KENNEDY MBUGUA

[KENKIN1672@GMAIL.COM](mailto:KENKIN1672@GMAIL.COM)

TECHCRUSH

CLOUD COMPUTING TRACK

YEAR 2025

CAPSTONE PROJECT

IAM Roles and Secure Access Automation

Project 3: IAM Roles and Secure Access Automation (GROUP 4) FOR GROUP 4 ONLY

Objective:

Automate the setup of secure identity and access controls using Azure CLI and Bash scripting.

Tasks:

1. Create a resource group, virtual network, and two subnets (Web and DB).

2. Create Azure AD groups: 'WebAdmins' and 'DBAdmins'.

3. Assign Reader role to DBAdmins for DB subnet resources.

4. Add test users to the AD groups and validate role assignments.

BONUS: Include scripts to revoke access or remove roles for cleanup, also using a CI/CD pipeline to automate the whole process

DELIVERABLES: Script(s) used for deployment and management of IAM roles, screenshot of the entire deployment.

Tasks:

1. Create a resource group, virtual network, and two subnets (Web and DB).

LOCATION="eastus"

RG\_NAME="IAMResourceGroup"

VNET\_NAME="IAMVNet"

SUBNET\_WEB="WebSubnet"

SUBNET\_DB="DBSubnet"

SUBNET\_PREFIX\_WEB="10.0.1.0/24"

SUBNET\_PREFIX\_DB="10.0.2.0/24"

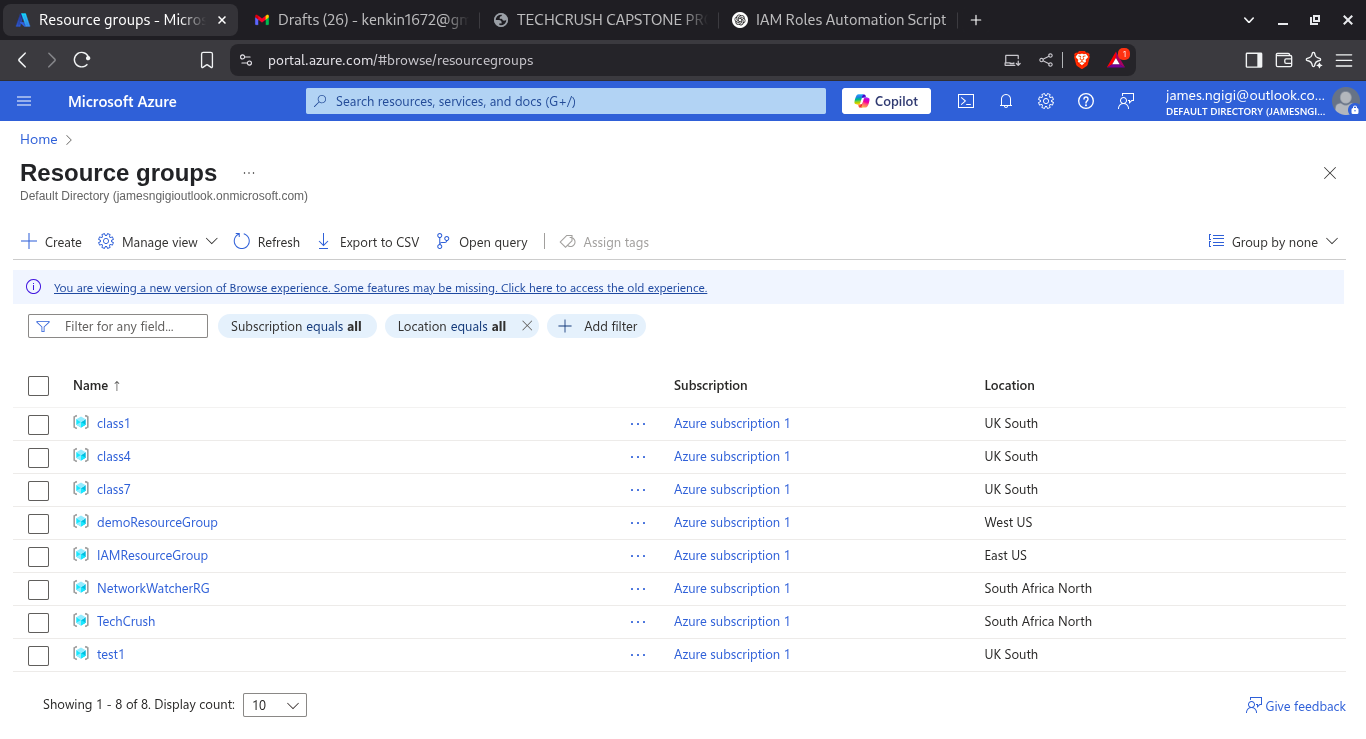
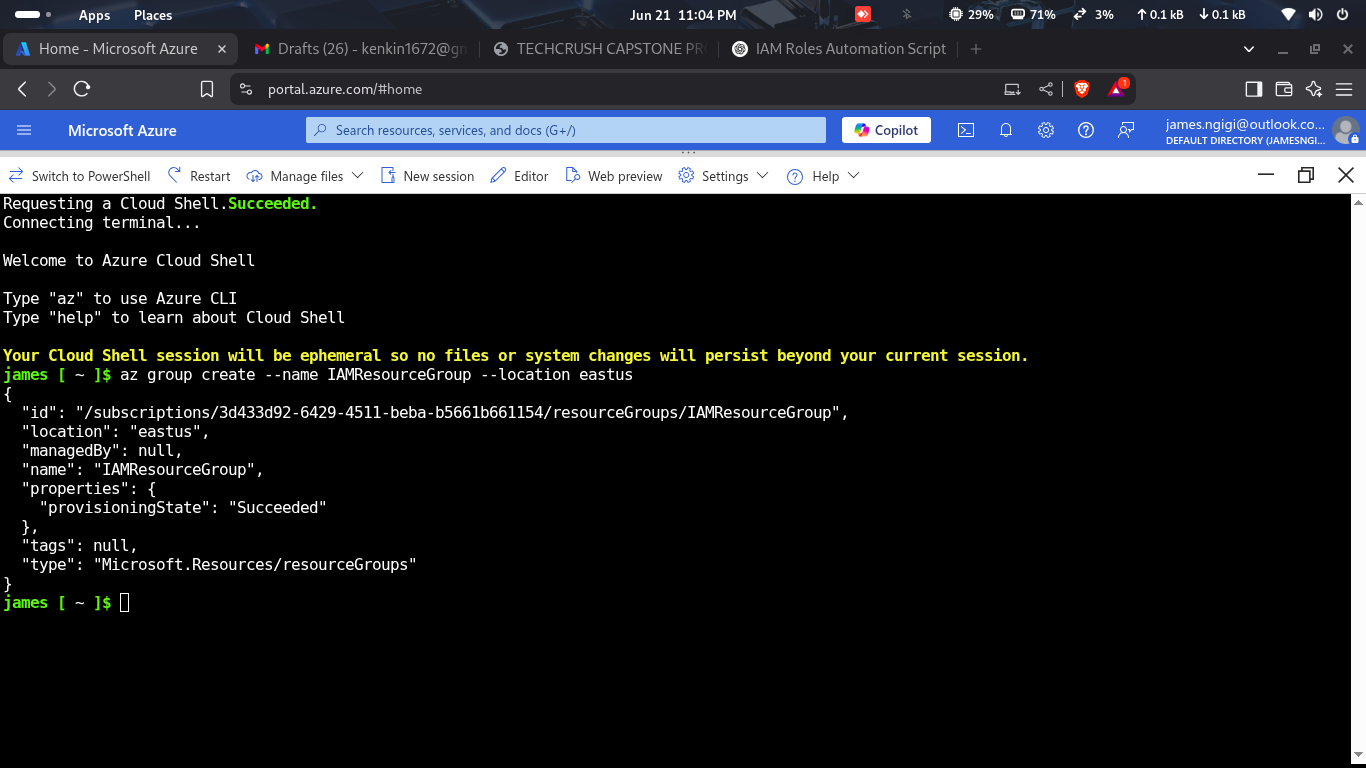
VNET\_PREFIX="10.0.0.0/16"

WEB\_ADMINS="WebAdmins"

DB\_ADMINS="DBAdmins"

