Deploying and Managing an Azure VM with Entra ID Access

Tuesday, September 23, 2025 1:29 AM

Overview

In this project, we deployed a **Linux virtual machine (VM) on Microsoft Azure** and integrated it with **Microsoft Entra ID** (Azure AD) for identity-based access management. The goal was to:

- Create and configure an Azure VM.
- Set up Microsoft Entra ID users.
- Assign appropriate roles to grant access to the VM resource

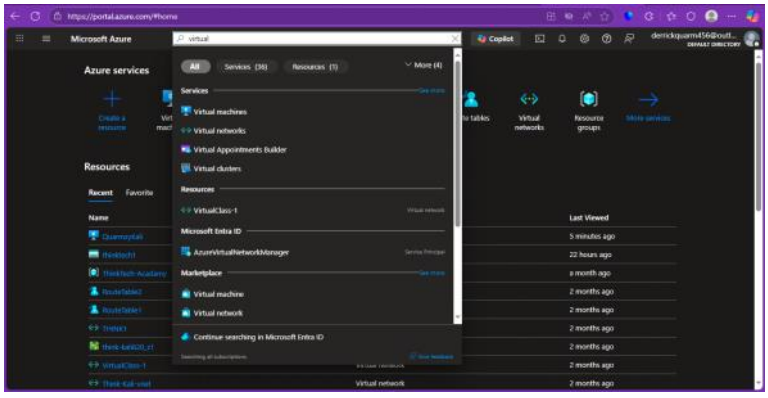
Step-by-Step Guide: How to View Your Virtual Machines in Azure

Step 1: Sign in to the Azure Portal

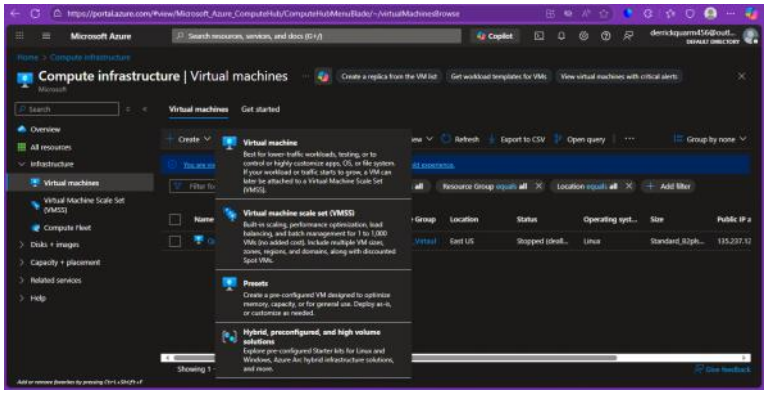
- Go to the Microsoft Azure portal and sign in with your account.

Searching for Virtual Resources:

1. Using the global search bar, searched for **"virtual Machines"** to quickly access:

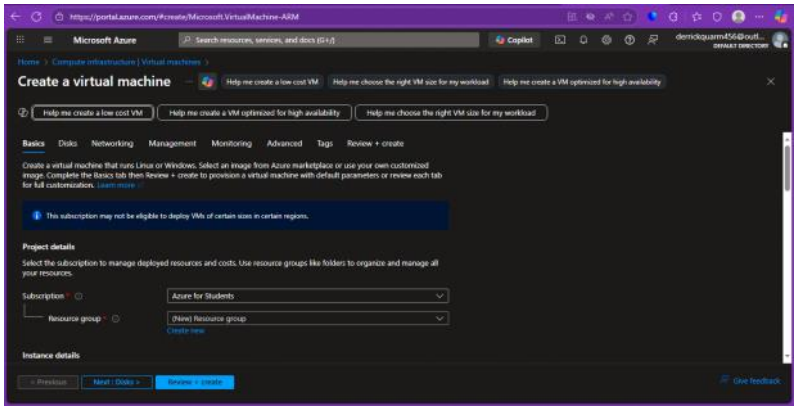


1. Create a "New Virtual Machine"



- Subscription: Select the Azure subscription that will be billed for this VM.

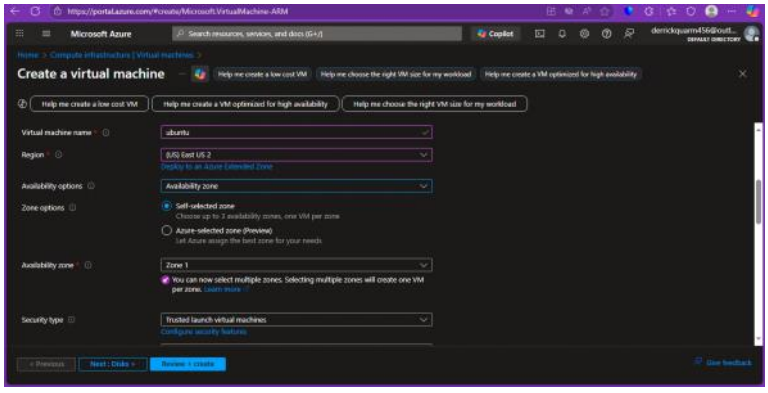
- Resource Group: Select an existing resource group or create a new one to logically contain your VM and its related resources

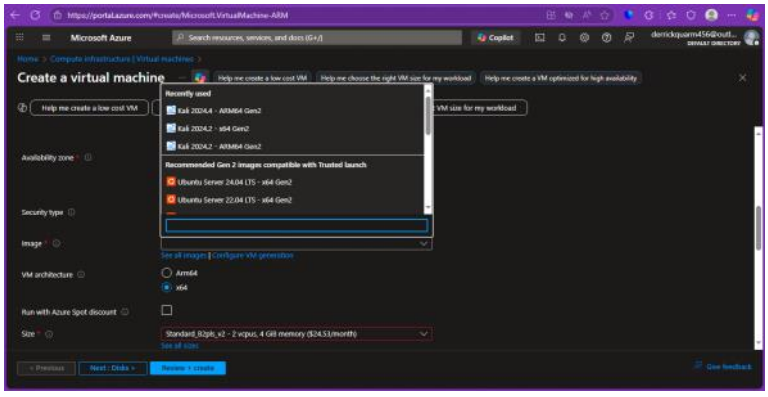


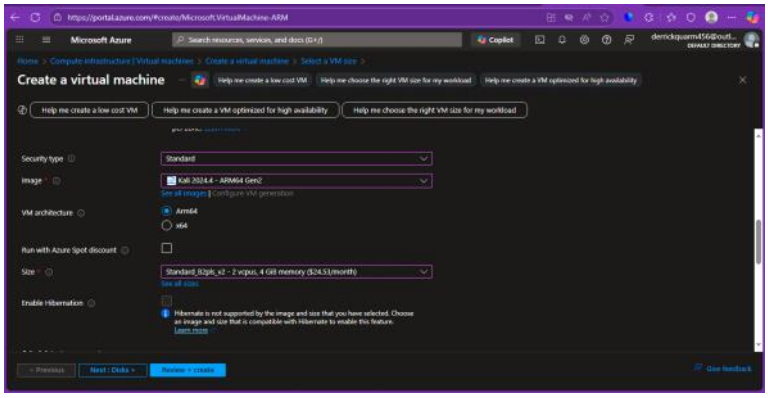
Instance Details:

