****

**PLACEMENT EMPOWERMENT PROGRAM**

**Cloud Computing & DevOps Centre**

**Setting up IAM roles and permissions in cloud:** Create an IAM role on your cloud platform. Assign the role to your VM to restrict/allow access.

**Name:** Pranav Karunakaran

**Dept:** IT

**NOTE:**

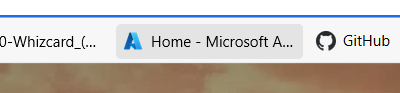
* **Azure** doesn't directly use the terminology "IAM Roles" like AWS does; instead, it uses **Azure Roles** with **Role-Based Access Control (RBAC)**. Below are steps to set up a role in Azure and assign it to a Virtual Machine (VM) to manage access.

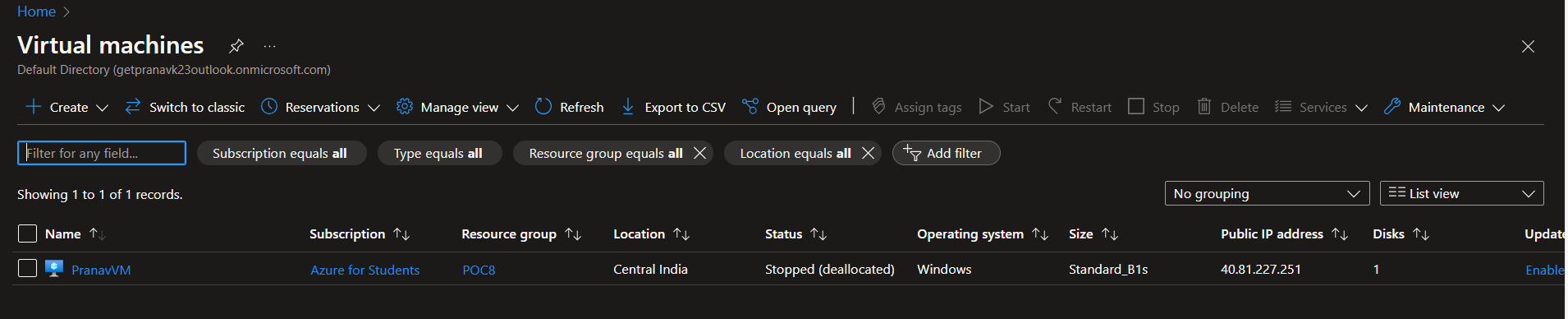
**Step-by-step process:**

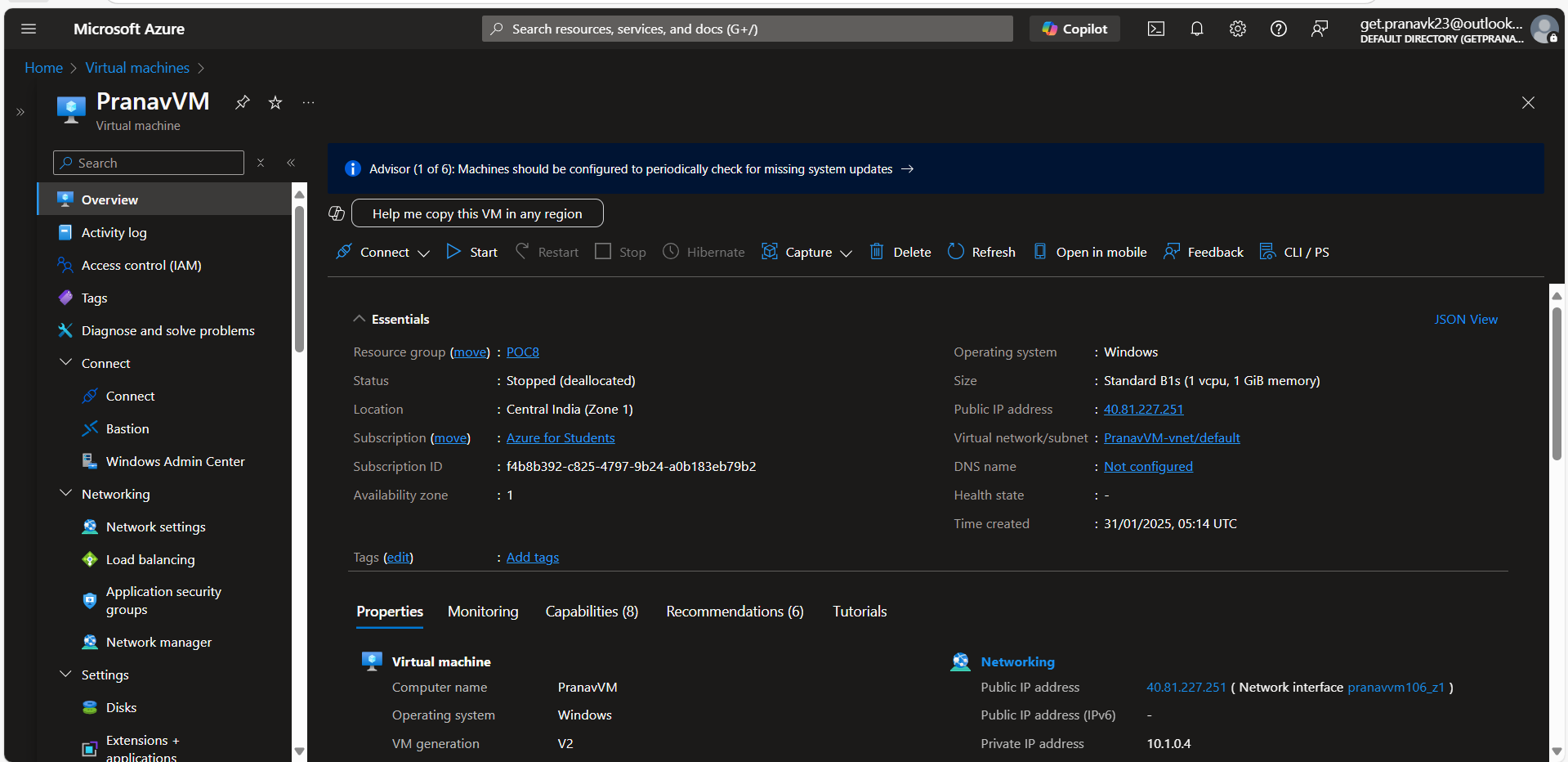
**Step 1**: Creating a custom role. This is optional if you want to create it you can.

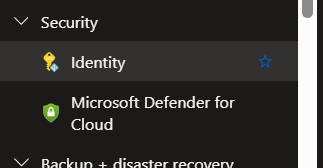
* Assign Role to a Virtual Machine Identity

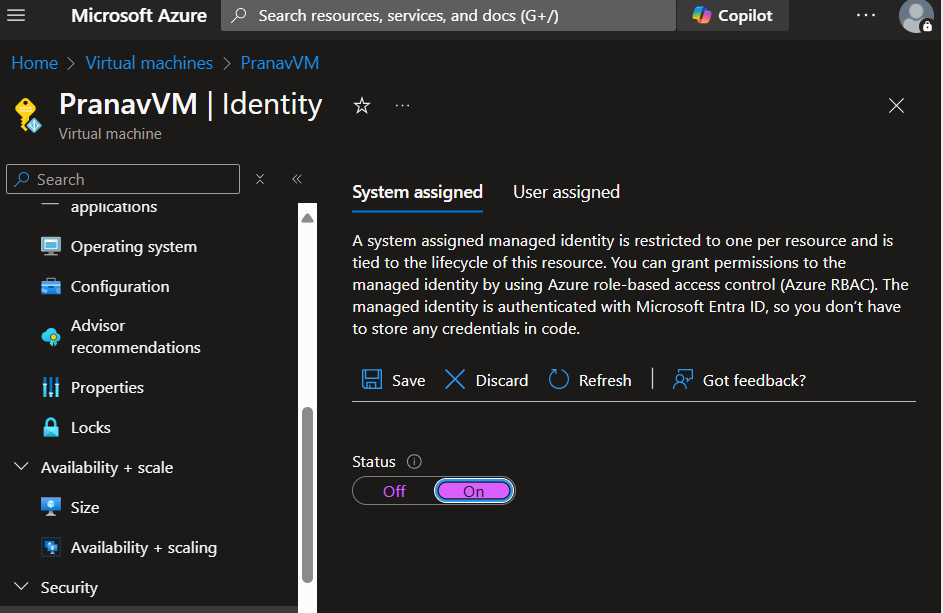
**Step 2:** Go to the **Azure Portal**.



