Azure Assignment Completion Report Completed by: Narayan

**Azure Assignment: Role-Based Access Control & Entra ID**

**1. Observe Assigned Subscriptions:**

* Sign in to [Azure Portal](https://portal.azure.com)
* Search for **"Subscriptions"** in the search bar.
* You’ll see all subscriptions assigned to your account.

**2. Observe Azure Entra ID or Create New:**

* Navigate to **Azure Active Directory** (Entra ID).
* If not available, click **Manage tenants > +Create**.
* Choose **Azure Active Directory**, give details, and click **Review + Create**.
* Once created, switch to the new directory.

**3. Create Test Users and Groups:**

* Go to **Azure Active Directory > Users > + New user**
  + Add basic info: username, name, password.
  + Create 2 users: user1@test.com, user2@test.com
* Go to **Groups > + New group**
  + Type: **Security**
  + Name: **TestGroup**
  + Add both users as members.

**4. Assign RBAC Role to a User and Test:**

* Go to **Subscriptions > [Your Subscription] > Access control (IAM)**
* Click **+ Add > Add role assignment**
* Choose role (e.g., **Reader**), assign access to **User**, select user1@test.com, and click **Save**.

**5. Create a Custom Role and Assign:**

* Go to **Access Control (IAM) > Roles > + New custom role**
* Name it (e.g., **VMReader**)
* In **Permissions**, add: Microsoft.Compute/virtualMachines/read
* Review and create the custom role.
* Assign it to user2@test.com using the same **Add role assignment** steps.
* **Azure Assignment: Create Virtual Machine and Virtual Network using Azure CLI**
* **Step 1: Log in to Azure CLI**
* az login
* This opens a browser window to sign in with your Azure credentials.
* **Step 2: Create a Resource Group**
* az group create --name MyResourceGroup --location eastus
* **Step 3: Create a Virtual Network (VNet)**
* az network vnet create \
* --resource-group MyResourceGroup \
* --name MyVNet \
* --address-prefix 10.0.0.0/16 \
* --subnet-name MySubnet \
* --subnet-prefix 10.0.1.0/24
* **Step 4: Create a Public IP Address**
* az network public-ip create \
* --resource-group MyResourceGroup \
* --name MyPublicIP
* **Step 5: Create a Network Security Group (NSG)**
* az network nsg create \
* --resource-group MyResourceGroup \
* --name MyNSG
* **Step 6: Create a Network Interface (NIC)**
* az network nic create \
* --resource-group MyResourceGroup \
* --name MyNIC \
* --vnet-name MyVNet \
* --subnet MySubnet \
* --network-security-group MyNSG \
* --public-ip-address MyPublicIP
* **Step 7: Create a Virtual Machine (VM)**
* az vm create \
* --resource-group MyResourceGroup \
* --name MyVM \
* --nics MyNIC \
* --image UbuntuLTS \
* --admin-username azureuser \
* --generate-ssh-keys
* **Step 8: Open Port 22 for SSH Access**
* az vm open-port --port 22 --resource-group MyResourceGroup --name MyVM
* **Step 9: Verify the VM is Running**
* az vm show --resource-group MyResourceGroup --name MyVM --show-details --output table

## ✅ **Assignment: Create and Assign a Policy at Subscription Level**

### 🔹 ****Method 1: Using Azure Portal****

#### ****Step 1: Go to Azure Policy****

* Open [Azure Portal](https://portal.azure.com)
* In the search bar, type **"Policy"** and open it.

#### ****Step 2: Select Definitions****

* On the left pane, click **"Definitions"**
* Click **"+ Policy definition"** to create a new policy.

#### ****Step 3: Define a New Policy****

* **Definition Location**: Select your subscription
* **Name**: DenyPublicIP
* **Description**: Deny creation of Public IPs
* **Category**: Networking (or custom)
* **Policy Rule**:

json

CopyEdit

{

"if": {

"field": "type",

"equals": "Microsoft.Network/publicIPAddresses"

},

"then": {

"effect": "deny"

}

}

* Click **Save**

#### ****Step 4: Assign the Policy to the Subscription****

* Go to **"Assignments" > "+ Assign Policy"**
* **Scope**: Select your Subscription
* **Policy Definition**: Search and select DenyPublicIP
* **Assignment Name**: Deny-PublicIP-Assignment
* Click **Next > Review + Create > Create**

✅ **Policy is now assigned to the subscription. Any resource creation that violates the rule will be blocked.**

### 🔹 ****Method 2: Using Azure CLI (Optional)****

#### ****Step 1: Login****

az login

#### ****Step 2: Create the Policy Definition****

Save the following to a file named denyPublicIP.json:

json

CopyEdit

{

"properties": {

"displayName": "Deny creation of Public IP",

"policyType": "Custom",

"mode": "All",

"description": "Deny the creation of public IPs",

"policyRule": {

"if": {

"field": "type",

"equals": "Microsoft.Network/publicIPAddresses"

},

"then": {

"effect": "deny"

}

}

}

}

#### ****Step 3: Create the Policy in Azure****

az policy definition create --name "DenyPublicIP" \

--display-name "Deny creation of Public IP" \

--description "This policy denies creation of public IPs" \

--rules denyPublicIP.json \

--mode All \

--subscription <your-subscription-id>

#### ****Step 4: Assign the Policy****

az policy assignment create --name "DenyPublicIPAssignment" \

--policy "DenyPublicIP" \

--scope /subscriptions/<your-subscription-id>

### ✅ Summary:

| **Task** | **Method** | **Completed** |
| --- | --- | --- |
| Create Policy Definition | Portal/CLI | ✅ |
| Assign Policy | Portal/CLI | ✅ |
| Scope Level | Subscription | ✅ |
| Policy Effect | Deny Public IP | ✅ |

### ****Task****: Create an Azure Key Vault, store secrets, configure access policies, and retrieve the secret using Azure CLI.