- Virtual machine name: Enter a unique name for your VM.
- Region: Choose the Azure data center region where you want your VM to reside (e.g., (US) East US 2).
- Availability Options: This is for high availability. Your screenshot shows "Availability zone" options.
- Availability zone: You can choose to deploy your VM to a specific zone (1, 2, or 3) within the region for isolation from failures in other zones. You can also select the "Azure-selected zone" option.
- Image: Select the operating system. You have selected an Ubuntu Server image (e.g., 24.04 LTS). This is a good choice for a Linux-based VM.
- Security Type: You have the option for a Trusted launch virtual machine, which provides advanced security features. It's recommended and compatible with the Gen2 VM images you are viewing.

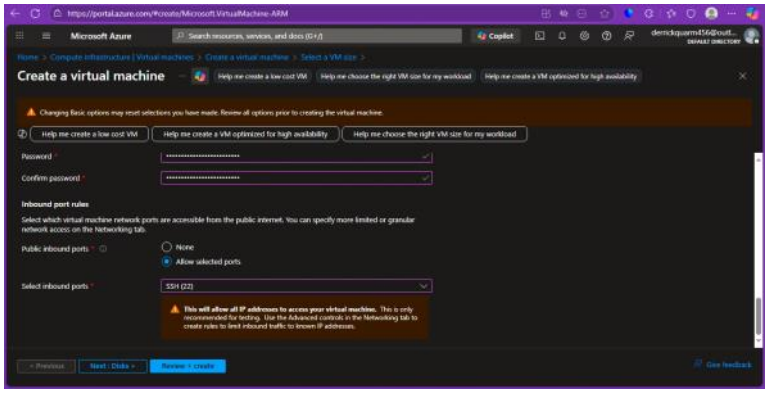
- VM Architecture: Choose between x64 (standard Intel/AMD) or Arm64. You have x64 selected, which is the most common.
- Size: This determines the VM's power (CPU, RAM). You have selected Standard_B2ps_v2 (2 vCPUs, 4 GB memory). This is a cost-effective, burstable size suitable for dev/test workloads.







- Authentication:
- For a Linux VM, you will typically use an SSH public key. You can generate a new key pair or use an existing one.
- Alternatively, you can use password authentication, but SSH keys are more secure.



Disks Tab - Configure Storage

- Click the Next: Disks > button to proceed.
- OS disk type: Choose between HDD Standard, SSD Standard, or SSD Premium. SSD Premium offers the best performance.
- You can also attach additional data disks here if your application needs separate storage.

- **Step 3: Networking Tab - Configure Network Connectivity**

- Click the Next: Networking > button.
- Azure will create a virtual network and subnet for you, or you can select an existing one.

- A public IP address will be created by default, allowing you to connect to the VM over the internet (e.g., via SSH). For security, you can change this to "None" if you only need private network access.

- **Step 4: Management, Monitoring, and Advanced Tabs (Optional)**

- You can quickly proceed through these tabs using the default settings for your first VM. They cover areas like:

- Auto-shutdown schedule to save costs.

- Backup and monitoring options.

- Custom data scripts to configure the VM on startup.

- **Step 5: Review + Create**

- Click the Review + create button.

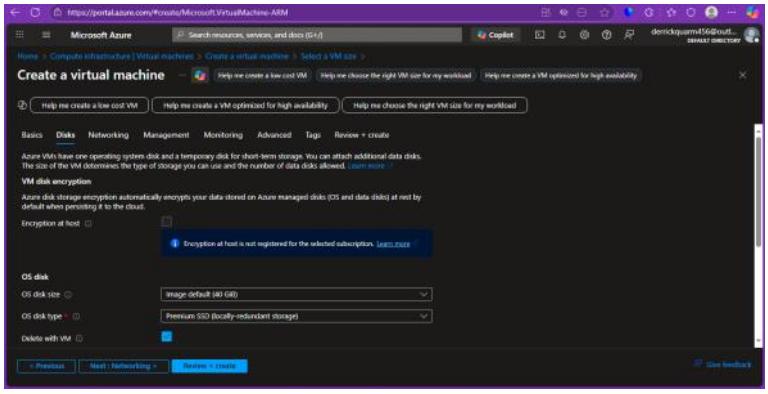
- Azure will validate your configuration. If there are errors, it will tell you which tab to go back to and fix.

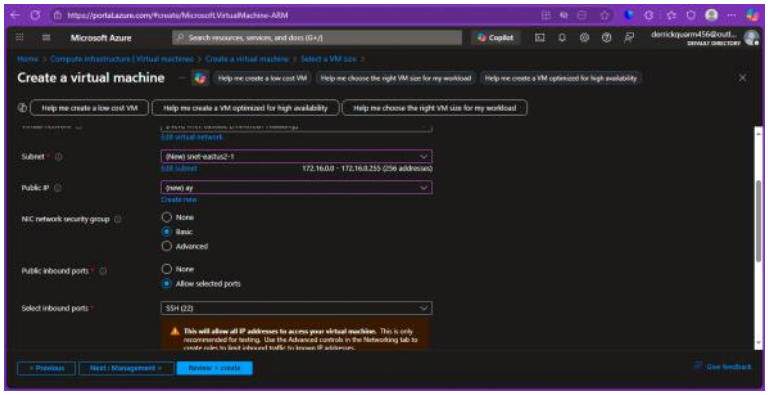
- If validation passes, you will see a summary of your configuration and the estimated monthly cost.

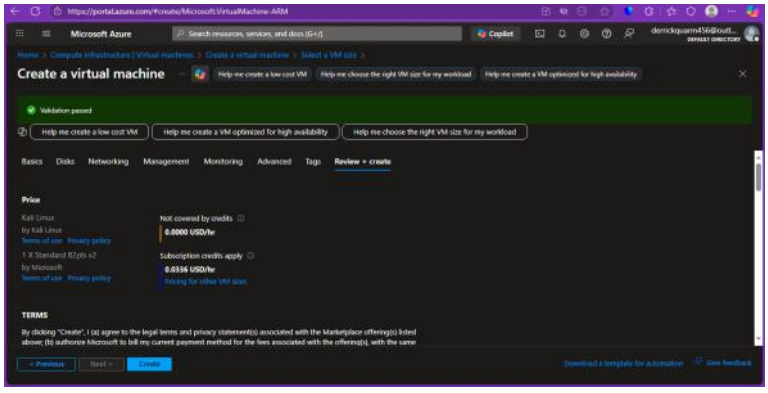
- **Step 6: Create the VM**

- Finally, click the Create button.

