**Lab 14: Azure Managed Identities**

**Introduction:**

Managed identities in Azure offer a secure way for Azure resources to authenticate and authorize without requiring credentials or secrets stored in the code. There are two types of managed identities: system-assigned and user-assigned. In this lab, we will explore how to enable both types and how to use them for authentication. The objective of this lab is to understand how to securely access Azure services using managed identities and configure them for optimal use.

**Objectives:**

* Enable a system-assigned managed identity on an Azure VM.
* Create and associate a user-assigned managed identity.
* Authenticate using managed identities and the Azure Identity library in Python.

**Steps:**

**Part 1: Enabling a System-Assigned Managed Identity**

**Step 1:** Access the Azure VM Resource (it is named drlee)

* **Explanation**: This type of managed identity is directly tied to the resource's lifecycle.
* **How to Do It**: In the Azure portal, search for your VM by typing "Virtual Machines" in the search bar and select the VM you want to enable the managed identity for.

**Step 2:** Enable the Managed Identity

* **Explanation**: Enabling the identity allows the VM to authenticate with Azure services securely.
* **How to Do It**:
  + In the VM's left-hand menu, click on "Identity."
  + In the "System assigned" tab, toggle the Status to "On."
  + Click "Save" to enable the managed identity.

**Step 3:** Verify the Identity

* **Explanation**: Ensure that the managed identity has been created successfully.
* **How to Do It**: In the "Identity" tab, you should see the managed identity information like object ID and principal ID.

**Part 2: Creating and Associating a User-Assigned Managed Identity**

**Step 1:** Create the User-Assigned Managed Identity

* **Explanation**: User-assigned identities can be used across multiple resources.
* **How to Do It**:
  + In the Azure portal, search for "Managed Identities."
  + Click "Create" to start a new managed identity.
  + Provide a name, subscription, and resource group, then click "Create."

**Step 2:** Associate the User-Assigned Managed Identity

* **Explanation**: Associating it with a resource allows that resource to use the identity for authentication.
* **How to Do It**:
  + Navigate back to the VM's "Identity" tab.
  + Click the "User assigned" tab, then "Add."
  + Select the identity you created from the list and click "Add" to associate it.

**Part 3: Using Managed Identities with Python (Optional – Do not do)**

**Step 1:** Set Up Your Python Environment

* **Explanation**: The Azure Identity library simplifies authentication using managed identities.
* **How to Do It**:
  + Install the Azure Identity library using pip:

pip install azure-identity

**Step 2:** Authenticate Using DefaultAzureCredential

* **Explanation**: This class automatically detects the right authentication method based on the environment.
* **How to Do It**: In your Python code, use the following:

from azure.identity import DefaultAzureCredential credential = DefaultAzureCredential() token = credential.get\_token("https://management.azure.com/.default")

* This script retrieves an authentication token using the managed identity.

**Step 3:** Work with Azure Machine Learning

* **Explanation**: Once authenticated, you can use the obtained token to interact with Azure services, such as Machine Learning.
* **How to Do It**: Use the **credential** object to make authenticated requests to Azure Machine Learning services.

**Summary:**

In this lab, you learned how to enable system-assigned and user-assigned managed identities and how to authenticate using the Azure Identity library. Managed identities provide a secure way to manage access to Azure resources, ensuring compliance and security for your applications and workloads.