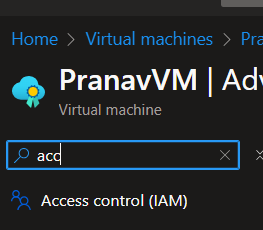
**Step 3:** Navigate to **Virtual Machines > Your VM > Identity**. 

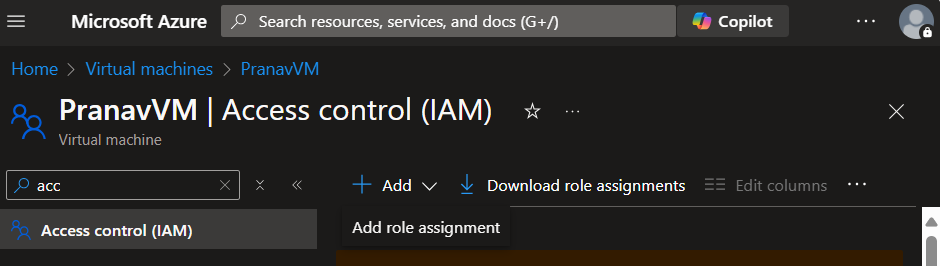


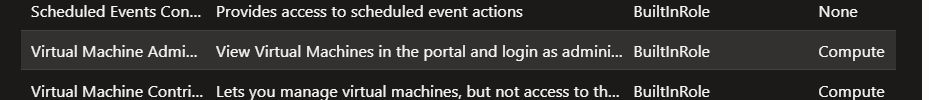


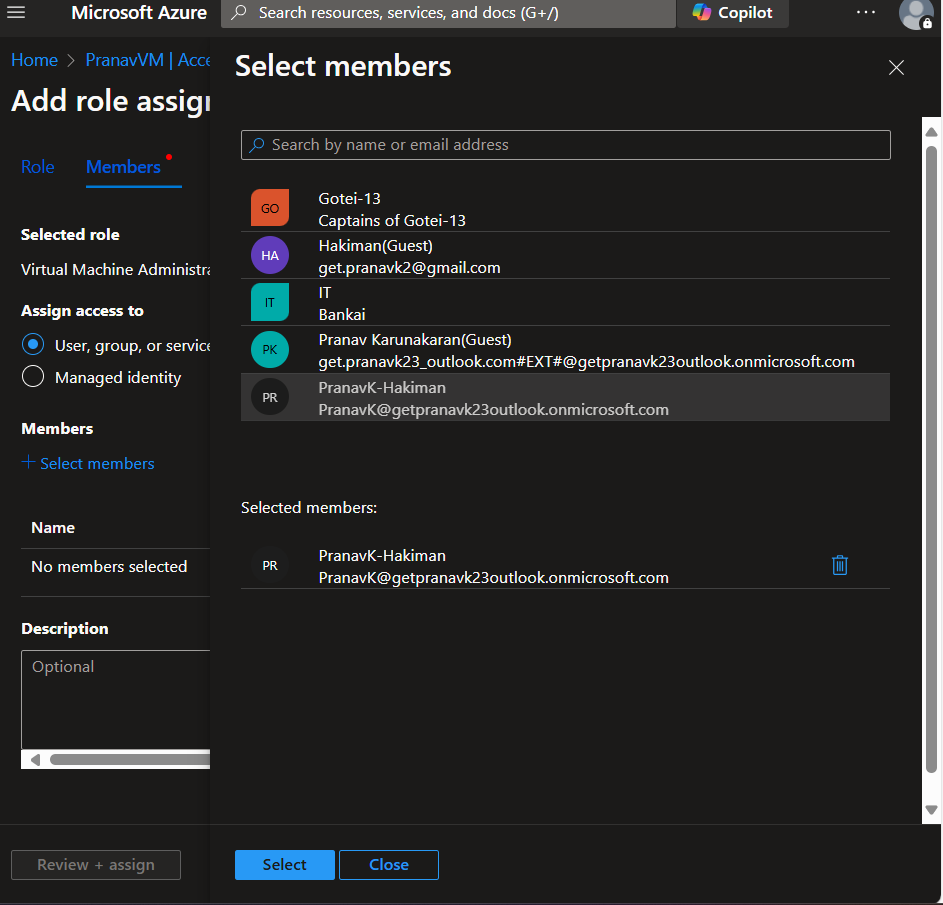
**Step 4:** Enable System-assigned managed identity. 