- Deployment will begin. This process can take a few minutes. You can monitor the progress from the Azure portal's notifications.







Connect to Your Virtual Machine

Connect via SSH (for Linux/macOS or Windows)

Since you deployed a Linux VM (Kali Linux is a Linux distribution), you connect using the SSH protocol.

Using Command Line (macOS, Linux, or Windows Command Prompt/PowerShell)

Open a Terminal:

On macOS or Linux: Open the "Terminal" application.

On Windows 10/11: Open "Command Prompt" or "PowerShell".

Run the SSH Command:

Step-by-Step: How You Connected via PuTTY

Step 1: Open PuTTY
You searched for "PuTTY" in Windows and opened the PuTTY application

Step 2: Configure PuTTY Session
In the PuTTY Configuration window:

Host Name (or IP address): 20.96.185.143

Port: 22 (default for SSH)

Connection type: SSH (selected)

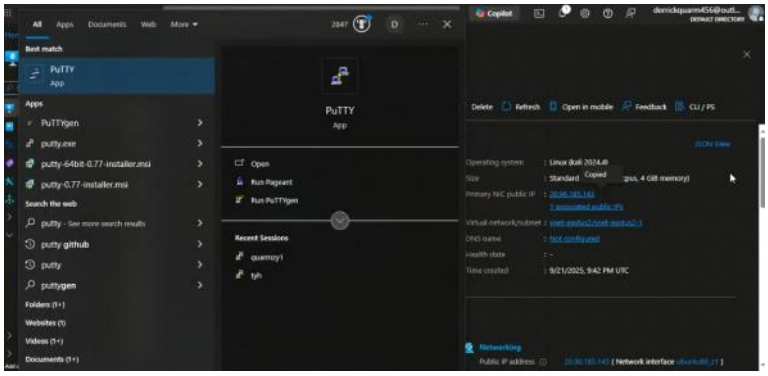
Step 4: Connect

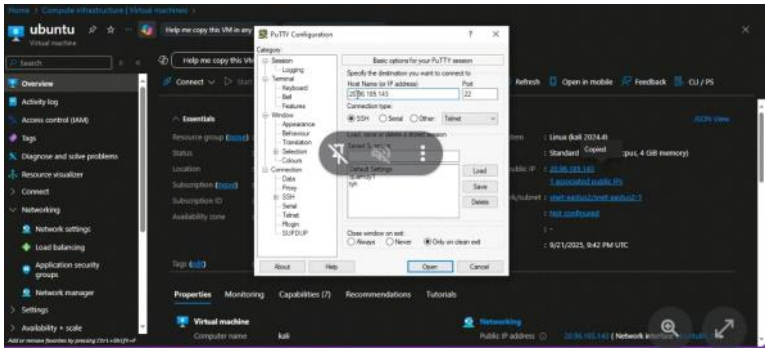
1. Click **Open** (bottom of the window).
2. You'll see a **security alert** (first time connecting) → Click **Yes** to trust the host key.

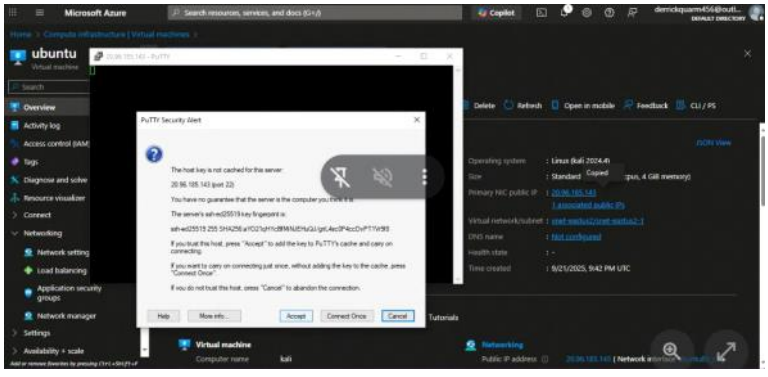
Step 5: Login

- A terminal window appears asking:

  login as:
- Enter your **username** and password

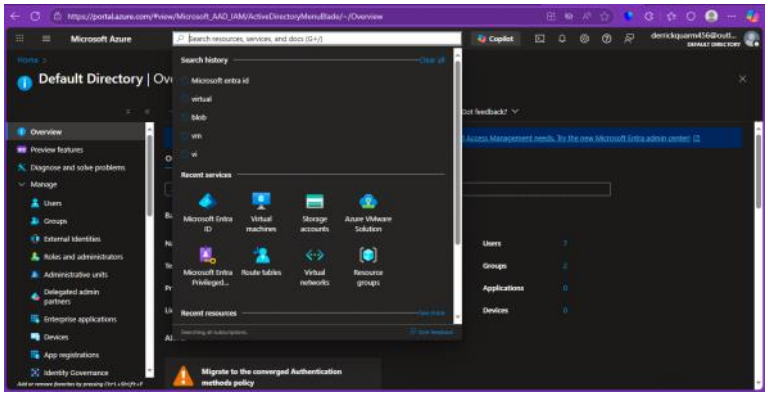


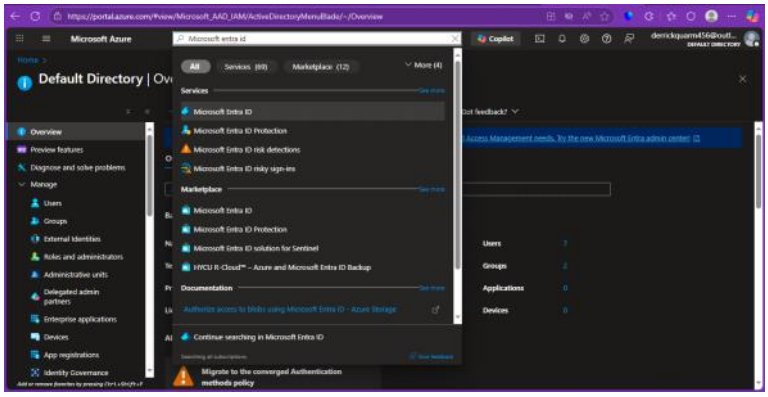




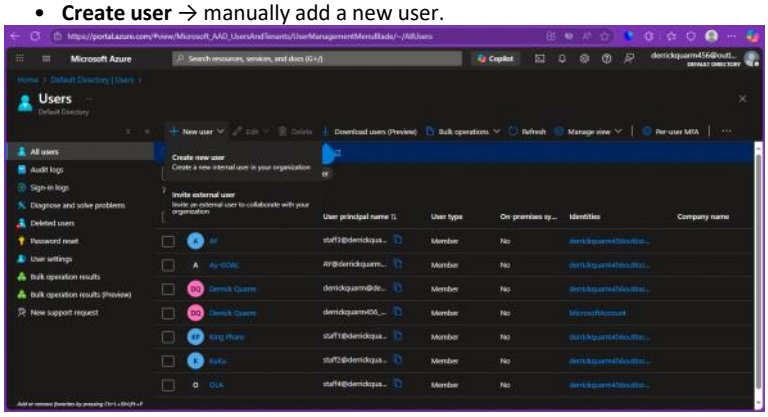
Setting up Microsoft Entra ID users

- **Sign in** to Azure Portal.
- In the global search menu, type **Microsoft Entra ID** and click on it.

