Managing Identities

Lab: Implementing user-assigned managed identities for Azure resources

Scenario

Adatum Corporation wants to use managed identities to authenticate applications running in Azure VMs

Objectives

After completing this lab, you will be able to:

- Create and configure user-assigned managed identities
- Validate functionality of user-assigned managed identities

Lab Setup

Estimated Time: 30 minutes

User Name: **Student**

Password: **Pa55w.rd**

Exercise 1: Creating and configuring a user-assigned managed identity.

The main tasks for this exercise are as follows:

1. Deploy an Azure VM running Windows Server 2016 Datacenter
2. Create a user-assigned managed identity.
3. Assign the user-assigned managed identity to the Azure VM.
4. Grant RBAC-based permissions to the user-assigned managed identity.

Task 1: Deploy an Azure VM running Windows Server 2016 Datacenter

1. From the lab virtual machine, start Microsoft Edge and browse to the Azure portal at **http://portal.azure.com** and sign in by using the Microsoft account that has the Owner role in the target Azure subscription.
2. In the Azure portal, in the Microsoft Edge window, start a **Bash** session within the **Cloud Shell**.
3. If you are presented with the **You have no storage mounted** message, configure storage using the following settings:
    - Subscription: the name of the target Azure subscription
    - Cloud Shell region: the name of the Azure region that is available in your subscription and which is closest to the lab location
    - Resource group: **az3000500-LabRG**
    - Storage account: a name of a new storage account
    - File share: a name of a new file share
4. From the Cloud Shell pane, create a resource group by running (replace the `<Azure region>` placeholder with the name of the Azure region that is available in your subscription and which is closest to the lab location)

```
az group create --resource-group az3000501-LabRG --location <Azure region>
```

5. From the Cloud Shell pane, upload the Azure Resource Manager template **\allfiles\AZ-300T01\Module_05\azuredeploy05.json** into the home directory.
6. From the Cloud Shell pane, upload the parameter file **\allfiles\AZ-300T01\Module_05\azuredeploy05.parameters.json** into the home directory.
7. From the Cloud Shell pane, deploy an Azure VM hosting Windows Server 2016 Datacenter into the first virtual network by running:

```
az group deployment create --resource-group az3000501-LabRG --template-file
azuredeploy05.json --parameters @azuredeploy05.parameters.json
```

> Note: Wait for the deployment to complete. This might take about 5 minutes.

Task 2: Create a user-assigned managed identity and assign it to the Azure VM.

1. From the Cloud Shell pane, run the following to create a user-assigned managed identity:

```
az identity create --resource-group az3000501-LabRG --name az3000501-mi
```

2. From the Cloud Shell pane, run the following to assign the user-assigned managed identity to the Azure VM:

```
az vm identity assign --resource-group az3000501-LabRG --name az3000501-vm
--identities az3000501-mi
```

Task 3: Configure RBAC referencing the user-assigned managed identity.

1. From the Cloud Shell pane, run the following to create a resource group (replace the <Azure region> placeholder with the name of the Azure region into which you deployed the Azure VM in this exercise):

```
az group create --resource-group az3000502-LabRG --location <Azure region>
```

2. In the Azure portal, navigate to the **az3000502-LabRG - Access control (IAM)** blade.
3. From the **az3000502-LabRG - Access control (IAM)** blade, assign the Owner role to the newly created user-assigned managed identity.

> Result: After you completed this exercise, you have created and configured a user-assigned managed identity.

Exercise 2: Validating functionality of user-assigned managed identities

The main tasks for this exercise are as follows:

1. Configure an Azure VM for authenticating via user-assigned managed identity.
2. Validate functionality of user-assigned managed identity from the Azure VM.

Task 1: Configure an Azure VM for authenticating via user-assigned managed identity.