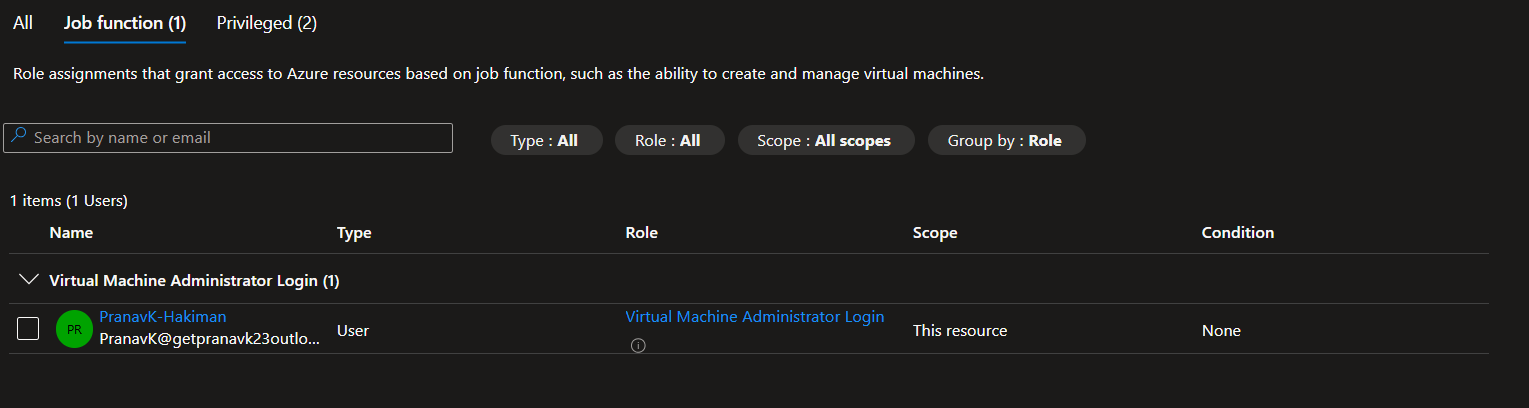
* **Assign Role via the Portal:**

**Step 5:** Go to Access Control (IAM) on the VM you created. 

Step 6: Click **Add > Add role assignment**. 

**Step 7:** Choose the role [VM Administrator].

**Step 8:** Select Members > Managed Identity, search for your VM, and assign the role. 

**Step 9:** Once done go to Role Assignments and check whther role has been assigned or not. 

**🡪The other way to assign roles to your VM is VIA Azure CLI**

az role assignment create \

--assignee $(az vm show --name myVM --resource-group myResourceGroup --query identity.principalId -o tsv) \

--role "Reader" \

--scope "/subscriptions/{subscription-id}/resourceGroups/{resource-group-name}/providers/Microsoft.Compute/virtualMachines/{vm-name}"