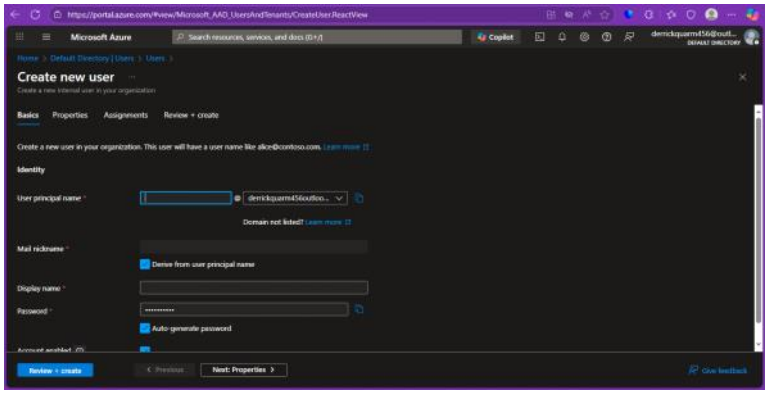


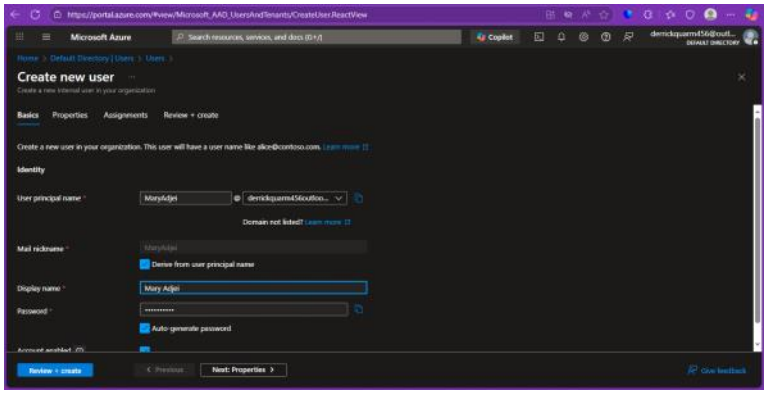


- Click **Users → All users → + New user**.
- Choose either:
  - **Create user** → manually add a new user.



- Fill in details:
  - Name
  - Username (username@yourdomain.onmicrosoft.com E.g. (maryadjei@derrickquarm456outlook.onmicrosoft.com)
  - Profile info (job title, department, etc.)
- Set **password** (initial password can be auto-generated).





Step 2: Click "Next: Properties"
After filling the basic information, click the Next: Properties button at the bottom.

Step 3: Properties Tab (Optional)
Fill in additional user information:

- Job title
- Department
- Office location .etc

Click "Next: "Assignments"

Step 4: Assignments Tab (Important)
Assign roles: Give the user appropriate permissions (**I left my on default**)

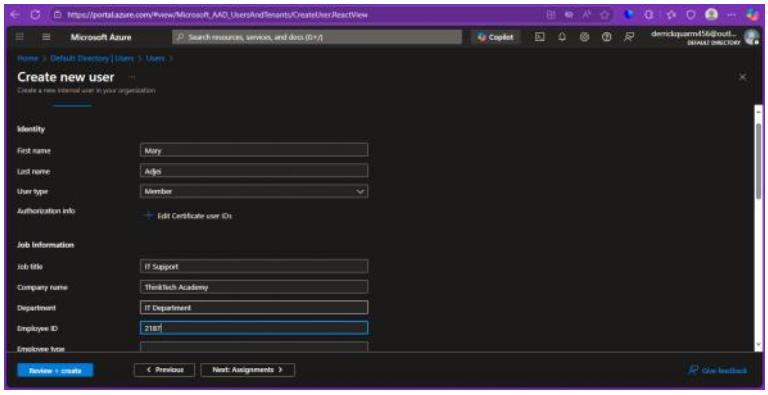
Common roles:

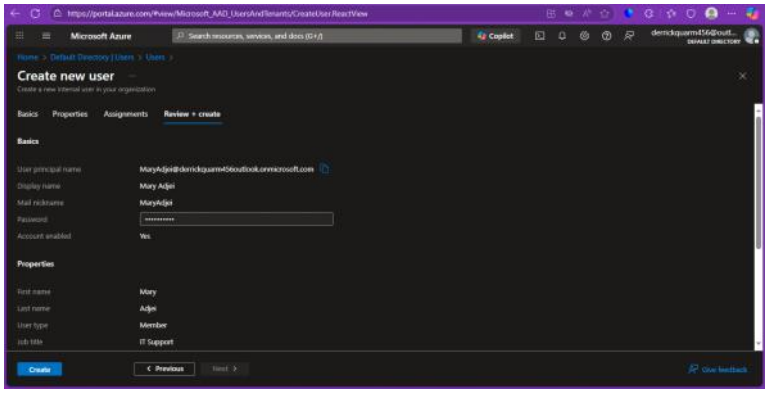
User - Basic access (default)

Global administrator - Full access (use carefully)

