This Guide will help you creating an Azure Key Vault within the same resource group as the Azure App Service web app, configure access policies, and allow the web app to retrieve secrets.

Note: for the App Service web app creating part please grant the contributor permissions at the resource group level to the managed identity using the command below:

az role assignment create --assignee-principal-type ServicePrincipal --assignee-object-id $(az webapp identity show --name <app-name> --resource-group <resource-group> --query principalId --output tsv) --role "Contributor" --resource-group <resource-group>

creating an Azure Key Vault , please follow these steps using the Azure CLI:

1. **Create an Azure Key Vault:**

Replace **<key-vault-name>** with the name you want for your Key Vault and **<resource-group>** with the name of the existing resource group.

Command : az keyvault create --name <key-vault-name> --resource-group <resource-group> --location <location>

- **<location>**: Replace with the Azure region where you want to create the Key Vault.

2. **Create a Secret in the Key Vault:**

You can create a secret in your Key Vault using the **az keyvault secret set** command. Replace **<secret-name>** and **<secret-value>** with your own values.

Command : az keyvault secret set --name <secret-name> --vault-name <key-vault-name> --value <secret-value>

3. **Configure Access Policies:**

To grant your Azure App Service web app access to the Key Vault, add an access policy. Replace **<app-name>** with the name of your web app:

Command : az keyvault set-policy --name <key-vault-name> --object-id $(az webapp identity show --name <app-name> --resource-group <resource-group> --query principalId --output tsv) --secret-permissions get list

This command grants the web app access to **get** and **list** secrets. Adjust the permissions as needed based on your requirements.