Access Azure Key Vault from On-prem using Service Principal and Managed (user-defined) Identity

Tuesday, January 5, 2021 1:53 PM

```
using System;
using Azure.Identity;
using Azure.Security.KeyVault.Secrets;

using Microsoft.Azure.Services.AppAuthentication;
using Microsoft.Azure.KeyVault;


namespace KeyVaultAccessor
{
   class Program
   {
      /**
       * BEFORE YOU BEGIN:
       *  TO USE DefaultAzureCredential, SET ENVIRONMENT VARIABLES
       * OPTION 1: Using Service Principal
       *  Create a Key Vault in Azure
       *  Create a Service Principal
       *  Get its Application (client) ID, Client Secret and Get Directory (tenant) ID
       *  Set local environment variables as shown below:
       *  AZURE_TENANT_ID = Directory (tenant) ID
       *  AZURE_CLIENT_ID = Application (client) ID
       *  AZURE_CLIENT_SECRET= Client Secret
       * OPTION 2: Using user-defined Managed Identity
       *  Get its Client ID, Object ID and Get Directory (tenant) ID
       *  Set local environment variables as shown below:
       *  AZURE_TENANT_ID = Directory (tenant) ID
       *  AZURE_CLIENT_ID = Client ID
       *  AZURE_OBJECT_ID = Object ID
       */

      static void Main(string[] args)
      {
         var keyVaultUrl = "https://dc1-keyvault11.vault.azure.net/";

         var client = new SecretClient(new Uri(keyVaultUrl), new DefaultAzureCredential());

         string secretName = $"BankAccountPassword-{Guid.NewGuid()}";

         var secret = new KeyVaultSecret(secretName, "f4G34fMh8v");
         secret.Properties.ExpiresOn = DateTimeOffset.Now.AddYears(1);

         client.SetSecret(secret);

        var answer = client.GetSecret(secretName);

         Console.WriteLine("The END");
      }
   }
}
```