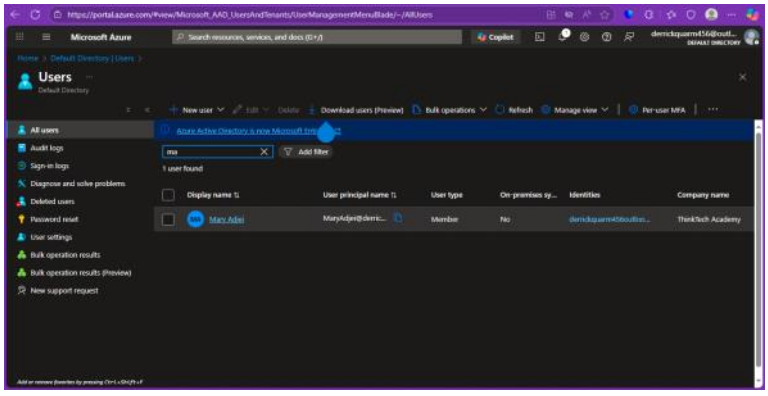
Other admin roles based on needs

Click "Next: Review + create





Step : Click Refresh to view the User account created



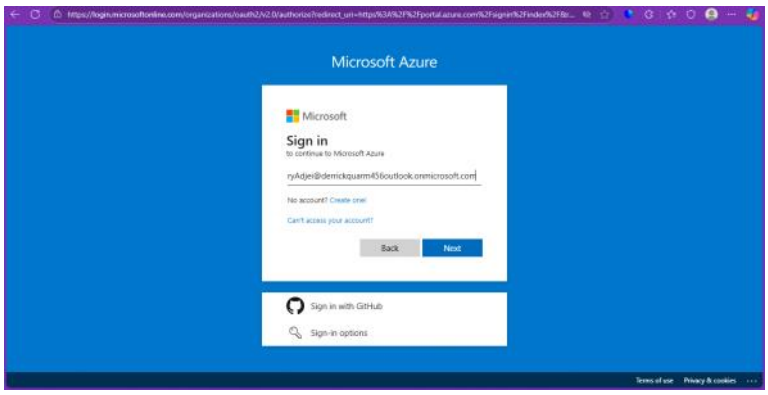
Step-by-Step: Login as the New User

- Go to Azure Portal
- Go to portal.azure.com

  You'll see the Microsoft login screen

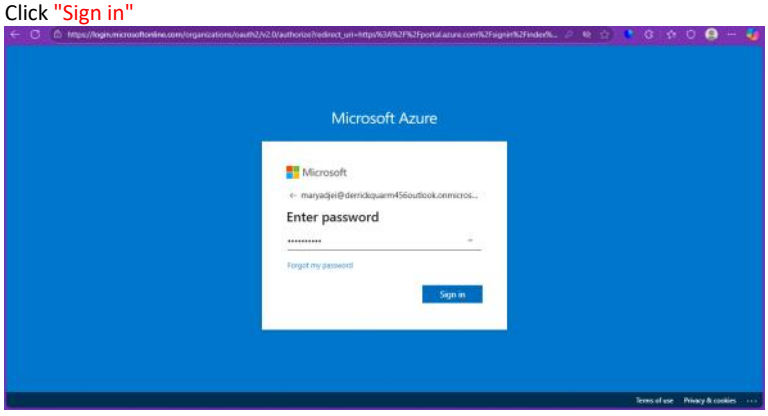
- Enter Username
  Username: E.g. (maryadjei@derrickquarm456outlook.onmicrosoft.com)

  Click "Next"



- Enter "Password"
  Password: Enter the auto-generated password that Azure provided when you created the user

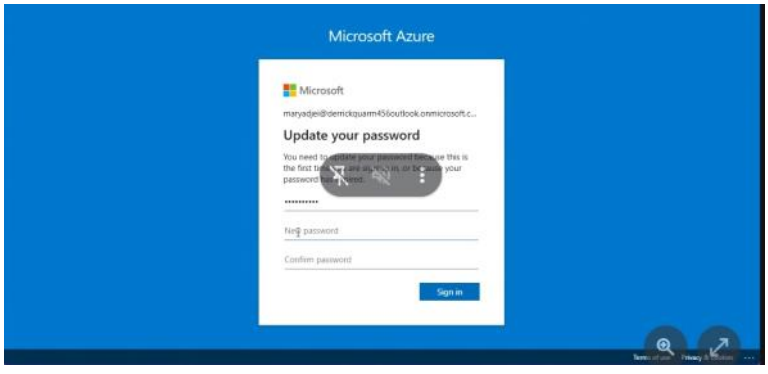
  Click "Sign in"



- Password Change Required (First Login)
  Since this is the first login, you'll likely be prompted to:

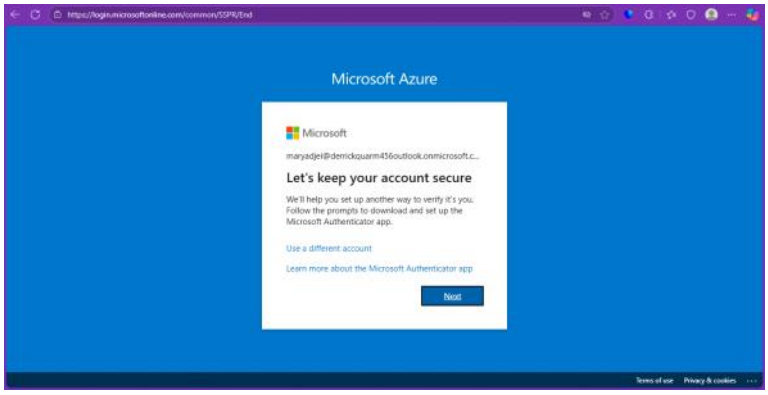
- Change your password - create a new secure password

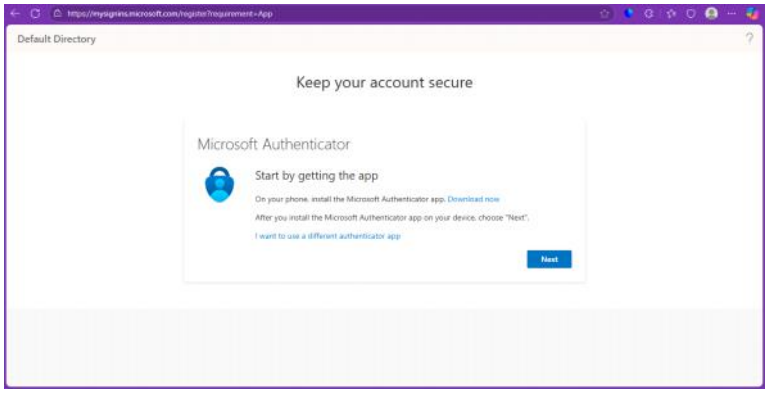
- Confirm new password - enter it again

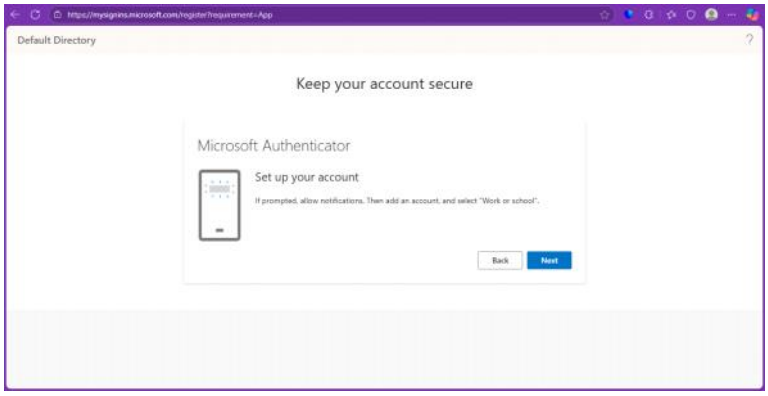


- Set Up Multi-Factor Authentication (MFA)
- Click "Next" on the "Let's keep your account secure" screen
- Download Microsoft Authenticator app on your phone:

