Assignment – 3

Submitted by ~ Ishika Dutta (CT_CSI_DV_5572)

Task 3.1
Observe assigned Subscriptions Observe Azure Entra ID or create own Azure Entra ID in personal Azure account Create test users and groups Assign a RBAC role to user and test Create a custom role and assigned to users and test

Observe Assigned Subscriptions

- Go to Azure Portal.
- In the top-right corner, click on your profile.
- Select **"Switch Directory"**.
- You'll see a list of **subscriptions** and **directories** you're part of.
- Alternatively, search **"Subscriptions"** in the search bar.
- Click a subscription to view **Access Control (IAM)**, policies, billing, etc.

Observe Azure Entra ID or Create Your Own in Personal Azure Account

Observe Azure Entra ID:

- In the Azure Portal, search "Microsoft Entra ID".
- View your default directory (tenant).
- Click Users, Groups, App registrations, Roles, etc. to explore.
- Check Tenant ID, name, and domain from Overview.

Create a New Azure Entra ID:

- Go to Microsoft Entra ID > Manage tenants (bottom-left).
- Click + Create > Choose Azure Active Directory.
- Fill in:
    - Organization Name
    - Initial Domain Name
    - Region
- Click Review + Create > Create.
- Switch to this new tenant using the profile icon > Switch Directory.

Create Test Users and Groups

Create Users:

- Go to Microsoft Entra ID > Users > + New User.
- Choose Create User (not invite).
- Enter:
    - Name
    - User name (auto domain)
    - Password (auto-generated or custom)
- Click Create.

Create Groups:

- Go to Microsoft Entra ID > Groups > + New Group.
- Group Type: Security.
- Name your group, e.g., "TestGroup".
- Add members (click on user names).
- Click Create.

Assign a RBAC Role to a User and Test

Assign RBAC Role (e.g., Reader or Contributor):

- Go to Subscriptions > Select your subscription.
- Click Access Control (IAM) > + Add > Add role assignment.
- Choose a Role (e.g., Reader).
- Assign access to: User, group, or service principal.
- Select a user you created.
- Click Review + Assign.

Test:

- Login
- Verify limited access (Reader cannot edit resources).

Create a Custom Role and Assign It to Users

Steps to Create Custom Role:

- Go to Subscriptions > Select your subscription.
- Click Access Control (IAM) > + Add > Add custom role.
- In Basics:
    - Name: e.g., "CustomReadVMs"
    - Description: "Can read VM resources"
- Permissions Tab:
    - Click + Add permissions
    - Search for: Microsoft.Compute/virtualMachines/read
    - Add selected.
- Assignable Scope:
    - Select your Subscription or Resource Group.
- Review + Create.

Assign the Custom Role:

- After creation, go to Access Control (IAM) > + Add > Add role assignment.
- Search your custom role and assign it to the test user.
- Test by logging in as the test user and navigating to Virtual Machines.

Task 3.2
Observe assigned Subscriptions Observe Azure Entra ID or create own Azure Entra ID in personal Azure account Create test users and groups Assign a RBAC role to user and test Create a custom role and assigned to users and test

(Repetition, Same as Task 3.1)

Task 3.3
Create Virtual maching and Vnet from Azure CLI

Login to Azure

```
az login
```

Set the Subscription (if multiple)

```
az account set --subscription "Your-Subscription-Name"
```

Create a Resource Group

```
az group create \
  --name MyResourceGroup \
  --location eastus
```

Create a Virtual Network and Subnet

```
az network vnet create \
  --resource-group MyResourceGroup \
  --name MyVNet \
  --address-prefix 10.0.0.0/16 \
  --subnet-name MySubnet \
  --subnet-prefix 10.0.0.0/24
```

Create a Public IP

```
az network public-ip create \
  --resource-group MyResourceGroup \
  --name MyPublicIP
```

Create a Network Security Group

```
az network nsg create \
  --resource-group MyResourceGroup \
  --name MyNSG
```

Create NSG Rule to Allow SSH

```
az network nsg rule create \
  --resource-group MyResourceGroup \
  --nsg-name MyNSG \
  --name AllowSSH \
  --protocol tcp \
  --priority 1000 \
  --destination-port-range 22 \
  --access allow
```