### 🔹 ****Step 1: Log in to Azure****

bash

CopyEdit

az login

This will open a browser window. Sign in with your Azure credentials.

### 🔹 ****Step 2: Create a Resource Group****

t

az group create --name MyResourceGroup --location eastus

### 🔹 ****Step 3: Create a Key Vault****

az keyvault create --name MyKeyVault123 --resource-group MyResourceGroup --location eastus

🔸 Note: Replace MyKeyVault123 with a globally unique name.

### 🔹 ****Step 4: Store a Secret in the Key Vault****

az keyvault secret set --vault-name MyKeyVault123 --name MySecret --value "ThisIsMySecretValue"

🔸 Here, MySecret is the name of the secret and "ThisIsMySecretValue" is the value.

### 🔹 ****Step 5: Configure Access Policy for Your User****

**Get your object ID:**

az ad signed-in-user show --query objectId -o tsv

Assume it returns: 11111111-2222-3333-4444-555555555555

**Set access policy:**

az keyvault set-policy \

--name MyKeyVault123 \

--object-id 11111111-2222-3333-4444-555555555555 \

--secret-permissions get list set delete

### 🔹 ****Step 6: Retrieve the Secret****

az keyvault secret show --name MySecret --vault-name MyKeyVault123 --query value -o tsv

This will display:  
ThisIsMySecretValue

### ✅ ****Summary****

* Created a Key Vault MyKeyVault123
* Stored secret MySecret
* Granted access permissions to manage secrets
* Retrieved the secret using CLI

### ****A. VM Backup Schedule + CPU Alert Rule****

### ****B. Backup Center Configuration + Retention Policy****

## 🔹 **A1. Schedule a Daily Backup of VM at 3:00 AM using Recovery Services Vault**

### ****Step 1: Create a Recovery Services Vault****

bash

CopyEdit

az backup vault create \

--resource-group MyResourceGroup \

--name MyRecoveryVault \

--location eastus

### ****Step 2: Register the VM with the Vault****

bash

CopyEdit

az backup protection enable-for-vm \

--resource-group MyResourceGroup \

--vault-name MyRecoveryVault \

--vm MyVM \

--policy-name DefaultPolicy

By default, Azure assigns the VM to the default backup policy.

### ****Step 3: Create a Custom Backup Policy to Run Daily at 3 AM****

bash

CopyEdit

az backup policy create \

--resource-group MyResourceGroup \

--vault-name MyRecoveryVault \

--name Daily3AMPolicy \

--policy "$(az backup policy get-default-policy --vault-name MyRecoveryVault --resource-group MyResourceGroup | jq '.properties | .schedulePolicy.scheduleRunTimes=["03:00:00"]')"

OR configure via Azure Portal:

* Go to **Recovery Services Vault > Backup policies**
* Click **+ Add**
* Name it: Daily3AMPolicy
* Frequency: Daily
* Time: **03:00 AM**
* Retention: e.g., 30 days
* Save

### ****Step 4: Assign Policy to the VM****

bash

CopyEdit

az backup protection backup-now \

--vault-name MyRecoveryVault \

--resource-group MyResourceGroup \

--container-name MyVM \

--item-name MyVM \

--retain-until 2025-12-31

## 🔹 **A2. Create Alert Rule for VM CPU > 80% and Send Email**

### ****Step 1: Go to Azure Portal > Virtual Machine > Monitoring > Alerts****

### ****Step 2: Click “+ New Alert Rule”****

* **Scope**: Select your VM
* **Condition**:
  + Signal name: Percentage CPU
  + Operator: Greater than
  + Threshold value: 80
  + Aggregation: Average over 5 minutes

### ****Step 3: Action Group****

* Click **Create New**
* **Name**: HighCPUAlertGroup
* **Notification**: Email
* **Email address**: your-email@example.com

### ****Step 4: Alert Rule****

* Name: HighCPUAlertRule
* Severity: 2 (Warning)
* Click **Create**

## 🔹 **B1. Provision Backups in Backup Center**

### ****Step 1: Open Azure Portal > Backup Center****

* Click **+ Backup**
* **Select Data Source**: Azure VM
* **Vault**: Select MyRecoveryVault
* **Policy**: Select Daily3AMPolicy
* **Select VM**: Choose MyVM
* Click **Enable Backup**

## 🔹 **B2. Configure Retention Period and Retain Old Backup**

### ****Step 1: Modify Backup Policy for Retention****

* Go to **Recovery Services Vault > Backup Policies**
* Edit Daily3AMPolicy
* Under **Retention Range**:
  + Daily Retention: e.g., **30 days**
  + Weekly/Monthly/Yearly as needed
* Save changes

### ****Step 2: Retain a Backup Manually****

bash

CopyEdit

az backup item list \

--resource-group MyResourceGroup \

--vault-name MyRecoveryVault \

--workload-type VM \

--output table

Then use:

bash

CopyEdit

az backup item show --vault-name MyRecoveryVault --name MyVM

Then:

bash

CopyEdit

az backup protection backup-now \

--vault-name MyRecoveryVault \

--resource-group MyResourceGroup \

--container-name <container-name> \

--item-name <item-name> \

--retain-until 2025-12-31

### ✅ Summary:

| **Task** | **Completed** |
| --- | --- |
| Create Vault & Backup Policy | ✅ |
| Schedule Backup at 3:00 AM | ✅ |
| Configure Email Alert for CPU > 80% | ✅ |
| Provision Backup from Backup Center | ✅ |
| Set Retention & Keep Old Backup | ✅ |