

# Protect Script Secrets with Azure Key Vault

Azure includes several services to help protect secret information for our applications and scripts. Within this hands-on lab, we'll be working with managed identities and key vault.

Managed identities help us to provide an Azure Active Directory (AD) identity for Azure resources we manage. We can then use this identity to securely access some Azure services, such as key vault.

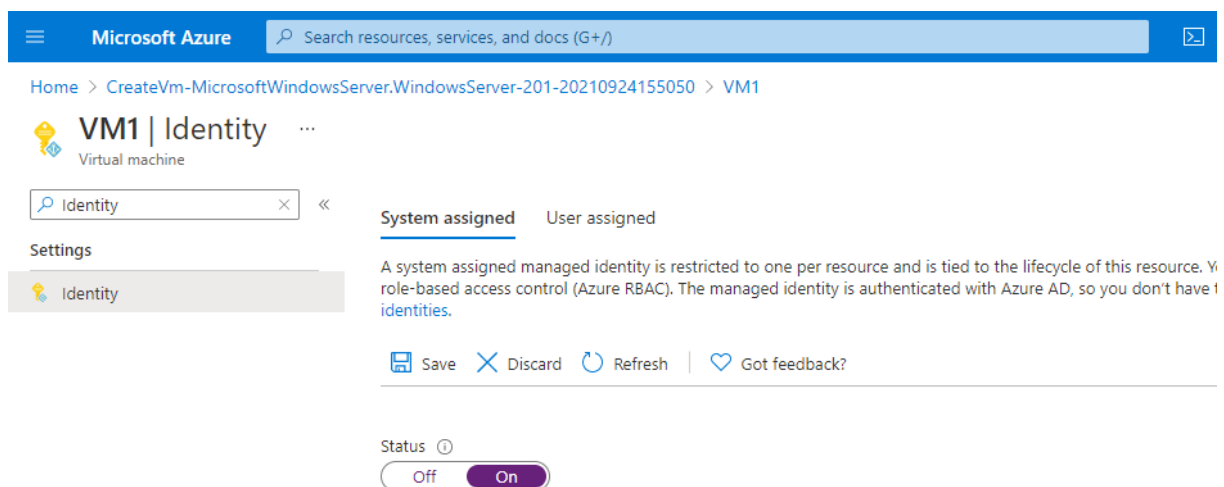
After completing this lesson, you will become familiar with how we can securely store secret information within a key vault, and then access that information securely from an Azure virtual machine.

## 1- Configure a Managed Identity for VM1

Configure a Managed Identity for VM1 by completing the following:

1- Navigate to the virtual machine, vm1, which has been created for you. You may search for vm1, access via all resources, or through the 'Virtual Machines' service page.

2- Click on Identity in the Settings section of the resource menu on the left-hand side.



3- Click System assigned within the working pane (middle of the screen) and change the Status to On.

4- Click Save, then click Yes.

## 2- Configure a Key Vault

Create a Key Vault:

- 1- Click on the + Create a resource option.
- 2- Search for key vault.
- 3- Choose the key vault option, then click on Create.
- 4- Create the key vault with the following settings:

- **Basics**

- Subscription: Select the existing subscription
- Resource group: Select the existing resource group
- Name: labkeyvault + 4 unique characters (e.g., labkeyvaultxx11)
- Region: Select the region in use for your existing resources
- Pricing tier: Standard
- Click Next.

- **Access policy**

- Click Add Access Policy
- Template: Key, Secret, & Certificate Management
- Select principal: vm1
- Click Add.

- 5- Click on Review + create >> Create.

### 3- Connect to VM1 using RDP

- 1- Navigate to the Virtual Machines services page.
- 2- Open the existing VM called vm1.
- 3- Click on the Connect option in the command bar and select RDP.
- 4- Use the RDP file with your preferred RDP client.

Note: you may choose to copy the public IP address and connect via RDP manually with your RDP client, instead of using the RDP file.

