ASSIGNMENT ONE: AZURE FIREWALL WRITEUP

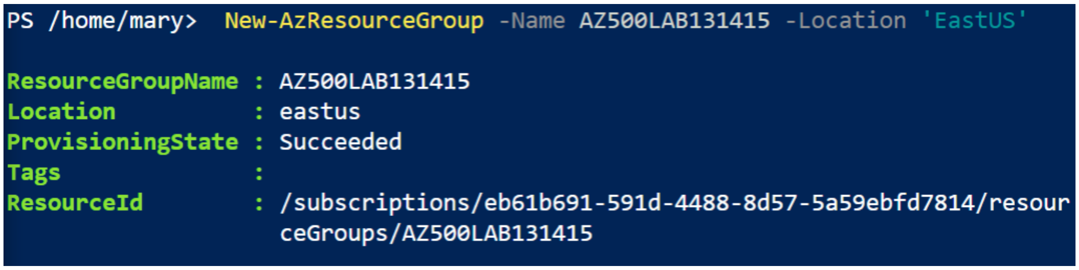
BY CS-CNS03-23082 – ABUOR ISABELLA MERCY

INTRODUCTION

This guided exercise embarks on a journey through five pivotal tasks, each unlocking a new facet of Azure's monitoring prowess. Starting with the deployment of an Azure virtual machine, the journey navigates through the creation of a Log Analytics workspace, the enabling of the Log Analytics virtual machine extension, and culminates in the collection, visualization, and querying of invaluable event and performance data. By the end of this exercise, you'll possess the skills to harness Azure Monitor's capabilities in harmonizing data collection and analysis, empowering you to make informed decisions for a seamlessly optimized virtual machine environment.

Task 1: Deploy an Azure virtual machine

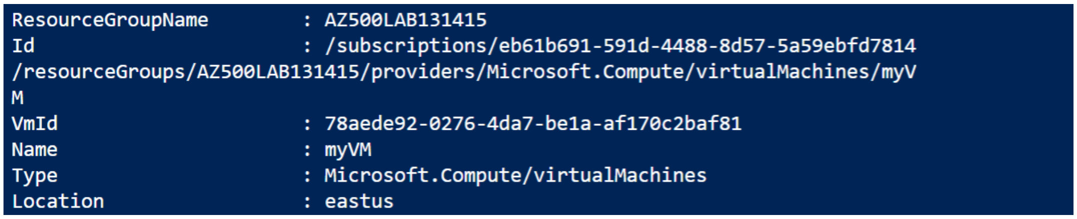
I this task deployment of the azure virtual machine was done through Cloud Shell by running the following to create a resource group that will be used in this lab:



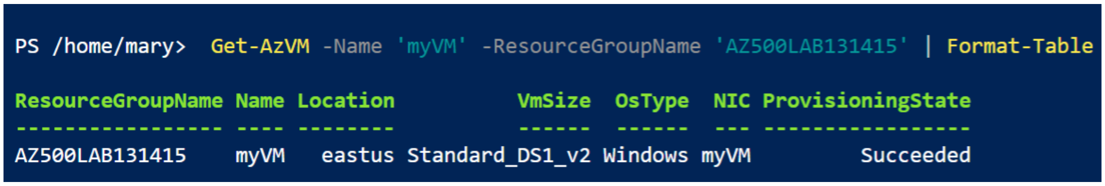
```
PS /home/mary>  New-AzResourceGroup -Name AZ500LAB131415 -Location 'EastUS'

ResourceGroupName : AZ500LAB131415
Location          : eastus
ProvisioningState : Succeeded
Tags              :
ResourceId        : /subscriptions/eb61b691-591d-4488-8d57-5a59ebfd7814/resour
                    ceGroups/AZ500LAB131415
```

then within the Cloud Shell pane, a new Azure virtual machine was created and below is the confirmation that the virtual machine named myVM was created and its ProvisioningState is Succeeded.



```
ResourceGroupName        : AZ500LAB131415
Id                       : /subscriptions/eb61b691-591d-4488-8d57-5a59ebfd7814
/resourceGroups/AZ500LAB131415/providers/Microsoft.Compute/virtualMachines/myV
M
VmId                     : 78aede92-0276-4da7-be1a-af170c2baf81
Name                     : myVM
Type                     : Microsoft.Compute/virtualMachines
Location                 : eastus
```

