Create an azure key vault

1. Sign in to the Azure Portal:
   a. Open your web browser and navigate to the Azure Portal.
   b. Sign in with your Azure account credentials.
2. Create a New Key Vault:
   a. In the Azure Portal's left-hand navigation pane, click on "+ Create a resource".
   b. In the "Search the Marketplace" box, type "Key Vault" and select "Key Vault" from the list of results.
   c. Click the "Create" button to start the process.
3. Configure the Basic Settings:
   a. Subscription: Choose the Azure subscription you want to use.
   b. Resource Group: Either create a new resource group or select an existing one.
   c. Key Vault Name: Provide a unique name for your Key Vault.
   d. Region: Choose the desired Azure region where your Key Vault will reside.
4. Advanced Settings (optional):
   a. There are several tabs with additional settings you can configure:
   b. Pricing tier: Defines the type of the vault (standard or premium).
   c. Soft-delete: Determines if deleted items can be retained and recovered for a period.
   d. Purge Protection: If enabled, items can't be purged during the retention period.
   e. Virtual Network Service Endpoint: Restrict your Key Vault access to specified VNETs.
   f. Review these settings and adjust as necessary based on your specific needs.
5. Review + Create:
   a. After configuring the necessary settings, click the "Review + Create" button. Azure will validate the configuration.
   b. Once validation passes, click the "Create" button to deploy the Key Vault.
6. Access and Use Your Key Vault:
   a. Once the deployment is complete, navigate to your resource groups or search for the Key Vault by name in the Azure Portal.
   b. Inside the Key Vault, you can add secrets, keys, and certificates.

Setup shared access policies in key vault for an account

1. Access the Key Vault's Access Policies:
   a. Once inside your Key Vault, find the "Settings" section on the left-hand menu.
   b. Click on "Access policies".

2. Add a New Access Policy:
   a. Click on the "+ Add Access Policy" link.
3. Configure Permissions:
   a. Configure from template: This dropdown menu provides some predefined configurations, such as "Key & Secret Management" or "Secret Management". You can select one or choose to set the permissions manually.
   b. Key permissions, Secret permissions, Certificate permissions: Depending on what you want the account to have access to, you'll choose the respective permissions from these sections. For instance, you can allow an account to get and list secrets but not delete them.
4. Select a Principal:
   a. Click on the "Select principal" link.
   b. In the search box, type the name of the account you want to grant permissions to. This could be a user, group, or application.
   c. Select the account from the list and click on "Select".
5. Save the Access Policy:
   a. Click on the "Add" button at the bottom to add the access policy.
6. 8. Complete the Configuration:
   a. It's important to note that changes to access policies are not saved automatically. After adding the policy, you will be back on the "Access policies" page.
   b. Click on the "Save" button on the top of the "Access policies" section to save your changes.

Creating a Secret in Azure Key Vault

1. Access Secrets in the Key Vault:
   a. Once inside your Key Vault, find the "Secrets" section on the left-hand menu and click on it.
2. Create a New Secret:
   a. Click on the "+ Generate/Import" button at the top.
   b. Provide a "Name" for your secret.
   c. In the "Value" field, input the secret's content/value.
   d. (Optional) You can also configure other settings such as activation or expiration dates.
3. Click on the "Create" button.

Adding a New Version to an Existing Secret

1. Access the Specific Secret:

  a. Inside the "Secrets" section of your Key Vault, click on the name of the secret you want to add a new version to.
2. Add a New Version:
  a. On the secret's overview page, click on the "+ New Version" button at the top.
  b. Provide the "Value" for this new version of the secret.
  c. (Optional) Adjust other settings if necessary, such as activation or expiration dates.
3. Click on the "Create" button.

Use Logic Apps to receive email about status changes of key vault secrets

1. https://learn.microsoft.com/en-us/azure/key-vault/general/event-grid-logicapps