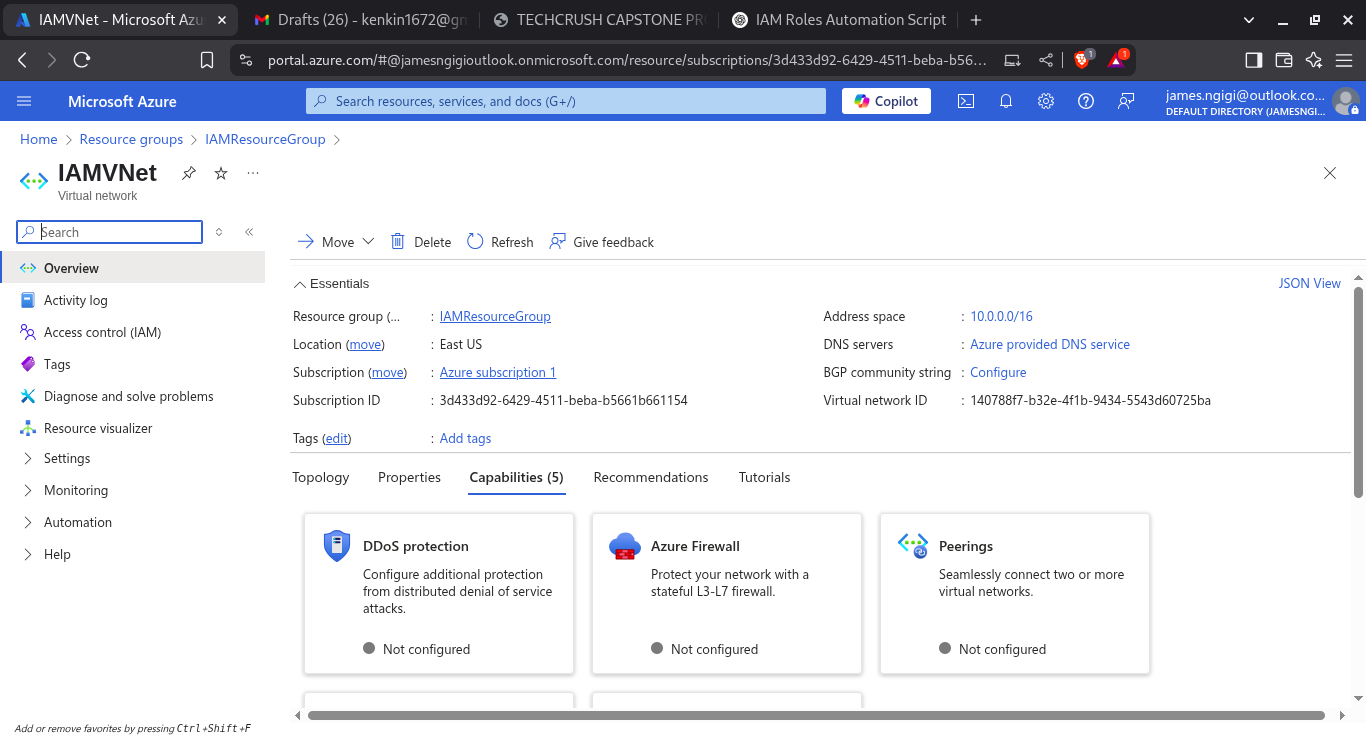
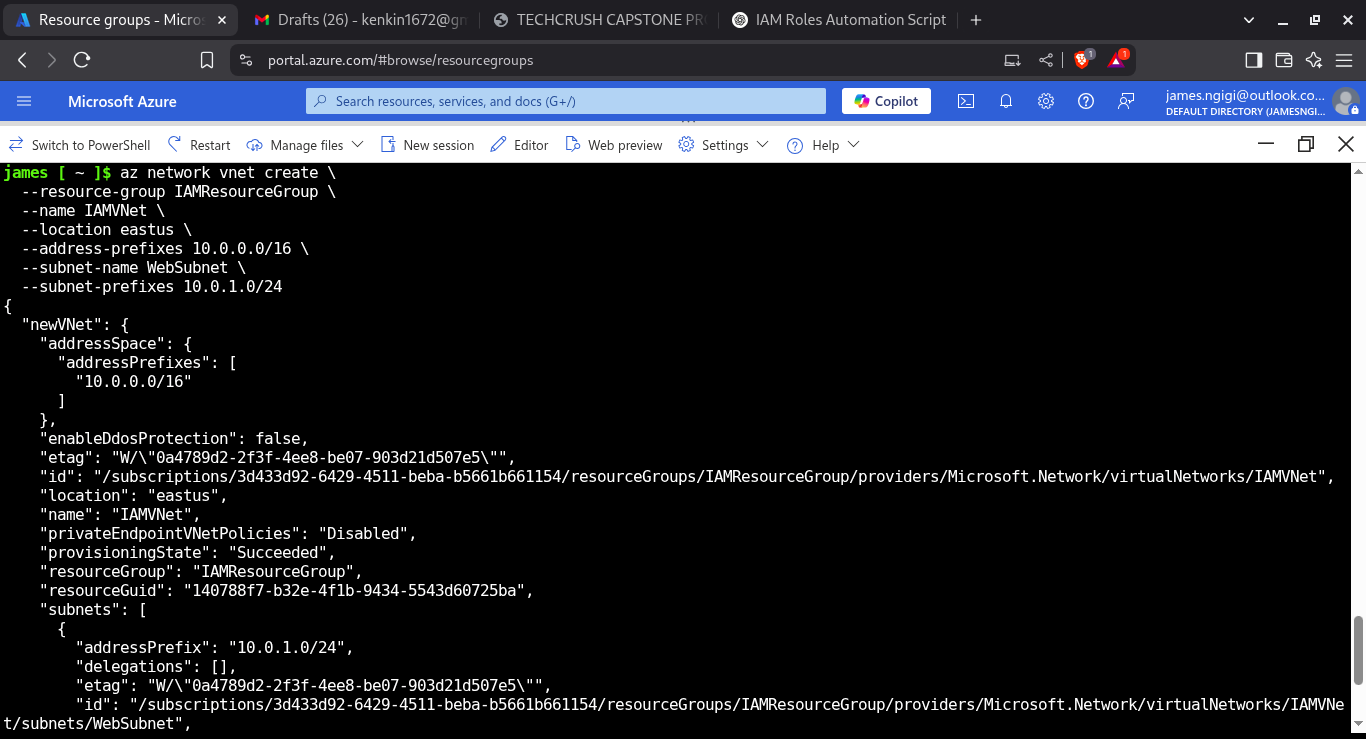
USER1=" kennedy.mbugua@jamesngigioutlook.onmicrosoft.com "

USER2="Mr.temiloluwa@jamesngigioutlook.onmicrosoft.com"

