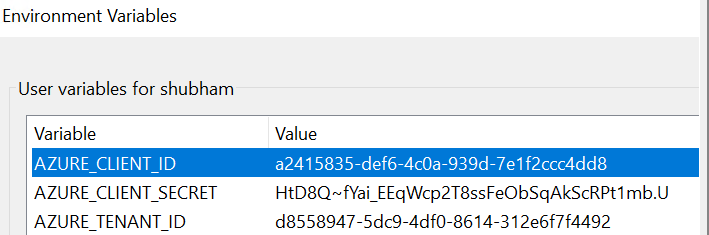
In this Files we are going to follow the steps which is required to connect dotnet core application connection string with Azure Key Vault.

Step-1

1. First create the app registration in Azure portal and generate the secret.
2. Create the Azure Key Vault .
3. Create the secret in Azure key vault and use Access configuration as Azure role-based access control .
4. Now add IAM Role and select role key value administrator and select member as a service principle which we have created in step1.

Step-2

1. If you are testing the application from visual studio and retrieving the app setting from Azure key vault then first you have environment variable for the Authentication .

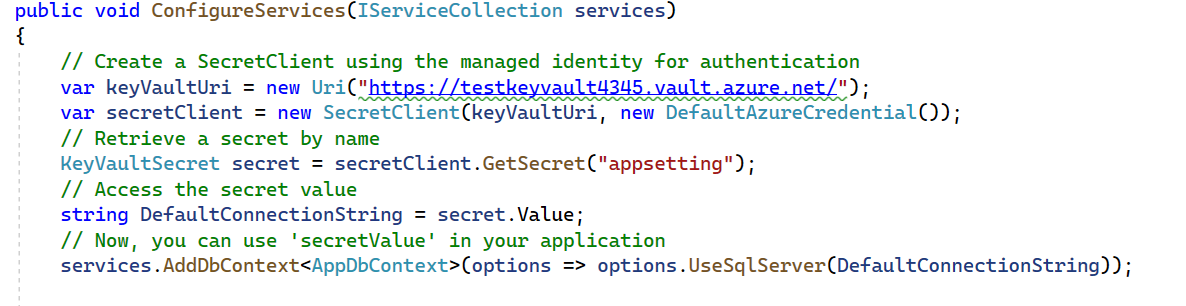


1. Next you have to install nuget package in your application.

Azure.Identity;

Azure.Security.KeyVault.Secrets;

1. Add below code in your startup.cs file.



// Create a SecretClient using the managed identity for authentication

var keyVaultUri = new Uri("https://testkeyvault4345.vault.azure.net/");

var secretClient = new SecretClient(keyVaultUri, new DefaultAzureCredential());

// Retrieve a secret by name

KeyVaultSecret secret = secretClient.GetSecret("appsetting");

// Access the secret value

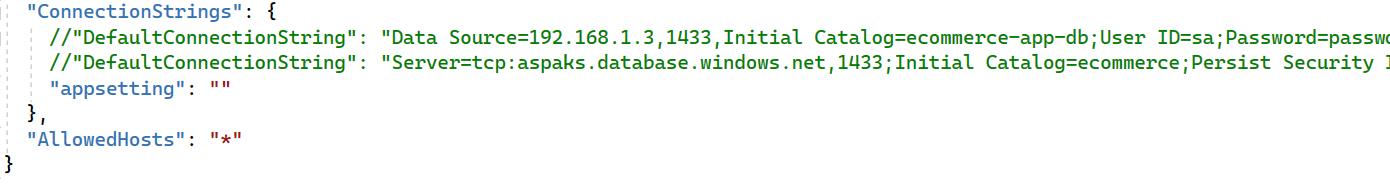
string DefaultConnectionString = secret.Value;

// Now, you can use 'secretValue' in your application

services.AddDbContext<AppDbContext>(options => options.UseSqlServer(DefaultConnectionString));

Here appsetting – is the secret name which you have created in key vault.

1. Next your appsetting.json file will be like this.



Here appsetting – is the secret name which you have created in key vault.