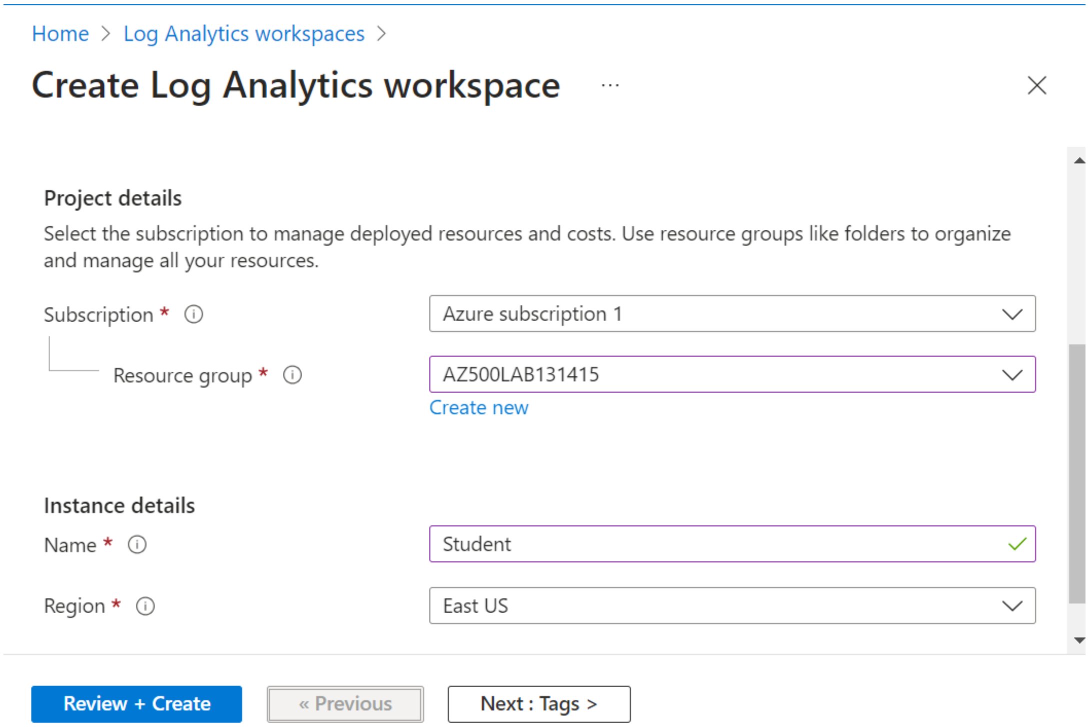


```
PS /home/mary>  Get-AzVM -Name 'myVM' -ResourceGroupName 'AZ500LAB131415' | Format-Table

ResourceGroupName Name Location          VmSize  OsType  NIC ProvisioningState
----------------- ---- --------          ------  ------  --- -----------------
AZ500LAB131415    myVM   eastus Standard_DS1_v2 Windows myVM         Succeeded
```

Task 2: Create a Log Analytics workspace

In this task, we created a Log Analytics workspace on the Log Analytics workspaces blade and on the Basics tab of the Create Log Analytics workspace blade, the following settings were specified.



Create Log Analytics workspace

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Azure subscription 1

Resource group * : AZ500LAB131415

Instance details

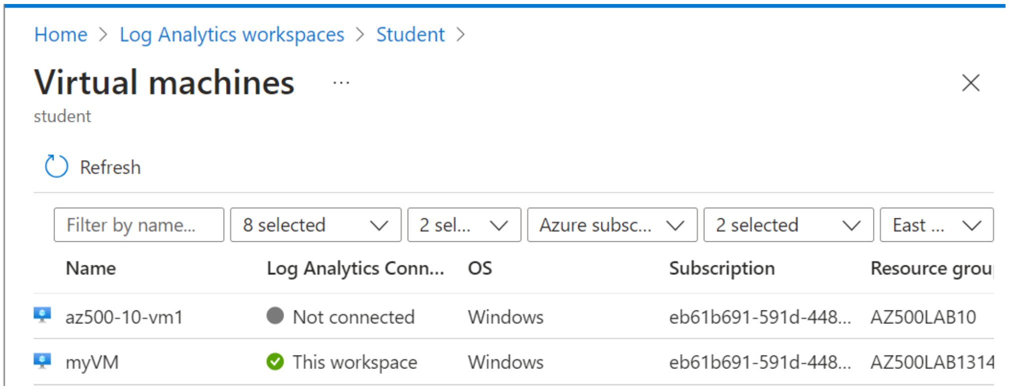
Name * : Student

Region * : East US

Task 3: Enable the Log Analytics virtual machine extension

In this task, we enabled the Log Analytics virtual machine extension. This extension installs the Log Analytics agent on Windows and Linux virtual machines. This agent collects data from the virtual machine and transfers it to the Log Analytics workspace that you designate. Once the agent is installed it will be automatically upgraded ensuring you always have the latest features and fixes.