**CREATING A RESOURCE GROUP**

az group create --name IAMResourceGroup --location eastus

**CREATING A VIRTUAL NETWORK.**



az network vnet create

--name IAMVNet

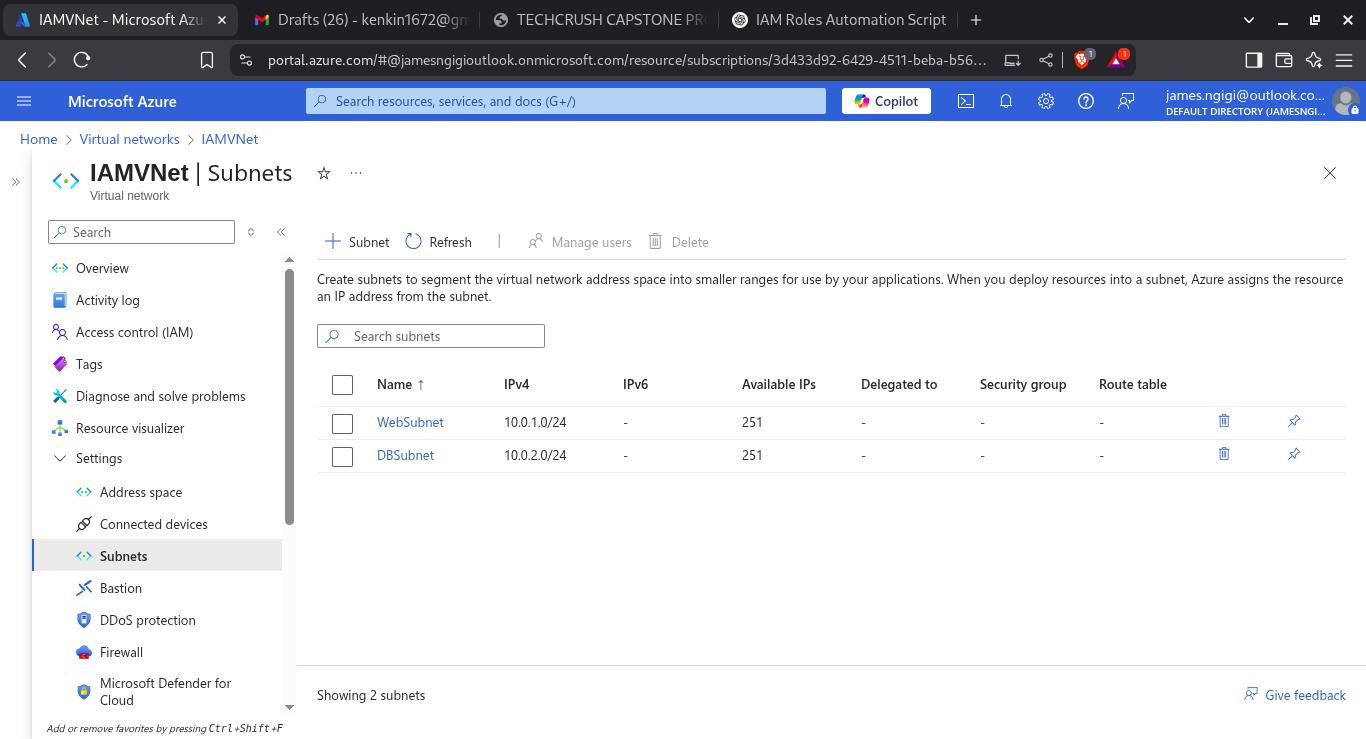
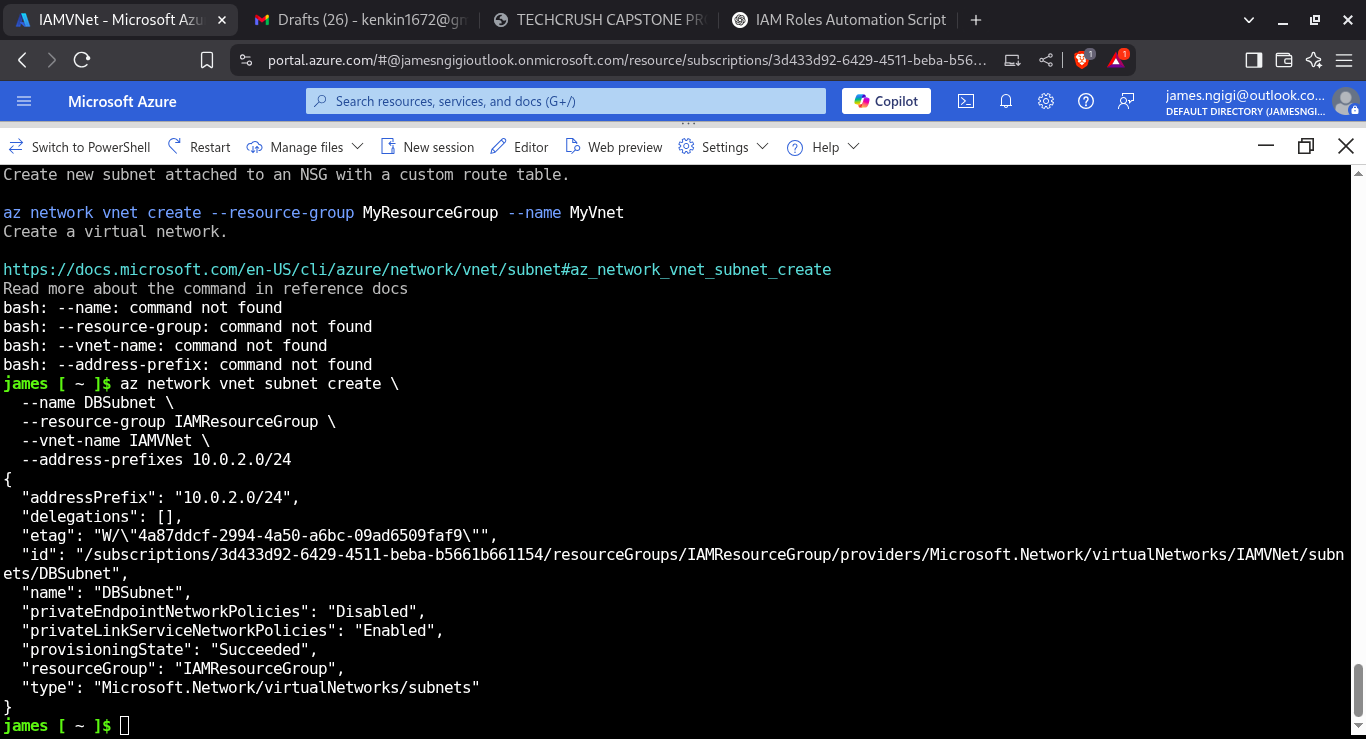
--resource-group IAMResourceGroup

--location eastus

--address-prefix 10.0.0/16

**CREATING TWO SUBNETS**

**DBSubnet**



az network vnet subnet create

--name DBSubnet

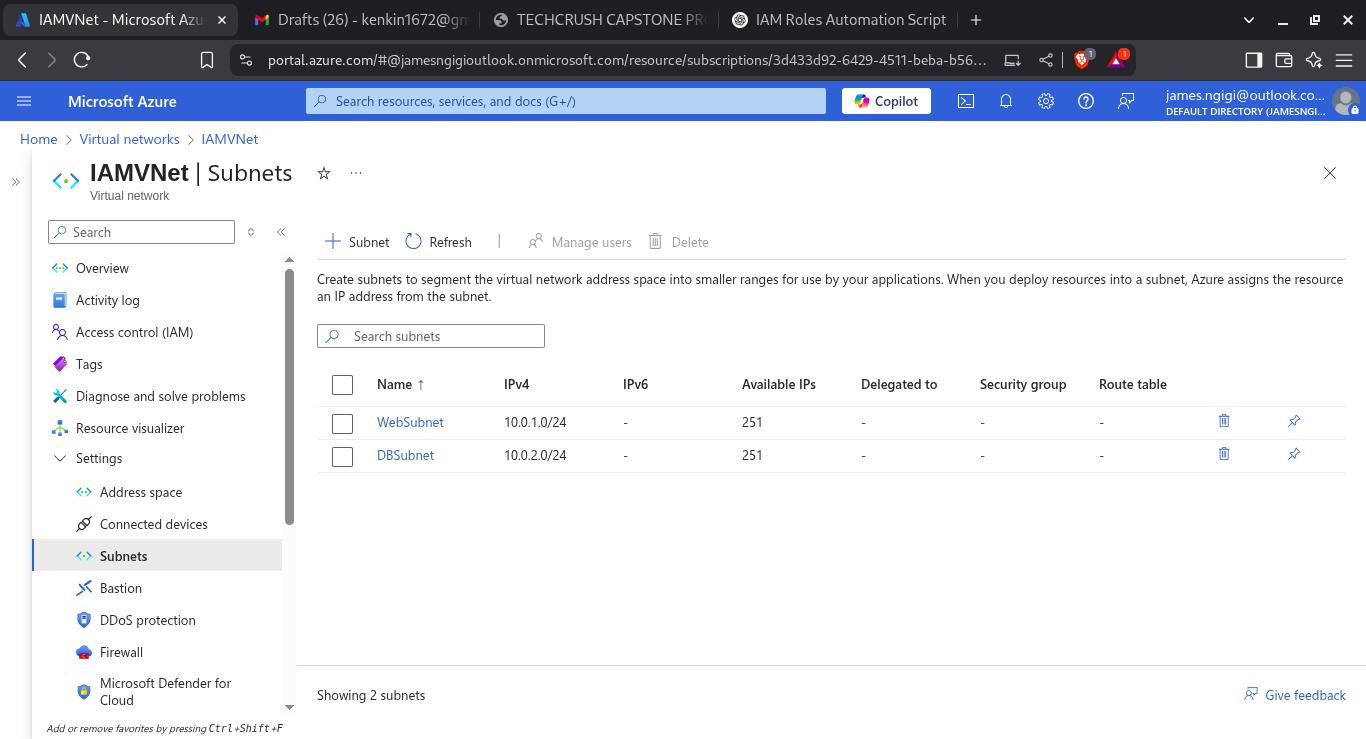
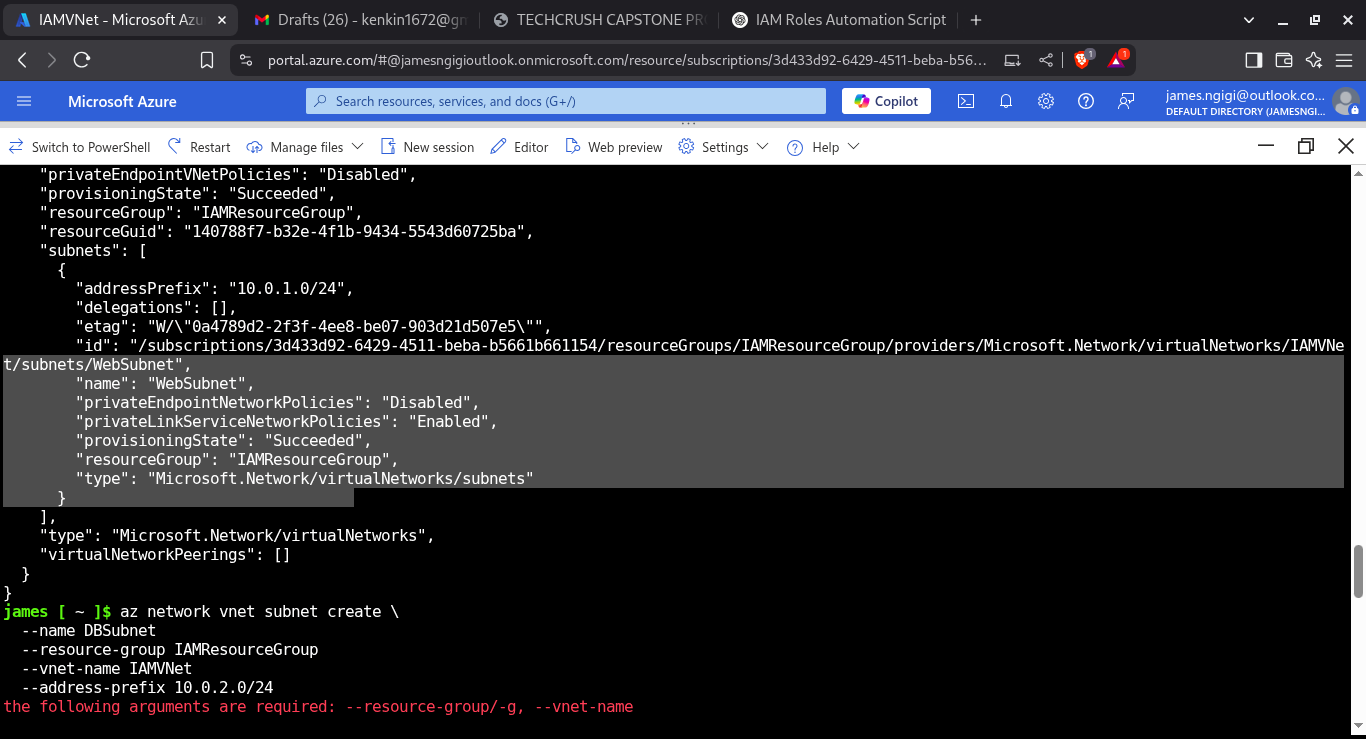
--resource-group IAMResourceGroup