Create a Network Interface

```
az network nic create \
  --resource-group MyResourceGroup \
  --name MyNIC \
  --vnet-name MyVNet \
  --subnet MySubnet \
  --network-security-group MyNSG \
  --public-ip-address MyPublicIP
```

Create a Virtual Machine

```
az vm create \
  --resource-group MyResourceGroup \
  --name MyVM \
  --nics MyNIC \
  --image UbuntuLTS \
  --admin-username azureuser \
  --generate-ssh-keys
```

Get the Public IP to SSH into VM

```
az vm show \
  --resource-group MyResourceGroup \
  --name MyVM \
  --show-details \
  --query "publicIps" \
  --output tsv
```

To Connect:

```
ssh azureuser@<Public-IP>
```

Task 3.4
Create and assign a any policy at subscription level

Set the Subscription

```
az account set --subscription "<Your-Subscription-Name-or-ID>"
```

Create a Policy Definition (Example: Disallow Public IP on VMs)

```
az policy definition create \
  --name "disallow-public-ip" \
  --display-name "Disallow Public IP on VMs" \
  --description "This policy denies VM creation with public IPs" \
  --rules '{
    "if": {
      "allOf": [
        {
          "field": "type",
          "equals": "Microsoft.Network/networkInterfaces"
        },
        {
          "field": "Microsoft.Network/networkInterfaces/ipConfigurations[*].publicIpAddress.id",
          "exists": "true"
        }
      ]
    },
    "then": {
      "effect": "deny"
    }
  }' \
  --mode All
```

Assign the Policy at the Subscription Level

To get subscription ID:

```
az account show --query id --output tsv
```

Assign the policy:

```
az policy assignment create \
  --name "no-public-ip-assignment" \
  --policy "disallow-public-ip" \
  --scope "/subscriptions/<your-subscription-id>" \
  --display-name "Enforce no public IP for VMs"
```

To Verify Assignment

```
az policy assignment list --scope "/subscriptions/<your-subscription-id>" --output table
```

Remove the Assignment (if needed)

```
az policy assignment delete --name "no-public-ip-assignment"
```

Task 3.5

Create an Azure key vault and store secrets. Configure access policies for the Key Vault to allow authorized users or applications to manage keys and secrets. retrieve secret from key vault using azure CLI

Create a Key Vault

```
az keyvault create \
  --name MyKeyVault12345 \
  --resource-group MyResourceGroup \
  --location eastus
```

Note: MyKeyVault12345 is globally unique

Add a Secret

```
az keyvault secret set \
  --vault-name MyKeyVault12345 \
  --name "MySecretName" \
  --value "ThisIsMySecretValue"
```

Configure Access Policies

Grant yourself access to manage secrets and keys

Get your current user object ID:

```
az ad signed-in-user show --query objectId --output tsv
```

Use that object ID to set access:

```
az keyvault set-policy \
  --name MyKeyVault12345 \
  --object-id <your-user-object-id> \
  --secret-permissions get list set delete \
  --key-permissions get list create delete
```

Retrieve Secret Using CLI

```
az keyvault secret show \
  --vault-name MyKeyVault12345 \
  --name "MySecretName" \
  --query value \
  --output tsv
```

Output:

```
ThisIsMySecretValue
```

Task 3.6
Create a VM from Powershell

Create a VM using PowerShell

Set Variables

```
$resourceGroup = "MyResourceGroup"
$location = "EastUS"
$vmName = "MyVM"
$vnetName = "MyVNet"
$subnetName = "MySubnet"
$ipName = "MyPublicIP"
$nicName = "MyNIC"
$nsgName = "MyNSG"
$adminUsername = "azureuser"
$adminPassword = ConvertTo-SecureString "YourPassword@123" -AsPlainText -Force
```

Create a Resource Group

```
New-AzResourceGroup -Name $resourceGroup -Location $location
```

Create Virtual Network and Subnet

```
$subnetConfig = New-AzVirtualNetworkSubnetConfig -Name $subnetName -AddressPrefix "10.0.0.0/24"
$vnet = New-AzVirtualNetwork -Name $vnetName -ResourceGroupName $resourceGroup -Location $location -AddressPrefix "10.0.0.0/16"
```