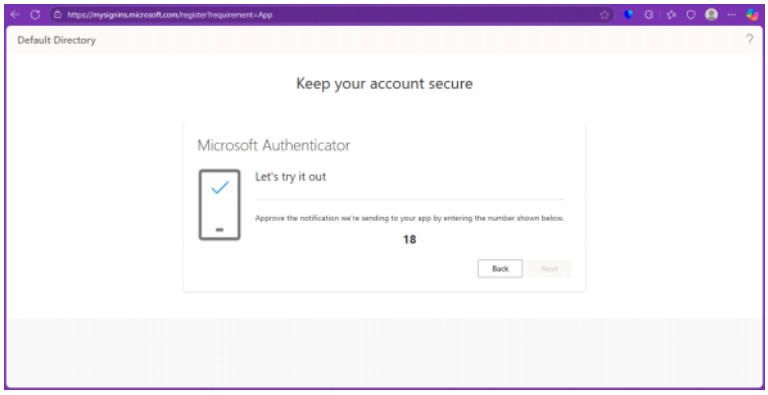
  Available on iOS App Store or Google Play Store

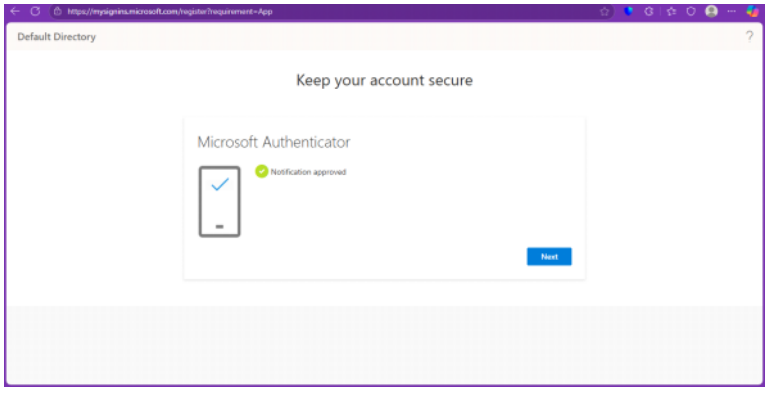

Microsoft Azure
Microsoft
Let's keep your account secure
We'll help you set up another way to verify it's you. Follow the prompts to download and set up the Microsoft Authenticator app.
Use a different account
Learn more about the Microsoft Authenticator app
Next
Terms of use
Privacy & cookies

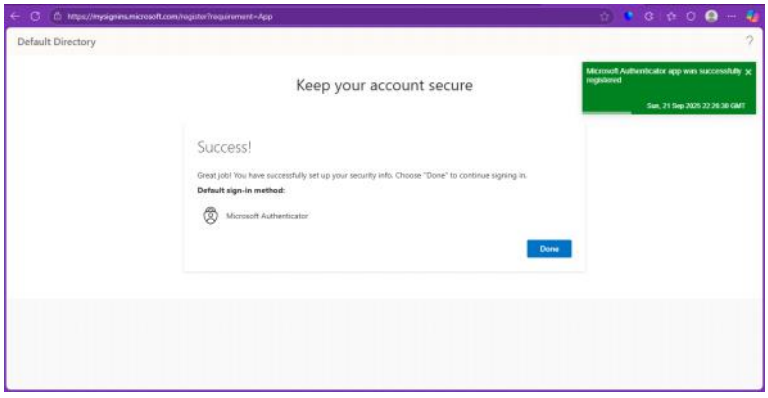

Default Directory
Keep your account secure
Microsoft Authenticator
Start by getting the app
On your phone, install the Microsoft Authenticator app. Download now
After you install the Microsoft Authenticator app on your device, choose "Next".
I want to use a different authenticator app
Next


Default Directory
Keep your account secure
Microsoft Authenticator
Set up your account
If prompted, allow notifications. Then add an account, and select "Work or school".
Back
Next


Default Directory
Keep your account secure
Microsoft Authenticator
Scan the QR code
Use the Microsoft Authenticator app to scan the QR code. This will connect the Microsoft Authenticator app with your account.
After you scan the QR code, choose "Next".
Can't scan image?
Back







Completed MFA Setup

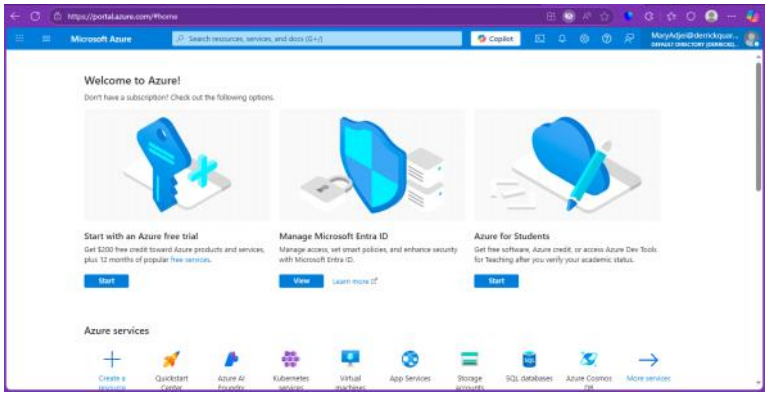
You successfully set up Microsoft Authenticator as your verification method

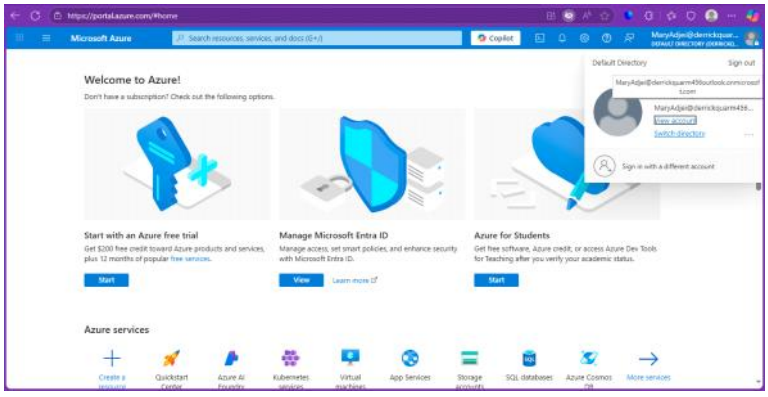
Saw the "Success!" message confirming security info setup

Step 2: Logged into Azure Portal

You're now in the Azure portal as maryadjei@derrickquarm456outlook.onmicrosoft.com

