Lab 4: Azure Key Vault

Objective

1. Create an Azure Key Vault
2. Create a Secret
3. Create a GitHub Workflow to access the secret.
4. Add Access Permissions on Key vault.

Note:

1. Steps to log into VM (Each participant will have a separate user/pwd)
    a. Open in a private window https://training.datacouch.io/pluralsight
    b. Enter the provided username and password.

    All the following steps are to be done within the Virtual Machine.

    c. Steps to Log into Azure Portal (4-5 participants will be in each group)
        i. Go to https://portal.azure.com
        ii. Login with the supplied credentials (username and password).
            1. Each group has a unique integer for their login [1-4] eg. **usergroup[1-4]** that will remain same for the duration of the course.
            2. Complete username and Password will be provided in the class.
            3. Each usergroup has an associated resource group which is **rg-usergroup[1-4]**

Section 1: Create a Key Vault

Steps

1. Login into Azure Portal
2. Type **"Key vaults"** on the search bar.
3. Click on **"+Create"** button
4. **Basics Tab**
    a. Select the resource group from the dropdown.
    b. Give unique name to Key vault name as "**learnkeyvault"+"group number"+"participant id"** e.g. if your group number is 4 and participant id is 02 , name the key vault as **"learnkeyvault402".**
    c. Region: Select **"East US"**
    d. Pricing Tier: Select **"Standard"**

e. Days to retain deleted vaults: Enter **"7"**
f. Click on **"Next: Access policy"**

5. **Access policy Tab**
    a. Check the checkbox for all the options.
        i. Azure Virtual Machines for deployment
        ii. Azure Resource Manager for template deployment
        iii. Azure Disk Encryption for volume encryption
    b. Don't change the other defaults and click on **"Review + create"**
6. **Review+Create Tab**
    a. Let the validation run and pass.
    b. Click on **"Create"** and wait for the deployment to complete.
    c. Click on **"Go to resource"**. This will take you to the overview page of the newly created Key Vault

Section 2: Create a Secret

Steps

1. Login into Azure Portal
2. Type **"Key vaults"** on the search bar.
3. Select the newly created key vault.
4. Click on **Secrets** under Settings
5. Click on **"+Generate/import"**
    a. Upload Options: "Manual"
    b. Name: **<any name>**
    c. Value: **<any value>**
    d. Leave the other defaults and click on create.
6. You will see the secret created and with the status as enabled.
7. Click on **the secret name** and again click on the current version.
8. Click on **"Show Secret Value"** to reveal the secret value.

Section 3: Create a GitHub workflow

Steps

7. Login into the Virtual Machine
8. On the GitHub portal, go to the repo that you created in Lab1. You would need access to the Secret and variable that you have created in that repo. If you don't have that, please complete Lab1 till the portion of creating the Secret and variable.
9. Create a new file under ./github/workflows/ and name it **"AzureKeyVault.yml"** and copy and paste the following code.

```yaml
on: [workflow_dispatch]

name: AzureKeyVault

env:
  kvname: <replace this with the name of your key vault>
  secretname: <replace this with the name of your secret>

jobs:
  access-keyvault:
    runs-on: ubuntu-latest
    steps:
      - name: Login to Azure
        uses: azure/login@v1
        with:
          creds: '${{ secrets.AZURE_CREDENTIALS }}'

      - name: Access Secret from Key Vault
        uses: azure/CLI@v1
        with:
          azcliversion: latest
          inlineScript: |
            echo "Let's find the secret"
            az keyvault secret show --vault-name ${{ env.kvname }} -n ${{ env.secretname }} --query
value
```

10. We have configured this workflow to run manually. Click on Actions again. Then click on the workflow name **"AzureKeyVault"** and click on **"Run workflow**".
11. Wait for the workflow to start the job and it should fail. Review the error from the logs.

Section 4: Add Access Permissions on Key vault.

Steps

1. Go back to Azure Portal and the Key Vault
2. Click on **"Access policies"** on the right and click on **"+Create"**
3. Under Secret permissions, click on **"Select All"** and click on **"Next"**
4. Start typing the name of your service principal that you created for Azure login. Once you see that name, click on that name. Make sure that name comes under Selected item and click on "**Next**" couple of times.
5. Click on **"Create"** and you would see the service principal name came under Application with rights to Secrets.
6. Again, run the "AzureKeyVault" workflow and it should show the secret value now.

End of Lab.