On the Log Analytics workspaces blade, and, on the entry representing the workspace you created in the previous task. On the Overview page, in the Connect a Data Source section, in the Azure Virtual machines (VMs) entry we connected the myVM as shown below:



Home > Log Analytics workspaces > Student >

Virtual machines ···

student

Refresh

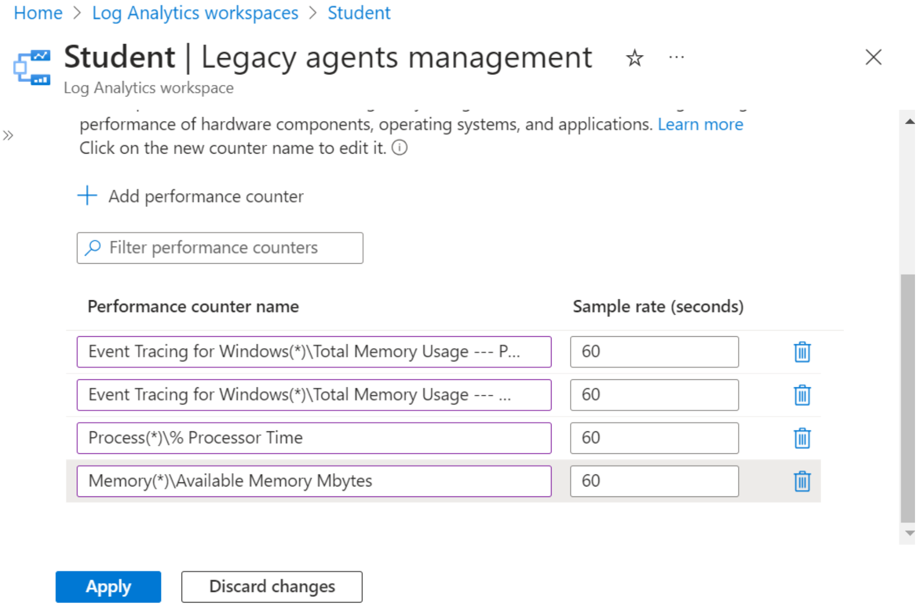
Filter by name... | 8 selected | 2 sel... | Azure subsc... | 2 selected | East ...

Name	Log Analytics Conn...	OS	Subscription	Resource grou
az500-10-vm1	● Not connected	Windows	eb61b691-591d-448...	AZ500LAB10
myVM	✓ This workspace	Windows	eb61b691-591d-448...	AZ500LAB1314

Task 4: Collect virtual machine event and performance data

In this task, we configured the collection of the Windows System log and several common performance counters and also review other sources that are available.

On the Log Analytics workspace you created earlier in this exercise in the Classic section, clicked Legacy agents management, reviewed the configurable settings. We then added windows event log.



Home > Log Analytics workspaces > Student

Student | Legacy agents management ☆ ···

Log Analytics workspace

performance of hardware components, operating systems, and applications. Learn more

Click on the new counter name to edit it. ⓘ

+ Add performance counter

Filter performance counters

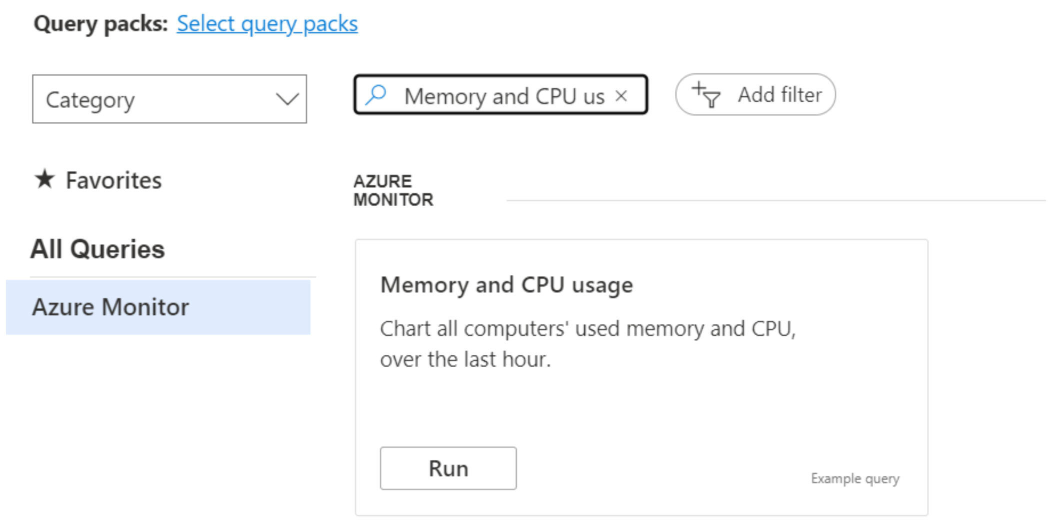
Performance counter name	Sample rate (seconds)
Event Tracing for Windows(*)\Total Memory Usage --- P...	60
Event Tracing for Windows(*)\Total Memory Usage --- ...	60
Process(*)\% Processor Time	60
Memory(*)\Available Memory Mbytes	60

