Azure Cloud Tasks Assignment

Task 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

1. Observe Assigned Subscriptions

- Go to Azure Portal → Click on profile → Select 'Switch Directory'.

- Check assigned subscriptions under 'Subscriptions' in sidebar.

- Note details like name, ID, and directory.

2. Observe or Create Azure Entra ID

- View: Search 'Microsoft Entra ID' in Azure Portal.

- Note Tenant Name, ID, and Directory Type.

- To Create: Go to Microsoft Entra ID → Manage tenants → + Create → Choose 'Azure Active Directory' and provide organization details.

3. Create Test Users and Groups

- Users: Microsoft Entra ID → Users → + New User → Fill username and password.

- Groups: Microsoft Entra ID → Groups → + New Group → Type: Security → Add user (e.g., testuser1).

4. Assign RBAC Role

- Go to Subscriptions → Access Control (IAM) → + Add → Add role assignment → Role: Reader → Assign testuser1.

- Test access by logging in with testuser1.

5. Create and Assign Custom Role

- Go to Subscriptions → Access Control (IAM) → + Add → Add custom role → Start from Reader and add permissions (e.g., start VM).

- Assign to testuser1.

Task 2: Create Virtual maching and Vnet from Azure CLI

1. Login to Azure

```
az login
```

2. Create Resource Group

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

3. Create Virtual Network and Subnet

```
az network vnet create --resource-group MyResourceGroup --name MyVNet --subnet-name MySubnet
```

4. Create VM

```
az vm create --resource-group MyResourceGroup --name MyVM --vnet-name MyVNet --subnet MySubnet --image UbuntuLTS --admin-username azureuser --generate-ssh-keys
```

Task 3: Create and assign a any policy at subscription level

1. Go to Azure Policy → Click 'Assignments' → + Assign Policy.

2. Scope: Select Subscription and Resource Group (optional).

3. Policy Definition: Search and select 'Deny public IP addresses'.

4. Configure Assignment: Name: DenyPublicIP, Description optional.

5. Review and Create → Finalize.

Task 4: 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

1. Create Key Vault

```
az keyvault create --name MyKeyVault --resource-group
MyResourceGroup --location eastus
```

2. Store Secret

```
az keyvault secret set --vault-name MyKeyVault --name MySecret --
value "mySecretValue"
```

3. Retrieve Secret

```
az keyvault secret show --name MySecret --vault-name MyKeyVault --
query value -o tsv
```

4. Configure Access Policy in Azure Portal under Key Vault → Access Policies.

Task 5: Create a VM from Powershell

1. Login

```
Connect-AzAccount
```

2. Create Resource Group

```
New-AzResourceGroup -Name MyRG -Location 'EastUS'
```

3. Create VM

```
New-AzVM -ResourceGroupName 'MyRG' -Name 'MyVM' -Location 'EastUS' -
VirtualNetworkName 'MyVNet' -SubnetName 'MySubnet' -SecurityGroupName
'MyNSG' -PublicIpAddressName 'MyPublicIP' -Credential (Get-Credential)
```

Task 6: 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

A. Daily Backup at 3:00 AM

1. Create Recovery Services Vault → Name: MyBackupVault → Region: Same as VM.

2. Configure Backup → Select VM → Enable Backup.

3. Set Backup Policy → Daily at 3:00 AM → Retain for 30 days.

B. Create Alert for CPU > 80%

1. Go to VM → Monitoring → Alerts → + Create Alert Rule.

2. Condition: Percentage CPU > 80 over 5 mins.

3. Action Group: Email notification setup.

4. Finalize Alert → Name: HighCPUAlert → Severity: 2.