Lab Document: Azure Key Vault

Lab Title

Azure Key Vault - Secure Management of Secrets, Keys, and Certificates

Objective

By the end of this lab, you will be able to:

- Create an Azure Key Vault
- Store and retrieve secrets securely
- Understand access control in Key Vault
- Use Key Vault with Azure identities

Prerequisites

- Active Azure Subscription
- Basic knowledge of Azure Portal
- Azure CLI or PowerShell installed (optional for CLI steps)

Lab Duration

45 - 60 minutes

Tasks to Perform

- 1. Create a Resource Group
- 2. Create an Azure Key Vault
- 3. Add a Secret to the Key Vault
- 4. Retrieve the Secret from the Key Vault
- 5. Configure Access Policies / RBAC
- 6. Test Secure Access

Step-by-Step Procedure

Task 1: Create a Resource Group

- 1. Log in to Azure Portal.
- 2. Search for **Resource Groups** → Click + Create.
- 3. Enter:
 - **Subscription**: Select your subscription.
 - Resource Group Name: KeyVaultLabRG.
 - **Region**: Select nearest region.
- 4. Click Review + Create → Create.

Task 2: Create an Azure Key Vault

- 1. In Azure Portal, search for **Key Vaults** → Click + **Create**.
- 2. Enter:
 - **Subscription**: Select your subscription.
 - Resource Group: Choose KeyVaultLabRG.
 - **Key Vault Name**: MyKeyVaultLab (must be unique).
 - Region: Same as resource group.
- 3. Under **Access Configuration**, select:
 - o Role-Based Access Control (RBAC) (recommended) OR
 - Vault Access Policy.
- 4. Click Review + Create → Create.

Task 3: Add a Secret

- 1. Open your newly created **Key Vault**.
- 2. From the left menu, select **Secrets** \rightarrow **+ Generate/Import**.
- 3. Enter details:
 - Name: DBPassword.
 - Value: MyStrongP@ssword123.
- 4. Click Create.

Task 4: Retrieve the Secret

Using Portal:

- 1. Go to the secret DBPassword.
- 2. Click on the current version.
- 3. Copy the Secret Value.

Using Azure CLI (optional):

az keyvault secret show --vault-name MyKeyVaultLab --name DBPassword --query value -o tsv

•

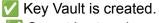
Task 5: Configure Access Control

- 1. Navigate to your Key Vault → Access Control (IAM).
- 2. Click + Add role assignment.
- 3. Assign role:
 - \circ Key Vault Secrets User \rightarrow Assign to your Azure AD user.
- 4. Save changes.

Task 6: Test Secure Access

- 1. Try to access the secret using a user with permissions.
- 2. Verify that without access policies, retrieval fails.

Validation



Secret is stored successfully.

Secret can be retrieved using authorized access.

✓ Unauthorized access is denied.

Cleanup (Optional)

To avoid unnecessary charges:

az group delete --name KeyVaultLabRG --yes --no-wait

Lab Summary

- Created a Key Vault in Azure.
- Stored and retrieved a secret.
- Configured access using Azure RBAC.
- Tested secure access management.