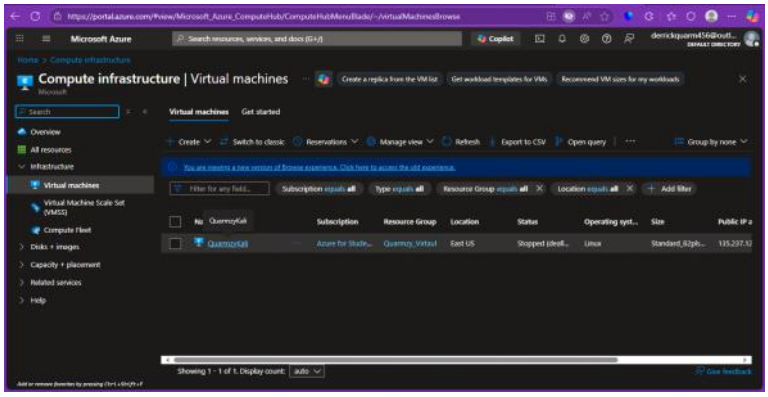
You see the "Welcome to Azure!" dashboard



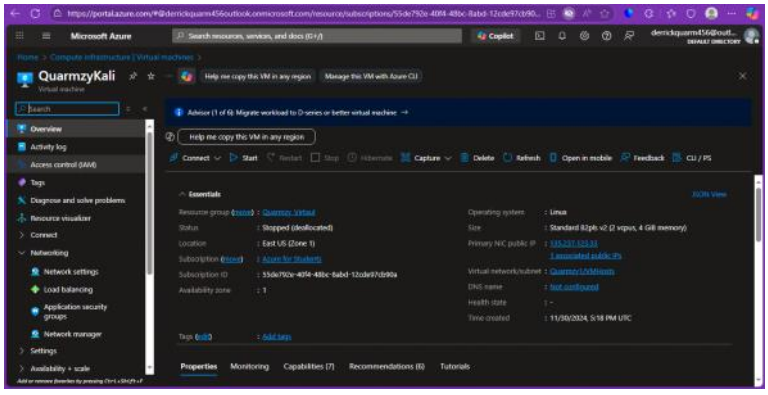


Step-by-Step: Assign VM Access to the New User

1. Search for the VM you want to assign access to the New user and click on it
   In my case my VM is "QuarmzyKali"

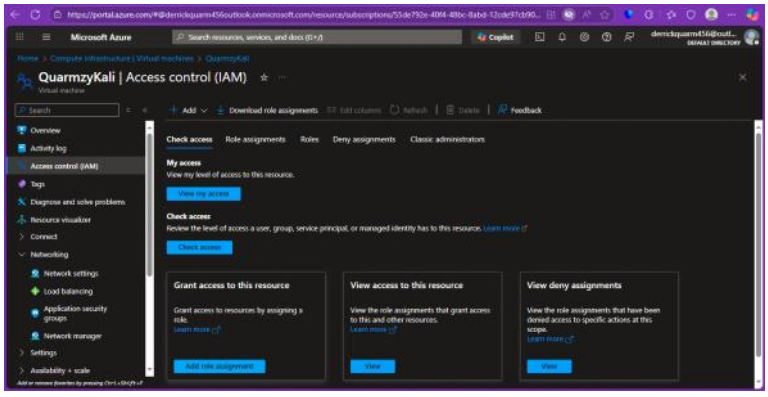


2. From the left-side panel select "Access control"(IAM)

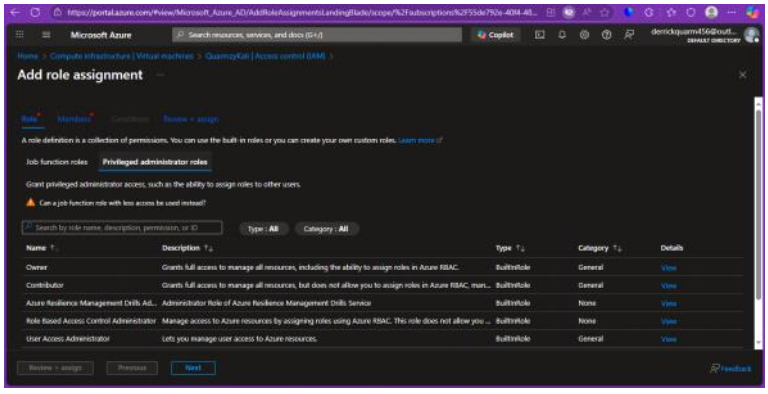


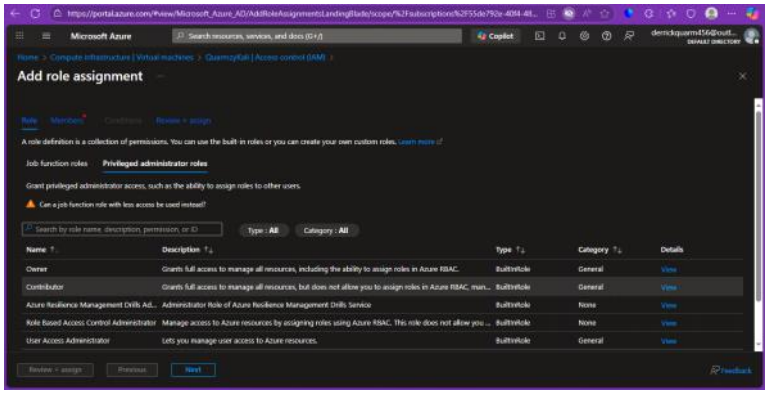
You're on the "Add role assignment" page for your VM "QuarmayKali"

3. Select the "Add Role Assignment"



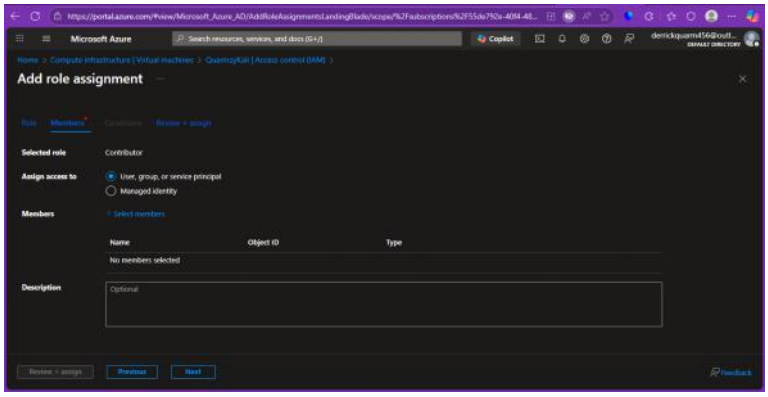
4. Choose the appropriate Role . In my case I choose "Contributor" role



