Lab-Using Azure Key Vault for Managed Identities

Lab scenario

When you use managed identities for Azure resources, your code can get access tokens to authenticate to resources that support Azure AD authentication.  However, not all Azure services support Azure AD authentication. To use managed identities for Azure resources with those services, store the service credentials in Azure Key Vault, and use the managed identity to access Key Vault to retrieve the credentials.

Estimated time: 20 minutes

Exercise 1 - Use Azure Key Vault to manage Virtual Machine identities

Task 1 - Create a Windows Virtual Machine

1. Browse to the [https://portal.azure.com](https://portal.azure.com/)
2. Select **+ Create a resource**.
3. Type **Windows Server** in Search the Marketplace search bar.
4. Select **Windows Server** and choose **Windows Server 2019 Datacenter** from Select a software plan dropdown.
5. You will have to create an administrator username and password for the VM on the basics tab.
6. On the **Management** tab, check the box to Login with Azure AD under the Azure AD section.
7. Go through the rest of the experience of creating a virtual machine.
8. Select Create.

Task 2 - Create a Key Vault

1. Sign in to the [https://portal.azure.com](https://portal.azure.com/) using a Global administrator account.
2. At the top of the left navigation bar, select Create a resource
3. In the Search the Marketplace box type in **Key Vault**.
4. Select **Key Vault** from the results.
5. Select **Create**.
6. Fill out all required information as shown below. Make sure that you choose the subscription that you’re using for this lab.

* **Resource group** - sc300KeyVaultrg
* **Key vault name** - sc300keyvault

1. Select **Review + create**.
2. Select **Create**.

Task 3 - Create a secret

1. Navigate to your newly created Key Vault.
2. Select **Secrets**.
3. Select **+ Generate/Import**.
4. In the Create a secret screen, from Upload options leave **Manual** selected.
5. Enter a name and value for the secret. The value can be anything you want.
6. Leave the activation date and expiration date clear, and leave Enabled as Yes.
7. Select **Create** to create the secret.

Task 4 - Grant access to Key Vault

1. Navigate to your newly created Key Vault
2. Select **Access Policies** from the menu on the left side.
3. Select **Add Access Policy**.
4. In the Add access policy section, under Configure from template (optional), choose Secret Management from the pull-down menu.
5. For **Select Principal**, choose **None selected** to open the list of principals to select. In the search field enter the name of the VM you created in task 2. Select the VM in the result list and choose Select.
6. Select **Add**.
7. Select **Save**.

Task 5 - Access data with Key Vault secret with PowerShell

1. In the lab virtual machine, open PowerShell.
2. In PowerShell, invoke the web request on the tenant to get the token for the local host in the specific port for the VM.

CodeCopy

$Response = Invoke-RestMethod -Uri 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https%3A%2F%2Fvault.azure.net' -Method GET -Headers @{Metadata="true"}

1. Next, extract the access token from the response.

CodeCopy

$KeyVaultToken = $Response.access\_token

1. Use PowerShell’s Invoke-WebRequest command to retrieve the secret you created earlier in the Key Vault, passing the access token in the Authorization header. You’ll need the URL of your Key Vault, which is in the Essentials section of the Overview page of the Key Vault.

CodeCopy

Invoke-RestMethod -Uri https://<your-key-vault-URL>/secrets/<secret-name>?api-version=2016-10-01 -Method GET -Headers @{Authorization="Bearer $KeyVaultToken"}

1. You should receive a response that looks like the following:

CodeCopy

'My Secret' https://mi-lab-vault.vault.azure.net/secrets/mi-test/50644e90b13249b584c44b9f712f2e51 @{enabled=True; created=16…

1. This secret can be used to authenticate to services that require a name and password.