Apply | Discard changes

Task 5: View and query collected data

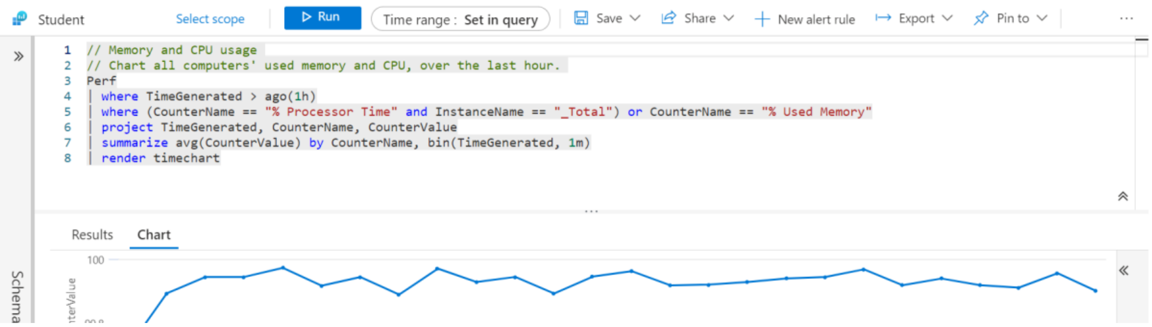
In this task, we ran a log search on your data collection. On the Log Analytics workspace you created earlier in this exercise in the General section, click Logs. On the Queries pane, in the All Queries column, scroll down to the bottom of the list of resource types, and click Virtual machines.

Review the list of predefined queries, select Memory and CPU usage, and click the corresponding Run button.



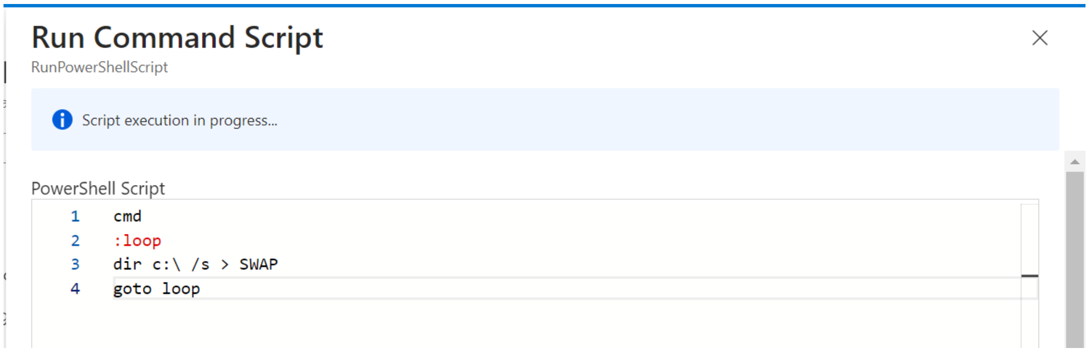
Memory and CPU usage

Chart all computers' used memory and CPU, over the last hour.



```
// Memory and CPU usage
// Chart all computers' used memory and CPU, over the last hour.
Perf
| where TimeGenerated > ago(1h)
| where (CounterName == "% Processor Time" and InstanceName == "_Total") or CounterName == "% Used Memory"
| project TimeGenerated, CounterName, CounterValue
| summarize avg(CounterValue) by CounterName, bin(TimeGenerated, 1m)
| render timechart
```

We then navigated to the Azure VM blade and ran command, on the RunPowerShellScript blade, type the following script, and click Run:



Script execution in progress...

```
cmd
:loop
dir c:\ /s > SWAP
goto loop
```

CONCLUSION

In conclusion, learning how to gather data from Azure virtual machines using Azure Monitor is really important for effective cloud management. This exercise walked you through different steps like setting up a virtual machine, creating a special place to store data called a Log Analytics workspace, turning on a helpful tool called the Log Analytics virtual machine extension, and getting useful information about how your virtual machine is working.