--vnet-name IAMVNet

--address-prefix 10.0.2.0/24

**CREATING TWO SUBNETS**

**WebSubnet**



az network vnet subnet create

--name WebSubnet

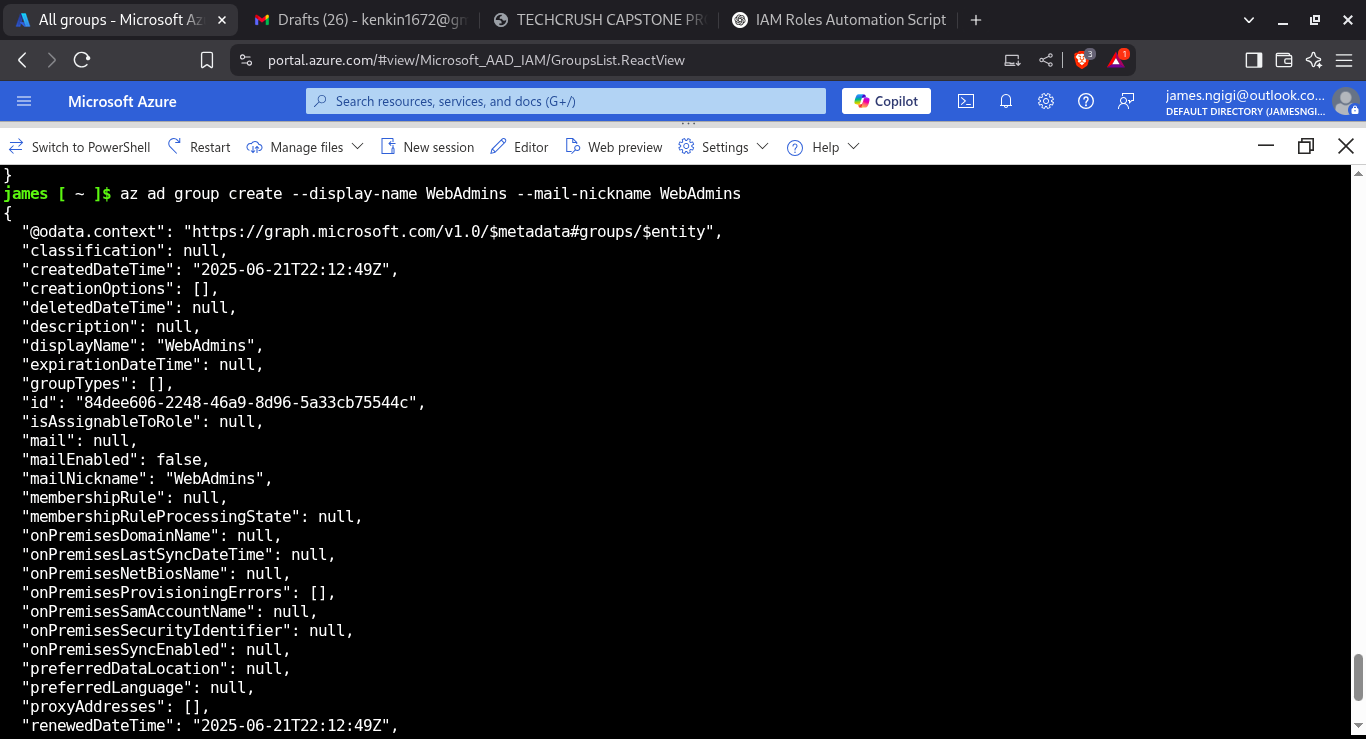
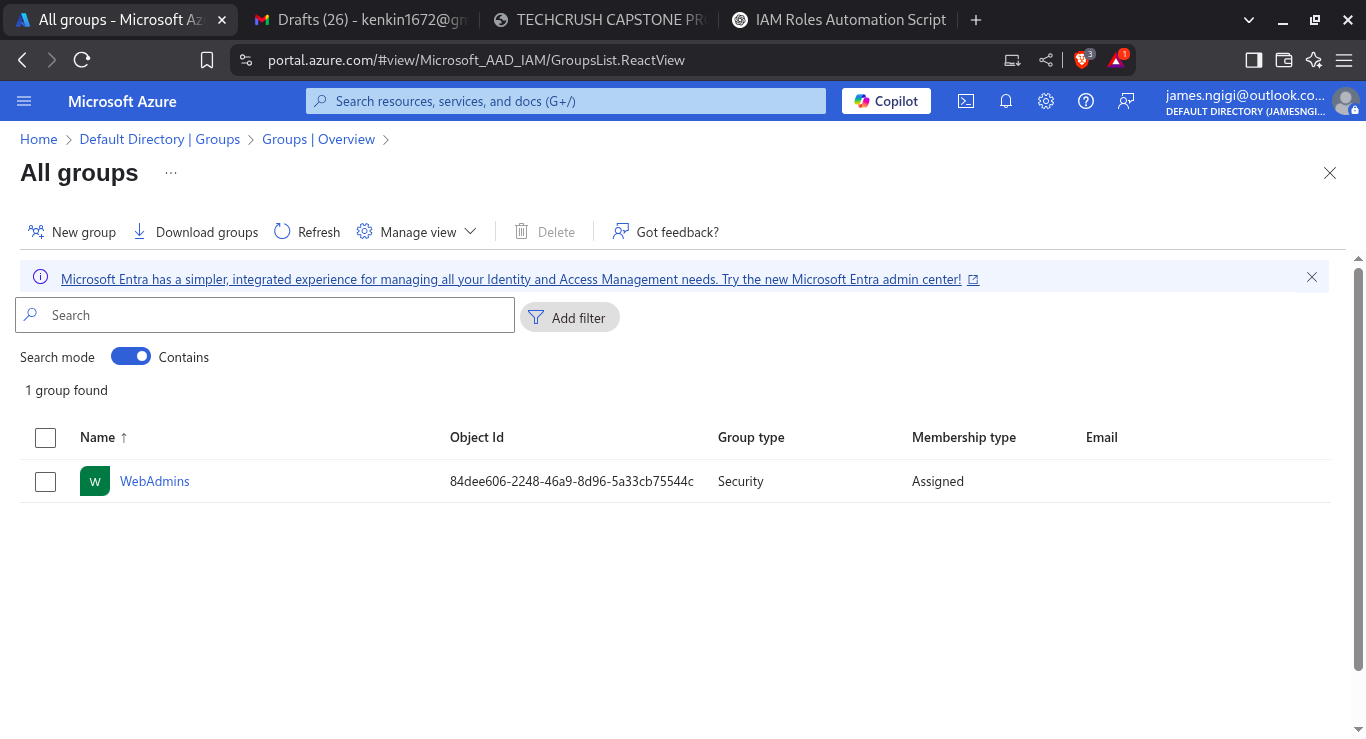
--resource-group IAMResourceGroup

