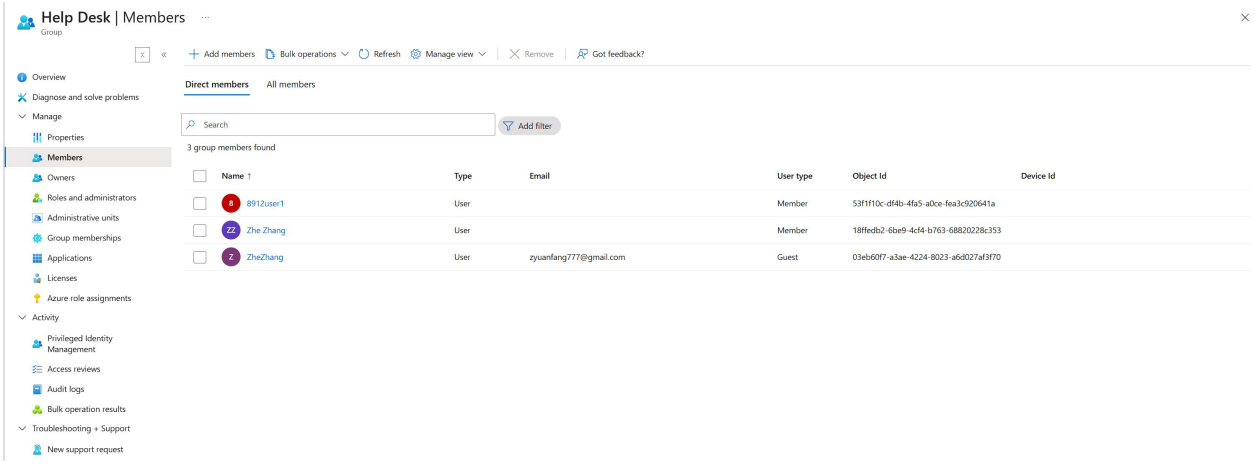
Step 4.1: Assign the "Virtual Machine Contributor" Role

- Go to **Management Groups** and open **"8912-mg1"**.
- Click **Access control (IAM)** > **Roles**.
- Click **+ Add > Add role assignment**.
- Search for **"Virtual Machine Contributor"**, select it, then click **Next**.



Step 4.2: Assign the Role to Help Desk

- Click **+ Select members**.
- Search for and select **Help Desk** (if not created, follow the next steps to create it).
- Click **Review + Assign**.



Task 5: Cleanup of Resources

Step 5.1: Delete Users

- Go to **Azure AD > Users**.
- Delete:
    - 8912user1
    - The external user invited in **Task 1.4**.

Step 5.2: Delete Groups

- Go to **Azure AD > Groups** and delete:
    - IT Administrator
    - Help Desk

Step 5.3: Delete Management Group

- Go to **Management Groups**.
- Select **"8912-mg1"** and delete it.

Step 5.4: Remove Role Assignments

- Navigate to **Management Groups > 8912-mg1 > Access Control (IAM)**.
- Remove the **Virtual Machine Contributor** role from **Help Desk**.

Step 5.5: Delete Tenant (Optional)

- Navigate to **Azure AD > Properties**.
- Click **Delete tenant** if no longer needed.

Results

- Successfully created **Azure AD users** and invited an external user.
- Successfully created **IT Administrator and Help Desk groups** and assigned ownership.
- Successfully created a **Management Group (8912-mg1)**.
- Assigned **Virtual Machine Contributor** to Help Desk.
- **Successfully removed all resources after lab completion**.

References

- Microsoft Azure Documentation: https://learn.microsoft.com/en-us/azure/active-directory/
- Azure Role-Based Access Control (RBAC): https://learn.microsoft.com/en-us/azure/role-based-access-control/