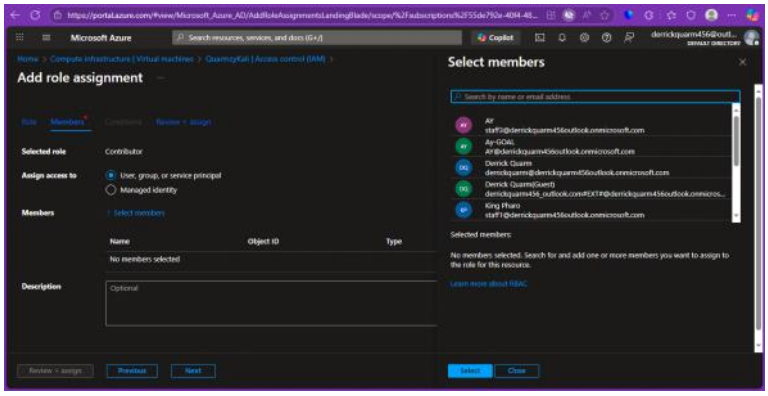


- Click "Next" at the bottom

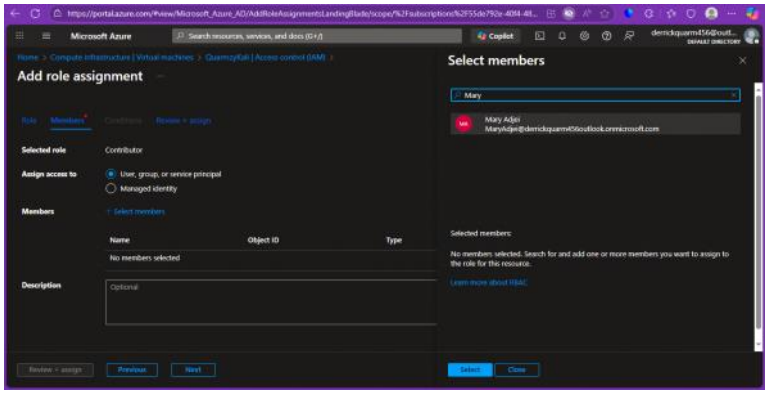
"Next"



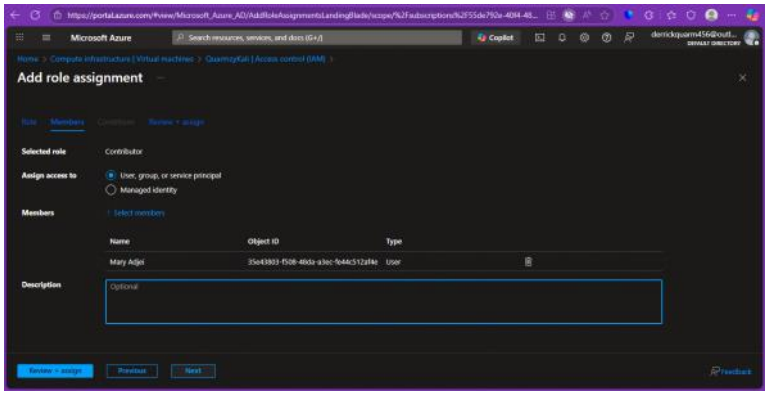
5. Select Member
Click "+ Select members"

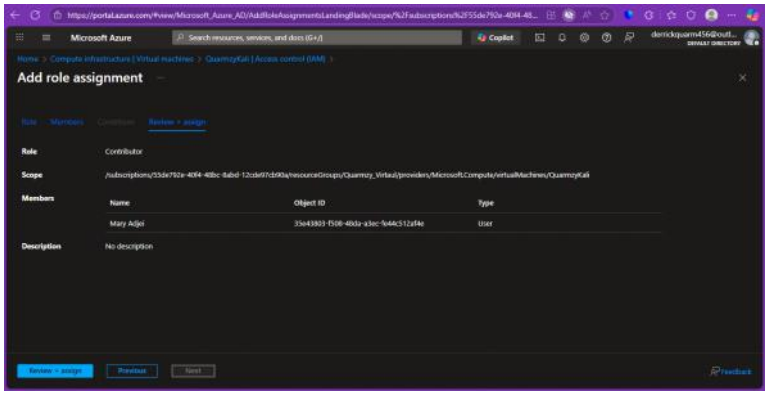


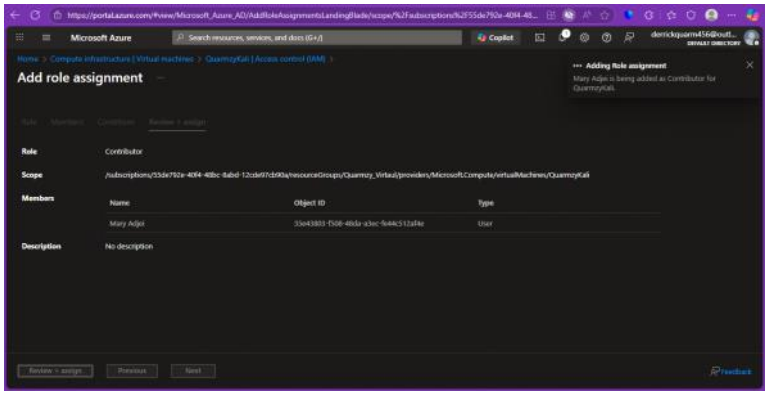
- Click "Select"



- Review and Assign
- Click "Review + assign"







Important Note About "Contributor" Role:

You've selected Contributor role, which gives Mary full control over the VM, including:

✅ Start, stop, restart the VM

✅ Connect via SSH

✅ Modify VM settings

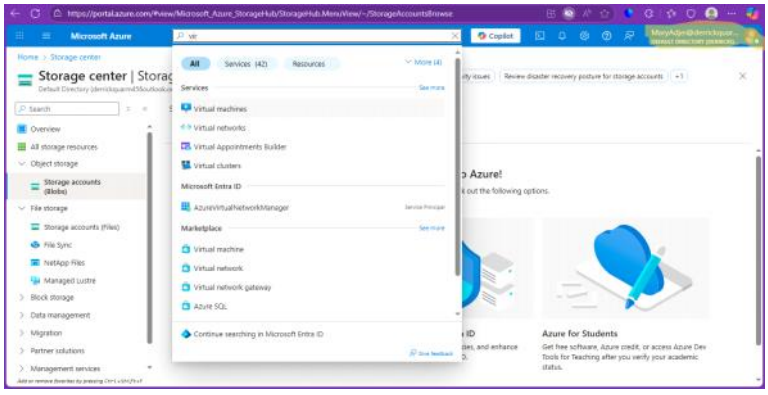
✅ Resize the VM

✅ Delete the VM

❌ Cannot assign roles to others

If you prefer more restricted access, you could choose:

Virtual Machine User Login - Can only connect to VM



The image above shows we are search Virtual Machine in "maryadjei" account