--vnet-name IAMVNet

--address-prefix 10.0.1.0/24

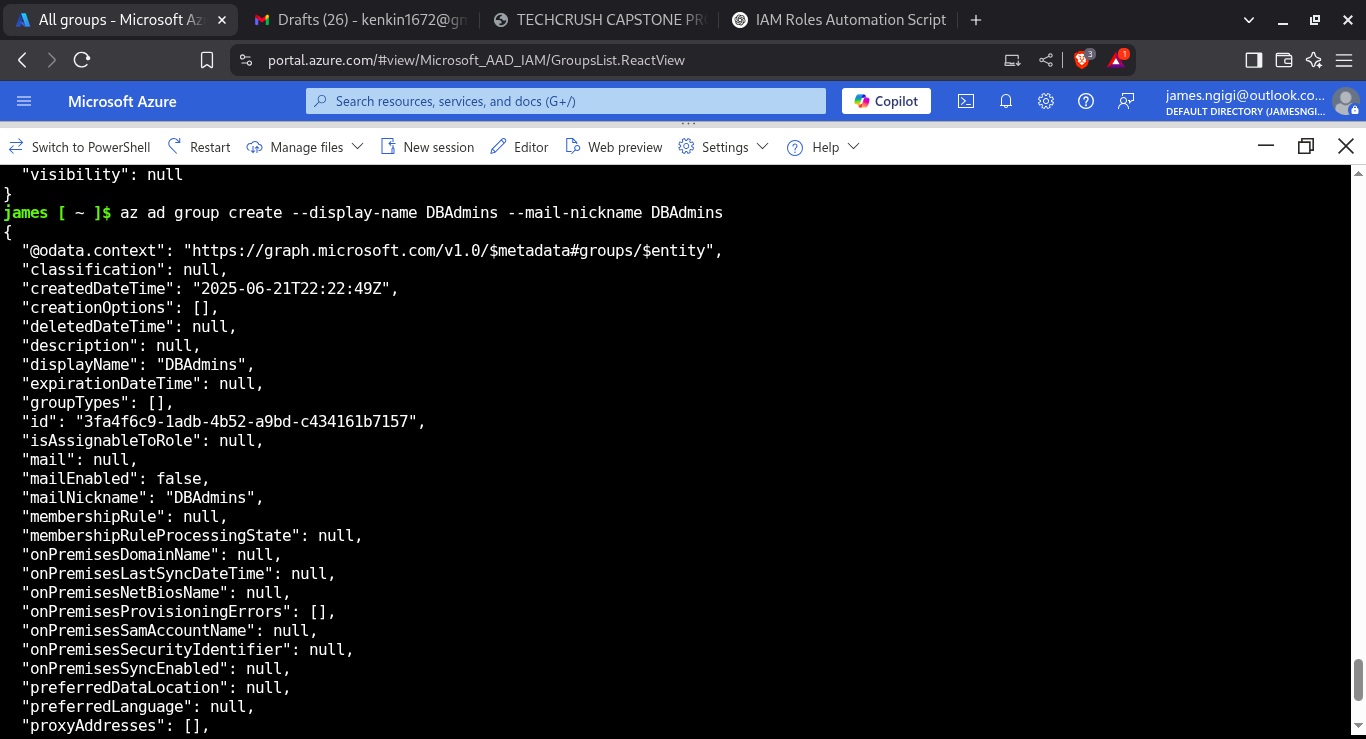
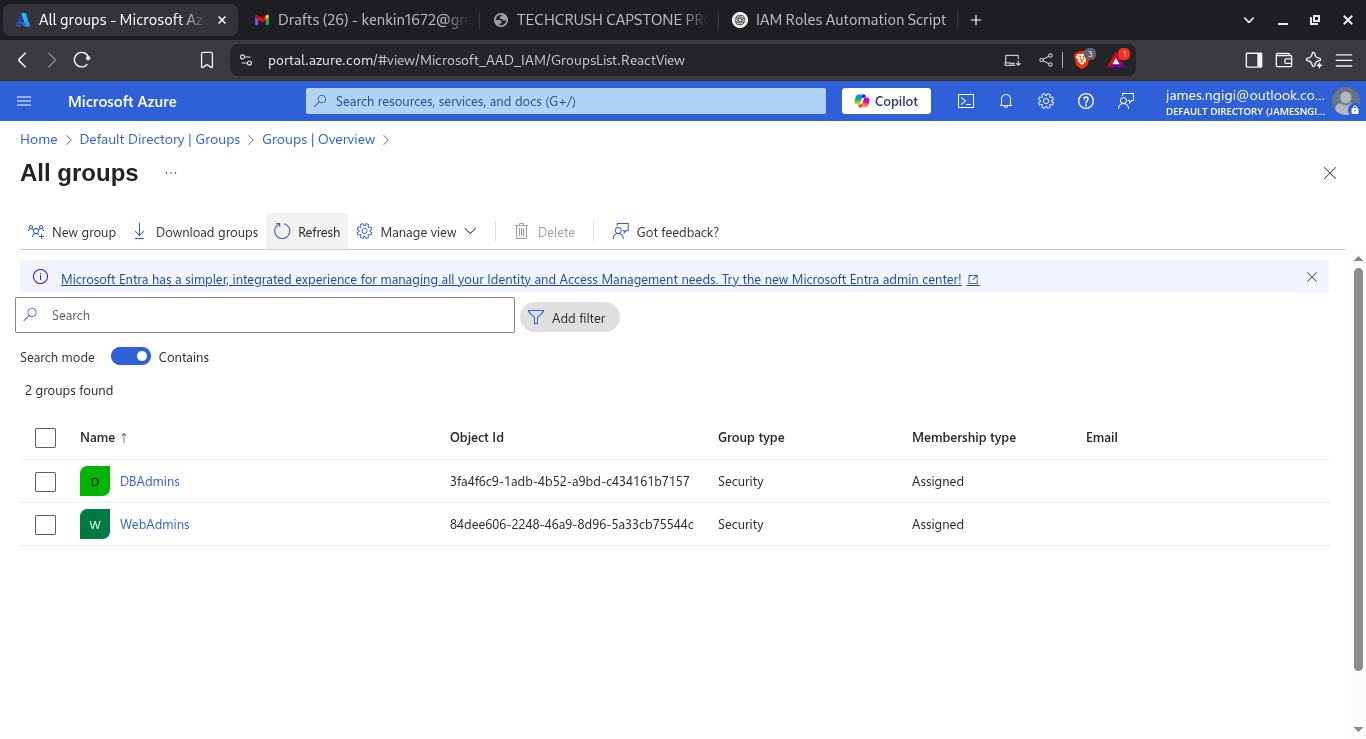
2. Create Azure AD groups: 'WebAdmins' and 'DBAdmins'.

