**Lesson 5 Demo 3**

**Azure Monitor**



**Steps to be followed:**

1. Deploying an Azure virtual machine
2. Creating a Log Analytics workspace
3. Enabling the Log Analytics virtual machine extension
4. Collecting virtual machine event and performance data
5. Viewing and querying collected data

**Step 1: Deploying an Azure virtual machine**

1. Sign in to the Azure portal <https://portal.azure.com/>
2. Open the Cloud Shell by clicking the first icon in the top right of the Azure Portal. If prompted, select **PowerShell,** and then select **Create storage**Graphical user interface, application

   Description automatically generatedGraphical user interface, text

   Description automatically generated

Graphical user interface, text, application

Description automatically generated

1. In the PowerShell session within the Cloud Shell pane, run the following to create a resource group that will be used in this lab:

**New-AzResourceGroup -Name AZ305LAB131415 -Location 'EastUS'**

Text

Description automatically generated

1. Now, run the following command to create a new Azure virtual machine:

**New-AzVm -ResourceGroupName "AZ305LAB131415" -Name "myVM" -Location 'EastUS' -VirtualNetworkName "myVnet" -SubnetName "mySubnet" -SecurityGroupName "myNetworkSecurityGroup" -PublicIpAddressName "myPublicIpAddress" -OpenPorts 80,3389**

1. When prompted, provide the username and password and press enter

Text

Description automatically generated

1. Run the following command to verify the virtual machine is created and its provisioning state is succeeded:

**Get-AzVM -Name 'myVM' -ResourceGroupName 'AZ305LAB131415' | Format-Table**

**Step 2: Creating a Log Analytics workspace**

1. Type **Log Analytics workspaces** in the search bar and select it

Graphical user interface, text, application, email

Description automatically generated

1. On the Log Analytics workspaces blade, click **+ Create**

Graphical user interface, text, application, email

Description automatically generated

Specify the following settings (leave others with their default values):

**Subscription: The name of the Azure subscription you are using in this lab**

**Resource group: AZ305LAB131415**

**Name: Any valid and globally unique name**

**Region: (US) East US**

1. Click on **Review + Create**

Graphical user interface, text, application

Description automatically generated

1. After the validation passes, click on **Create**

Graphical user interface, text, application

Description automatically generated

**Step 3: Enabling the Log Analytics virtual machine extension**

1. Click on **Go to resource**

Graphical user interface, text, application, email

Description automatically generated

1. Locate the Azure VM that you created (**myVM**) and select it

Graphical user interface, application

Description automatically generated

1. Click on **Connect**

Graphical user interface, text, application, email

Description automatically generated



Graphical user interface, text, application

Description automatically generated

**Step 4: Collecting virtual machine event and performance data**

1. Navigate back to the Log Analytics workspace you created earlier
2. In the **Settings** section, select **Agents configuration** and then click on **+ Add windows event log**

Graphical user interface, text, application, email

Description automatically generated

1. In the listing of event log types, select **System,** uncheck the information boxand then clickon **Apply**

Graphical user interface, text

Description automatically generated



1. Go to the **Windows Performance Counters**, click **+ Add performance counter**, review the listing of available performance counters, and add the following ones:

**Process(\*)\% Processor Time**

**Event Tracing for Windows\Total Memory Usage — Non-Paged PoolEvent Tracing for Event Tracing for Windows\Total Memory Usage — Paged Pool**

Graphical user interface, text, application

Description automatically generated

**Step 5: Viewing and querying collected data**

1. Navigate back to the **Log Analytics workspace** you created earlier
2. Go to the **General** section and then select **Logs**

Graphical user interface, application

Description automatically generated

1. In the **All Queries** column, scroll down and select **Virtual Machines**

Graphical user interface, text, application, email

Description automatically generated

1. Review the list of predefined queries, identify the one you want to test, and click the corresponding **Run** button

Graphical user interface, text, application

Description automatically generated

The query will automatically open in a new query tab.

Graphical user interface, text, application, chat or text message

Description automatically generated

You successfully monitored the use of the Log Analytics workspace to configure data sources and query logs.