### Install Azure CLI

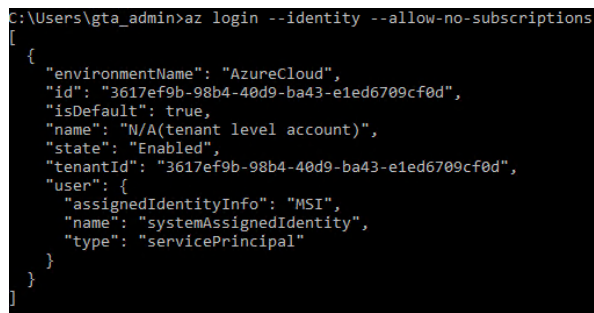
- 1- Right-click on the Start Menu then choose Run.
- 2- Type "**powershell**" and press enter.
- 3- Run the following command: **[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12**
- 4- Run the following command: **Invoke-WebRequest -Uri https://aka.ms/installazurecliwindows -OutFile \$home\Desktop\AzureCLI.msi.**
- 5- Run the following command: **Start-Process msixexec.exe -Wait -ArgumentList "/I \$home\Desktop\AzureCLI.msi /quiet".**
- 6- Type exit and press Enter.

## Copy the Key Vault Details

- 1- Navigate to the Key Vaults section in the Azure Portal.
- 2- Open the Key Vault you just created.
- 3- Copy the DNS Name from the working pane (middle of the screen) as we will use it in the next section.

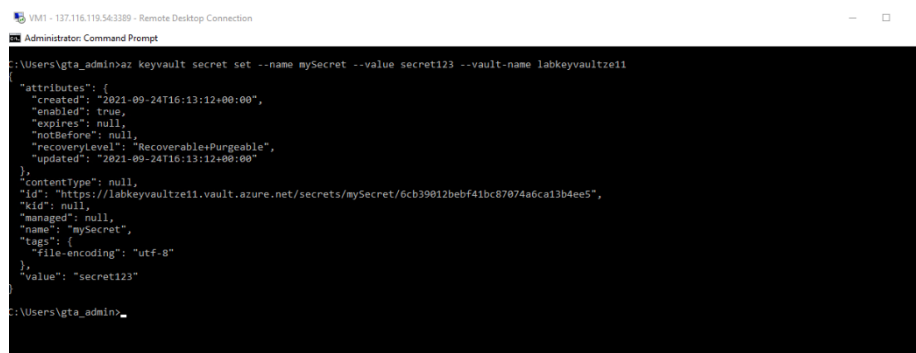
## 4- Test Key Vault using Azure CLI

- 1- Right-click on the Start Menu then choose Run.
- 2- Type cmd and press Enter.
- 3- Login using the managed identity: **az login --identity --allow-no-subscriptions**



```
C:\Users\gta_admin>az login --identity --allow-no-subscriptions
{
  "environmentName": "AzureCloud",
  "id": "3617ef9b-98b4-40d9-ba43-e1ed6709cf0d",
  "isDefault": true,
  "name": "N/A(tenant level account)",
  "state": "Enabled",
  "tenantId": "3617ef9b-98b4-40d9-ba43-e1ed6709cf0d",
  "user": {
    "assignedIdentityInfo": "MSI",
    "name": "systemAssignedIdentity",
    "type": "servicePrincipal"
  }
}
```

- 4- Type: **az keyvault secret set --name mySecret --value secret123 --vault-name labkeyvaultze11** (use the name of the Key Vault you created earlier)



```
Administrator: Command Prompt
C:\Users\gta_admin>az keyvault secret set --name mySecret --value secret123 --vault-name labkeyvaultze11
{
  "attributes": {
    "created": "2021-09-24T16:13:12+00:00",
    "enabled": true,
    "expires": null,
    "notBefore": null,
    "recoveryLevel": "Recoverable+Purgeable",
    "updated": "2021-09-24T16:13:12+00:00"
  },
  "contentType": null,
  "id": "https://labkeyvaultze11.vault.azure.net/secrets/mySecret/6cb39012bebf41bc87074a6ca13b4ee5",
  "kid": null,
  "managed": null,
  "name": "mySecret",
  "tags": {
    "file-encoding": "utf-8"
  },
  "value": "secret123"
}
```

- 5- Type: **az keyvault secret show --name mySecret --vault-name labkeyvaultze11**



```
Value: secret123
C:\Users\gta_admin>az keyvault secret show --name mySecret --vault-name labkeyvaultze11
{
  "attributes": {
    "created": "2021-09-24T16:13:12+00:00",
    "enabled": true,
    "expires": null,
    "notBefore": null,
    "recoveryLevel": "Recoverable+Purgeable",
    "updated": "2021-09-24T16:13:12+00:00"
  },
  "contentType": null,
  "id": "https://labkeyvaultze11.vault.azure.net/secrets/mySecret/6cb39012bebf41bc87074a6ca13b4ee5",
  "kid": null,
  "managed": null,
  "name": "mySecret",
  "tags": {
    "file-encoding": "utf-8"
  },
  "value": "secret123"
}
```