**CREATING WEBADMINS GROUP**



az ad group create --display-name WebAdmins --mail-nickname WebAdmins

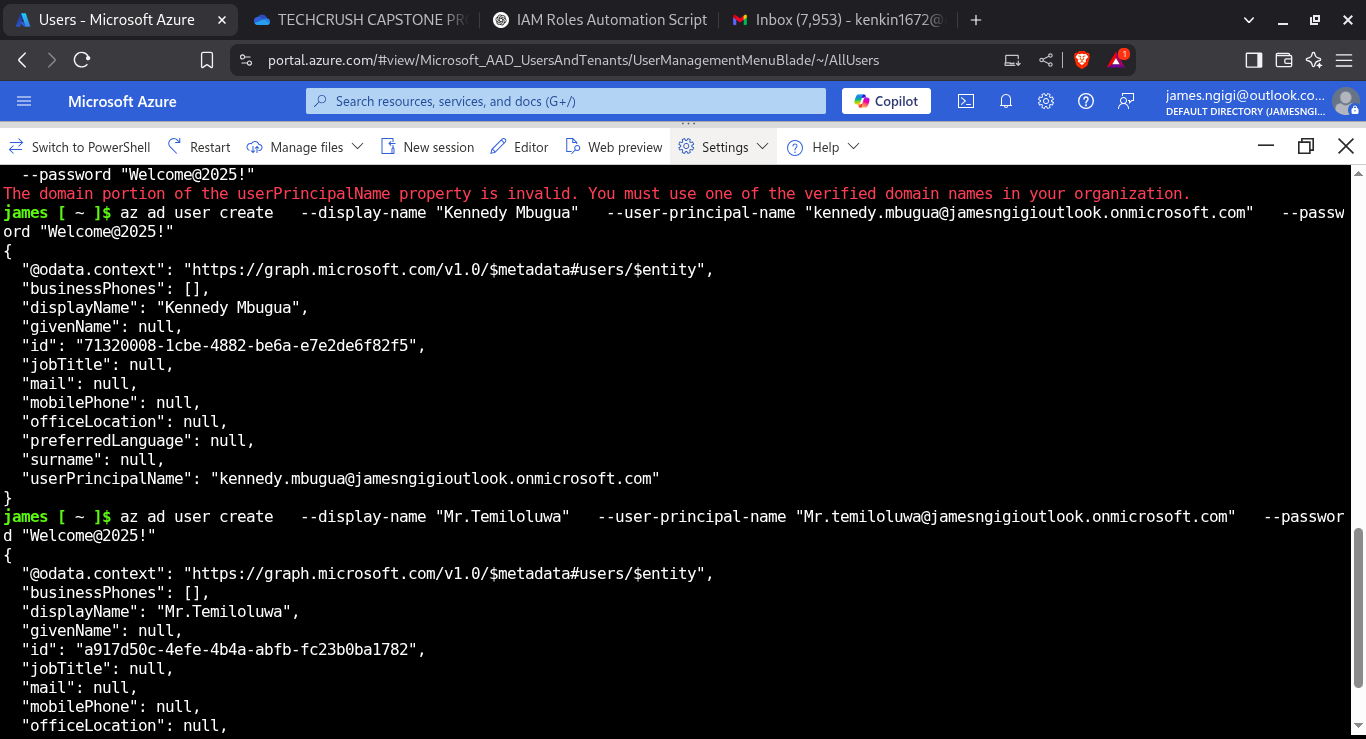
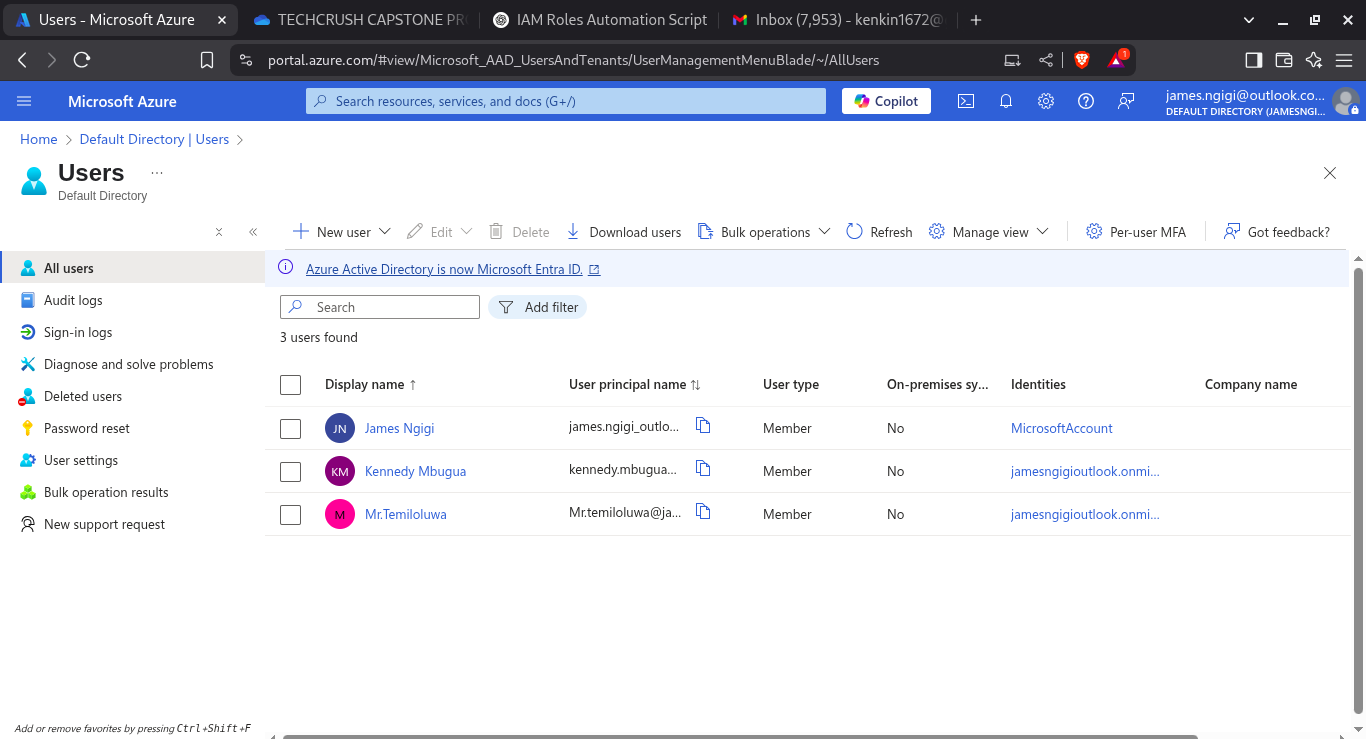
**CREATING DBAdmin GROUP**