Create Public IP

```
$publicIP = New-AzPublicIpAddress -Name $ipName -ResourceGroupName $resourceGroup -Location $location -AllocationMethod Dynamic
```

Create Network Security Group and Rule (Allow SSH)

```
$nsgRule = New-AzNetworkSecurityRuleConfig -Name "Allow-SSH" -Protocol Tcp -Direction Inbound -Priority 1000 -SourceAddressPref
$nsg = New-AzNetworkSecurityGroup -ResourceGroupName $resourceGroup -Location $location -Name $nsgName -SecurityRules $nsgRule
```

Create Network Interface

```
$subnet = Get-AzVirtualNetworkSubnetConfig -Name $subnetName -VirtualNetwork $vnet
$nic = New-AzNetworkInterface -Name $nicName -ResourceGroupName $resourceGroup -Location $location -Subnet $subnet -PublicIpAdd
```

Define VM Configuration

```
$vmConfig = New-AzVMConfig -VMName $vmName -VMSize "Standard_DS1_v2" |
    Set-AzVMOperatingSystem -Linux -ComputerName $vmName -Credential (New-Object System.Management.Automation.PSCredential($adm
    Set-AzVMSourceImage -PublisherName "Canonical" -Offer "UbuntuServer" -Skus "18.04-LTS" -Version "latest" |
    Add-AzVMNetworkInterface -Id $nic.Id
```

Create the VM

```
New-AzVM -ResourceGroupName $resourceGroup -Location $location -VM $vmConfig
```

To Get Public IP of the VM

```
(Get-AzPublicIpAddress -Name $ipName -ResourceGroupName $resourceGroup).IpAddress
```

SSH Into Your VM

```
ssh azureuser@<Public-IP>
```

Task 3.7/8/9/10

A. Schedule a Daily backup of VM at 3:AM using vault 1. Create an Alert rule for VM CPU percentage: Criteria: CPU% MoreThan 80 There Should be analert on Email." B.Provision backups in backup center 2. Schedule a Daily backup of VM at 3:AM using vault. Configure Retention period in backup policy and retain an old backup

VM Backup and CPU Alert (Daily Backup at 3AM + Email Alert on CPU > 80%)

Create a Recovery Services Vault (vault1)

```
az backup vault create \
  --name vault1 \
  --resource-group MyResourceGroup \
  --location eastus
```

Set Vault's Backup Storage Redundancy

```
az backup vault backup-properties set \
  --name vault1 \
  --resource-group MyResourceGroup \
  --backup-storage-redundancy LocallyRedundant
```

Register VM with Vault

```
az backup protection enable-for-vm \
  --resource-group MyResourceGroup \
  --vault-name vault1 \
  --vm MyVM \
  --policy-name DefaultPolicy
```

Create Alert Rule for CPU > 80% via Azure Monitor

- Go to Virtual Machine > Monitoring > Alerts
- Click + Create Alert Rule
- Under Scope, select your VM.
- Under Condition, choose:
    - Signal name: Percentage CPU
    - Operator: GreaterThan
    - Threshold: 80
- Action Group:
    - Click Create action group
    - Choose name, region.
    - Add an Email action.
- Set alert rule name, and click Create Alert Rule

Backup via Backup Center with Retention Configuration

Go to Backup Center

- Open Azure Portal
- Search Backup Center > + Backup
- Where is your workload running? → Azure
- What do you want to back up? → Virtual Machine
- Choose:
    - Subscription
    - Resource Group
    - Vault (vault1)
    - VM (MyVM)

- Select + Create new policy

Create Custom Backup Policy (3AM & Retention)

- Name: Daily3AMPolicy
- Backup schedule:
    - Frequency: Daily
    - Time: 3:00 AM
- Retention:
    - Daily: 30 days (adjust as needed)
    - Weekly, Monthly, Yearly: Configure if needed
- Save and assign this policy to your VM

Retain an Old Backup (via Restore Point Lock or Policy)

To retain an older backup version:

- Go to Recovery Services Vault > Backup Items > Azure VMs > MyVM
- Select a restore point
- Click Lock or mark it as "Don't delete"