1. In the Azure portal, navigate to the **az3000501-vm** blade.
2. Connect to the Azure VM by using Remote Desktop and authenticate by providing the following credentials:
    - Username: **Student**

- Password: **Pa55w.rd1234**

3. Once you establish a Remote Desktop session, you will be presented with an **Administrator: C:\Windows\system32\cmd.exe** window. To start a PowerShell session, at the command prompt, type `PowerShell` and press Enter.
4. From the PowerShell prompt, run the following to install the latest version of the PowerShellGet module (press Enter if prompted for confirmation):

```
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
Install-Module -Name PowerShellGet -Force -SkipPublisherCheck
```

5. From the PowerShell prompt, run the following to install the latest version of the Az module (type **Y** and press Enter when prompted for confirmation):

```
Install-Module -Name Az -AllowClobber -SkipPublisherCheck
```

6. Exit the current PowerShell session by typing `exit` and pressing Enter and then start it again by typing at the command prompt `PowerShell` and pressing Enter.
7. From the PowerShell prompt, run the following to install the AzureRM.ManagedServiceIdentity module:

```
[Net.ServicePointManager]::SecurityProtocol =
[Net.SecurityProtocolType]::Tls12
Install-Module -Name PowerShellGet -AllowPrerelease -SkipPublisherCheck
```

8. From the PowerShell prompt, run the following to install the the pre-release version of the AzureRM.ManagedServiceIdentity module:

```
Install-Module -Name Az.ManagedServiceIdentity
```

Task 2: Validate functionality of user-assigned managed identity from the Azure VM.

1. From the PowerShell prompt, run the following to sign-in as the user-assigned managed identity:

```
Add-AzAccount -Identity
```

2. From the PowerShell prompt, run the following to attempt to retrieve the currently used managed identity:

```
(Get-AzVM -ResourceGroupName az3000501-LabRG -Name az3000501-vm).Identity
```

3. Note the error message. As the message states, the current security context does not grant sufficent authorization to the target resource. To resolve this issue, switch to the Azure portal, navigate to the **az3000501-LabRG - Access control (IAM)** blade.
4. From the **az3000501-LabRG - Access control (IAM)** blade, assign the Contributor role to the user-assigned managed identity **az3000501-mi**.
5. Switch back to the Remote Desktop session, and, from the PowerShell prompt, run the following to attempt to retrieve the currently used managed identity:

```
(Get-AzVM -ResourceGroupName az3000501-LabRG -Name az3000501-vm).Identity
```

> Note: If you receive an error message indicating insufficient privileges, from the PowerShell prompt, run

```
Remove-AzAccount
```

followed by:

```
Add-AzAccount -Identity
```

```
```

1. From the PowerShell prompt, run the following to store location in a variable:

   ```
   $location = (Get-AzResourceGroup -Name az3000502-LabRG).Location
   ```

2. From the PowerShell prompt, run the following to create a public IP address resource:

   ```
   New-AzPublicIpAddress -Name az3000502-pip -ResourceGroupName az3000502-LabRG -AllocationMethod Dynamic -Location $location
   ```

3. Verify that the command completed successfully.

> Result: After you completed this exercise, you have validated the functionality of the user-defined managed identity.

Exercise 3: Remove lab resources

Task 1: Open Cloud Shell

1. At the top of the portal, click the **Cloud Shell** icon to open the Cloud Shell pane.
2. At the **Cloud Shell** command prompt, type in the following command and press **Enter** to list all resource groups you created in this lab:

   ```
   az group list --query "[?starts_with(name,'az30005')].name" --output tsv
   ```

3. Verify that the output contains only the resource groups you created in this lab. These groups will be deleted in the next task.

Task 2: Delete resource groups

1. At the **Cloud Shell** command prompt, type in the following command and press **Enter** to delete the resource groups you created in this lab

   ```
   az group list --query "[?starts_with(name,'az30005')].name" --output tsv | xargs -L1 bash -c 'az group delete --name $0 --no-wait --yes'
   ```

2. Close the **Cloud Shell** prompt at the bottom of the portal.

> Result: In this exercise, you removed the resources used in this lab.