az ad group create --display-name DBAdmins --mail-nickname DBAdmins

4. Add test users to the AD groups and validate role assignments.

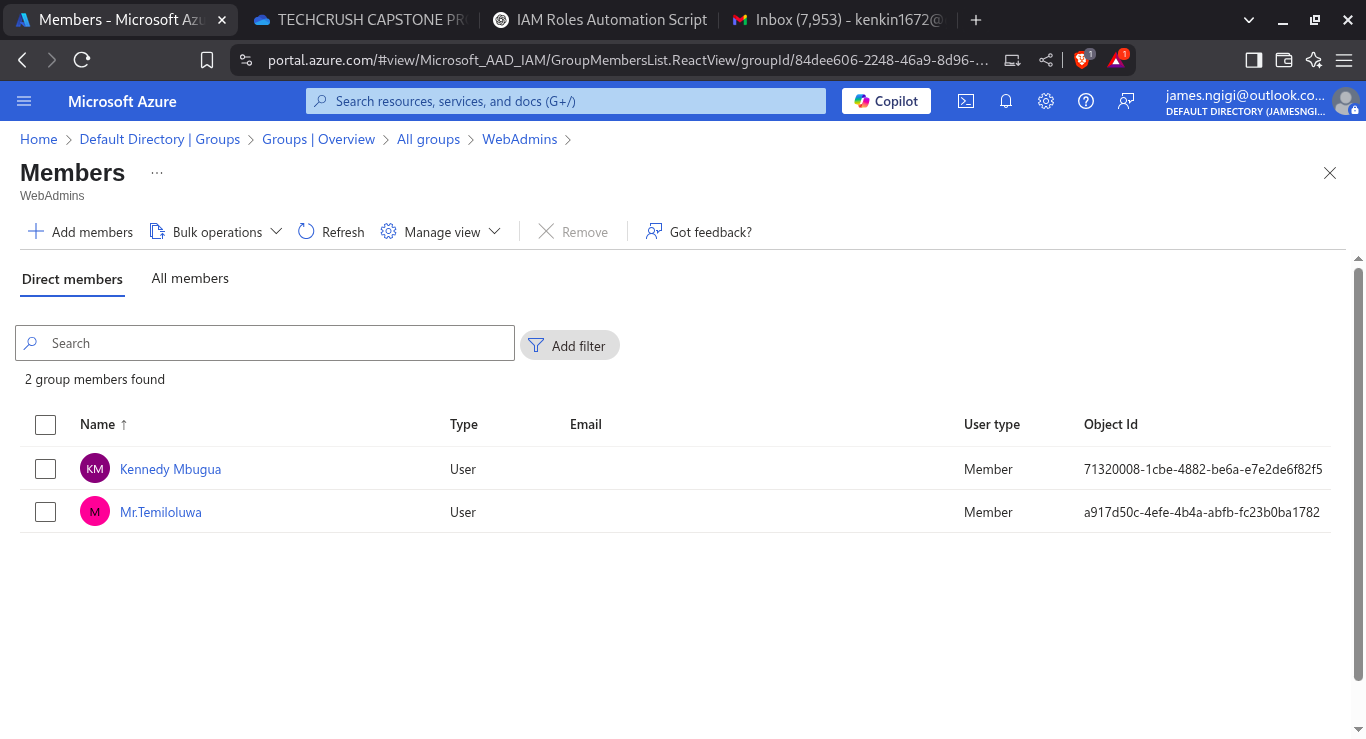
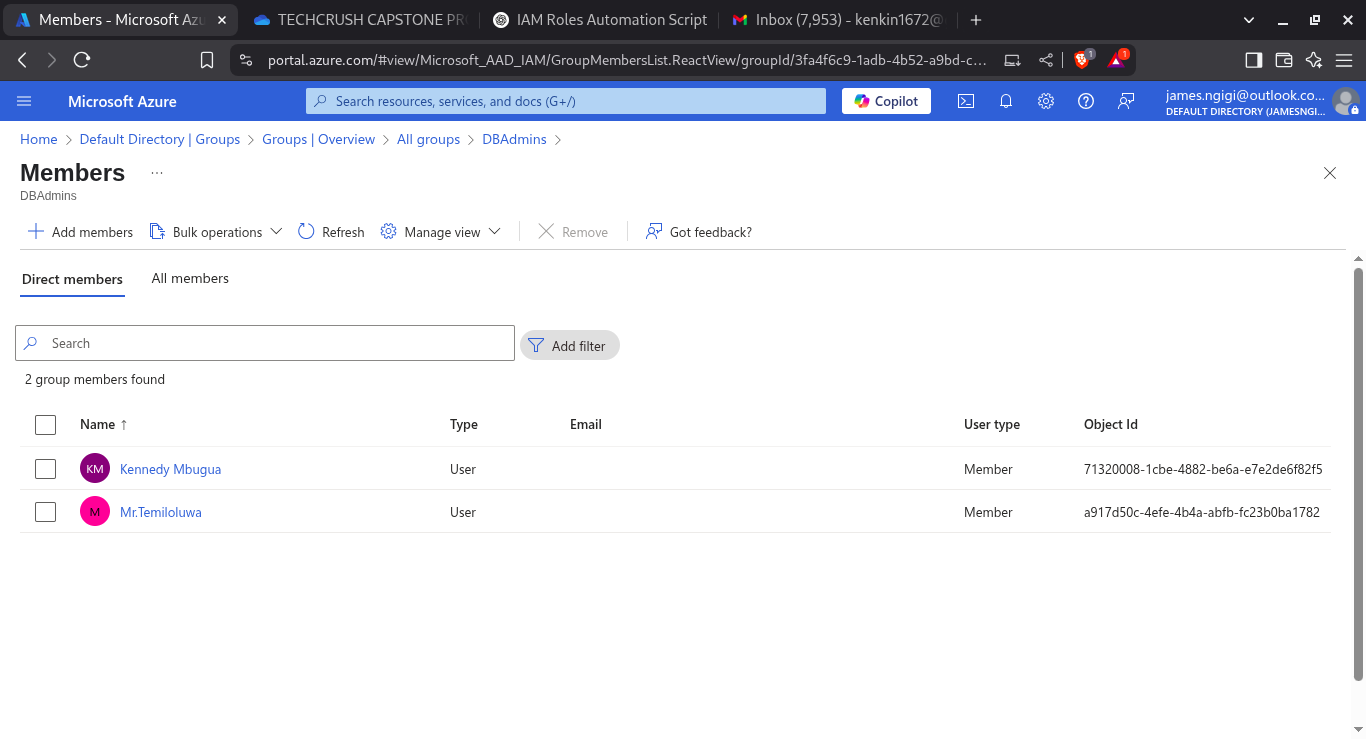
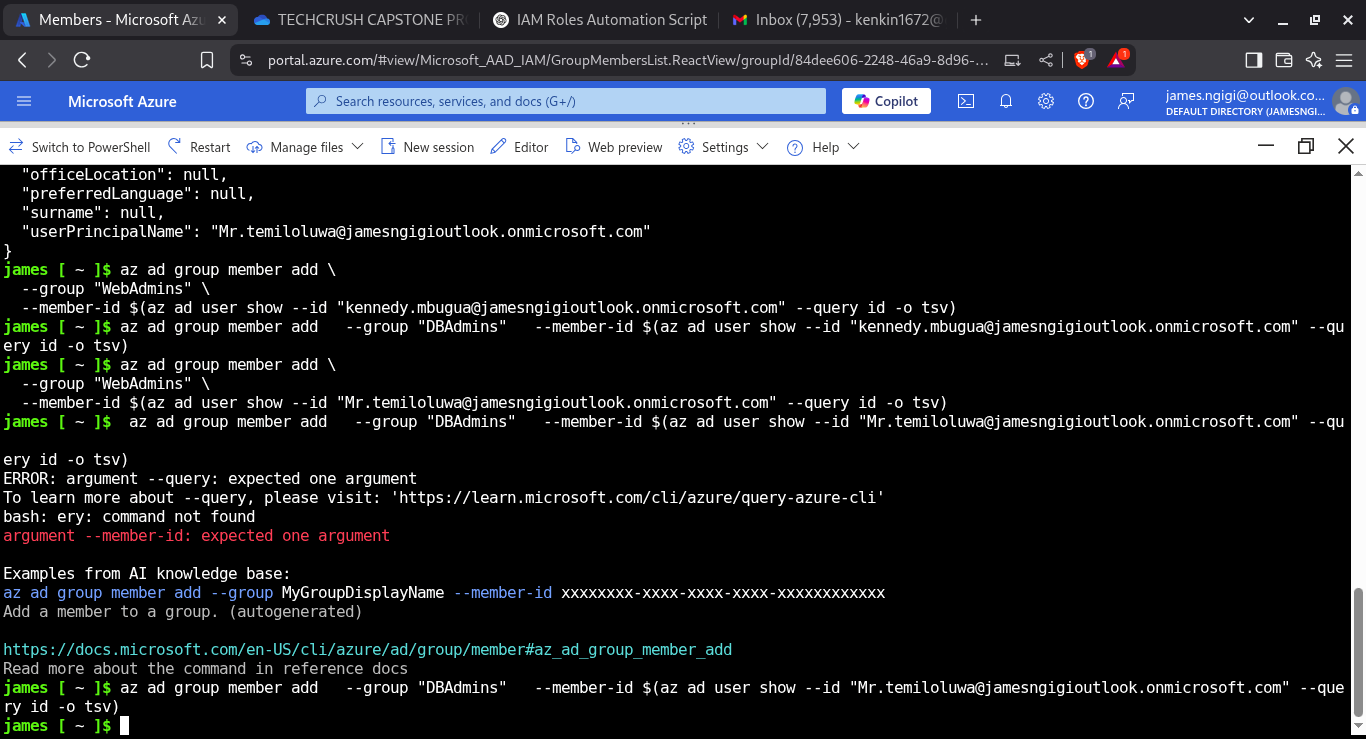
**CREATING USERACCOUNTS**



az ad user create --display-name "Kennedy Mbugua" --user-principal-name "[kennedy.mbugua@jamesngigioutlook.onmicrosoft.com](mailto:kennedy.mbugua@yourtenant.onmicrosoft.com)" --password "Welcome@2025!"

az ad user create --display-name "Mr.Temiloluwa" --user-principal-name "Mr[.temiloluwa@jamesngigioutlook.onmicrosoft.com](mailto:kennedy.mbugua@yourtenant.onmicrosoft.com)" --password "Welcome@2025!"

**ADDING USERS TO GROUPS**



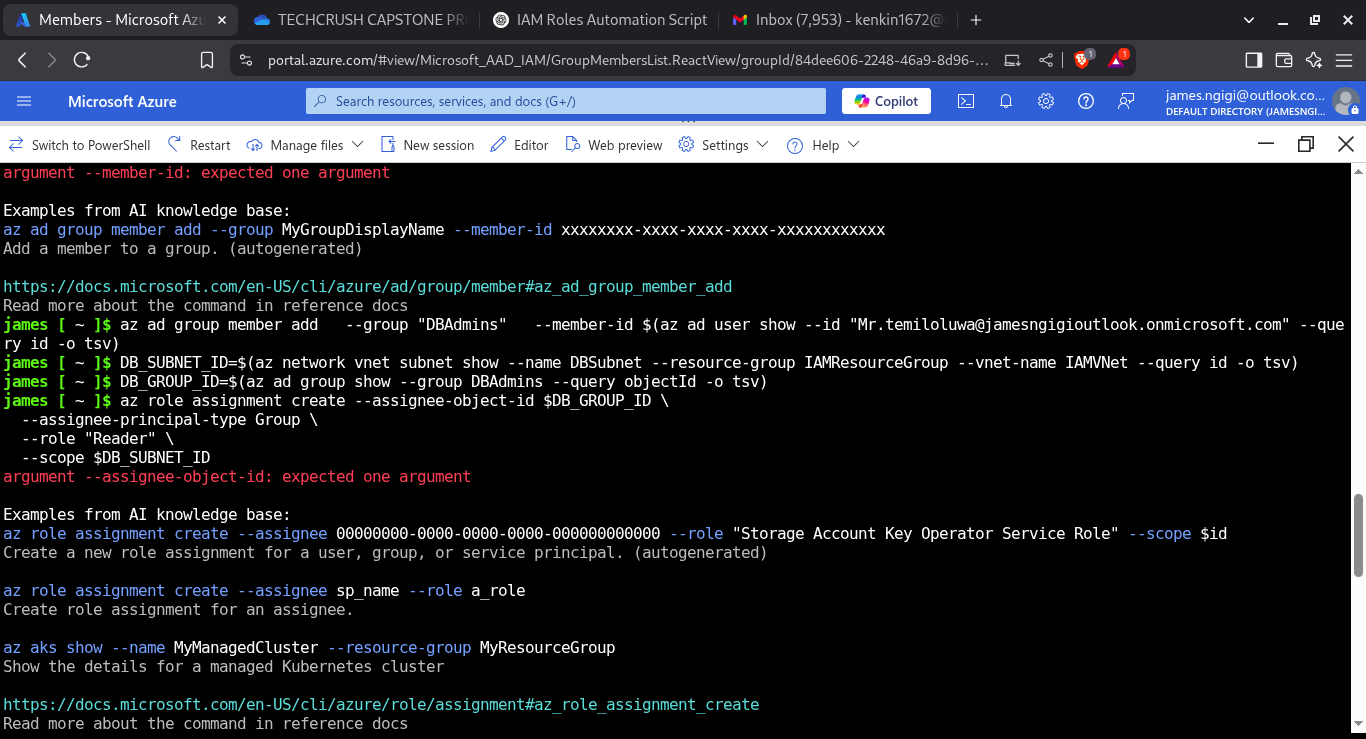
az ad group member add –group WebAdmins --member-id $(az ad user show --id kennedy.mbugua@jamesngigioutlook.onmicrosoft.com --query id -o tsv)

az ad group member add --group DBAdmins --member-id $(az ad user show --id Mr.temiloluwa@jamesngigioutlook.onmicrosoft.com --query id -o tsv)

3. Assign Reader role to DBAdmins for DB subnet resources.

**Assigning Reader role to DBAdmins on DB subnet**

Getting the subnet ID for DB subnet and getting the object ID of the DBAdmins group



DB\_SUBNET\_ID=$(az network vnet subnet show

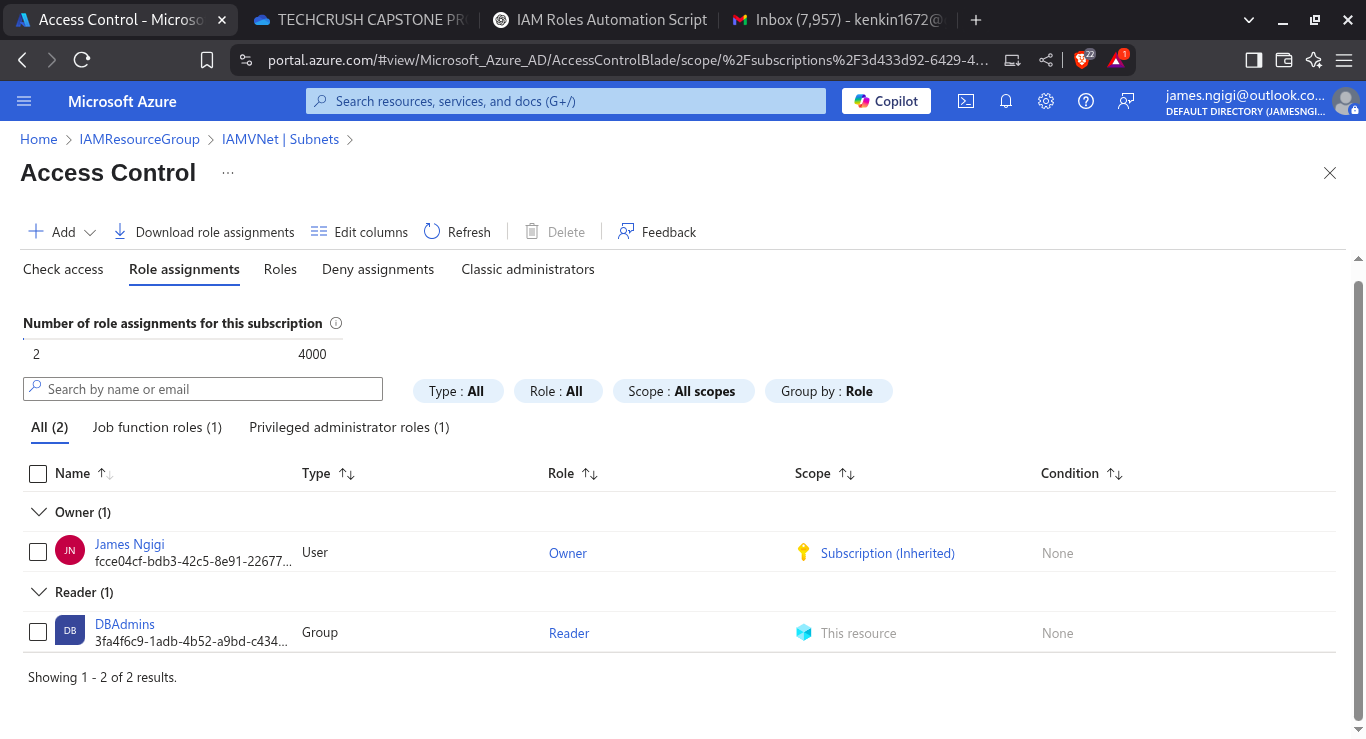
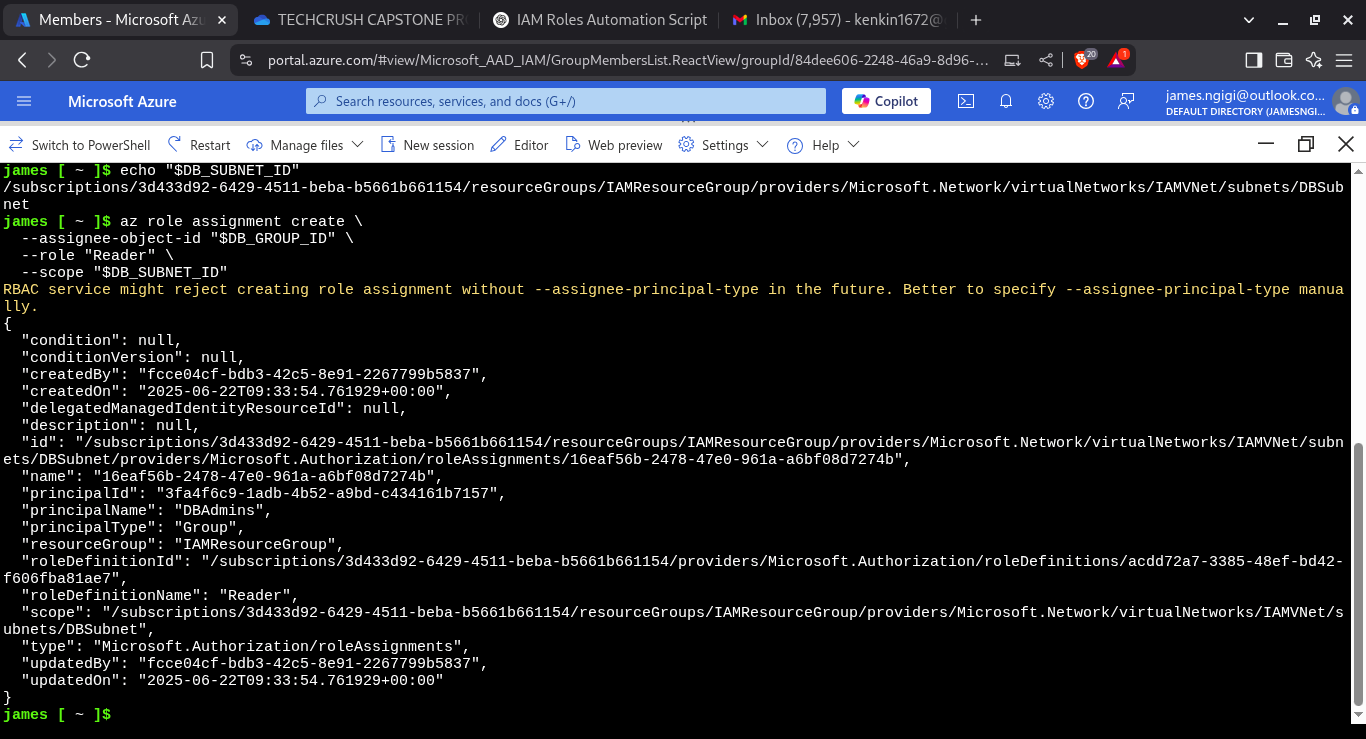
--name "DBSubnet"

--resource-group "IAMResourceGroup"

--vnet-name "IAMVNet"

--query id -o tsv)

Assigning Reader role to DBAdmins on DB subnet



az role assignment create --assignee-object-id "$DB\_GROUP\_ID" --role "Reader" --scope "$DB\_SUBNET\_ID"