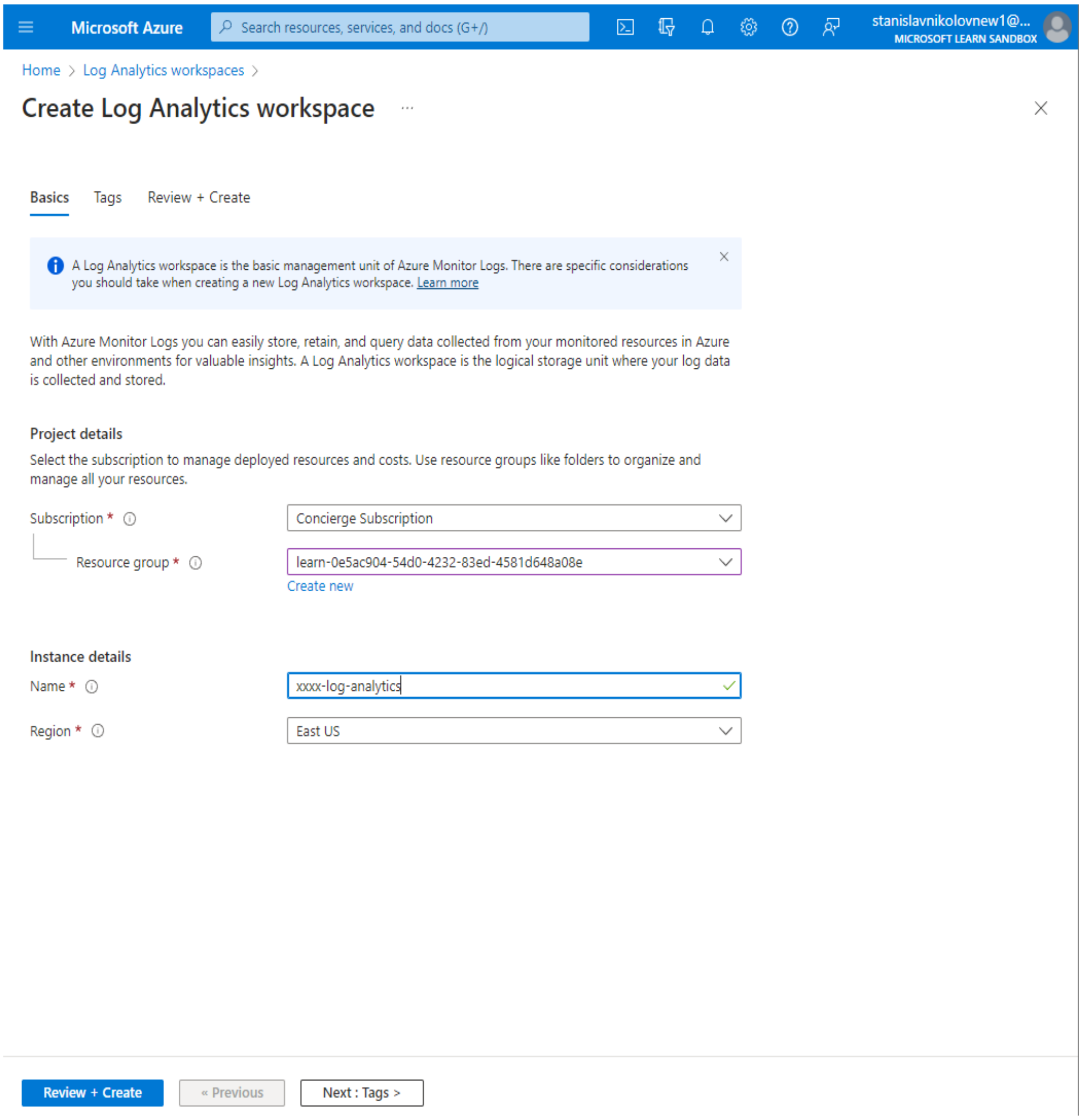
Exercise - Set up a Log Analytics workspace and Azure Monitor VM Insights.

In this unit, we will:

1. **Create a Log Analytics workspace.**
2. **Configure the Log Analytics workspace permissions model for the environment we're supporting.**
3. **Create two virtual machines and onboard both to Azure Monitor VM Insights.**



Create Log Analytics workspace

A Log Analytics workspace is the basic management unit of Azure Monitor Logs. There are specific considerations you should take when creating a new Log Analytics workspace. Learn more

With Azure Monitor Logs you can easily store, retain, and query data collected from your monitored resources in Azure and other environments for valuable insights. A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

Project details

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

Subscription * : Concierge Subscription

Resource group * : learn-0e5ac904-54d0-4232-83ed-4581d648a08e

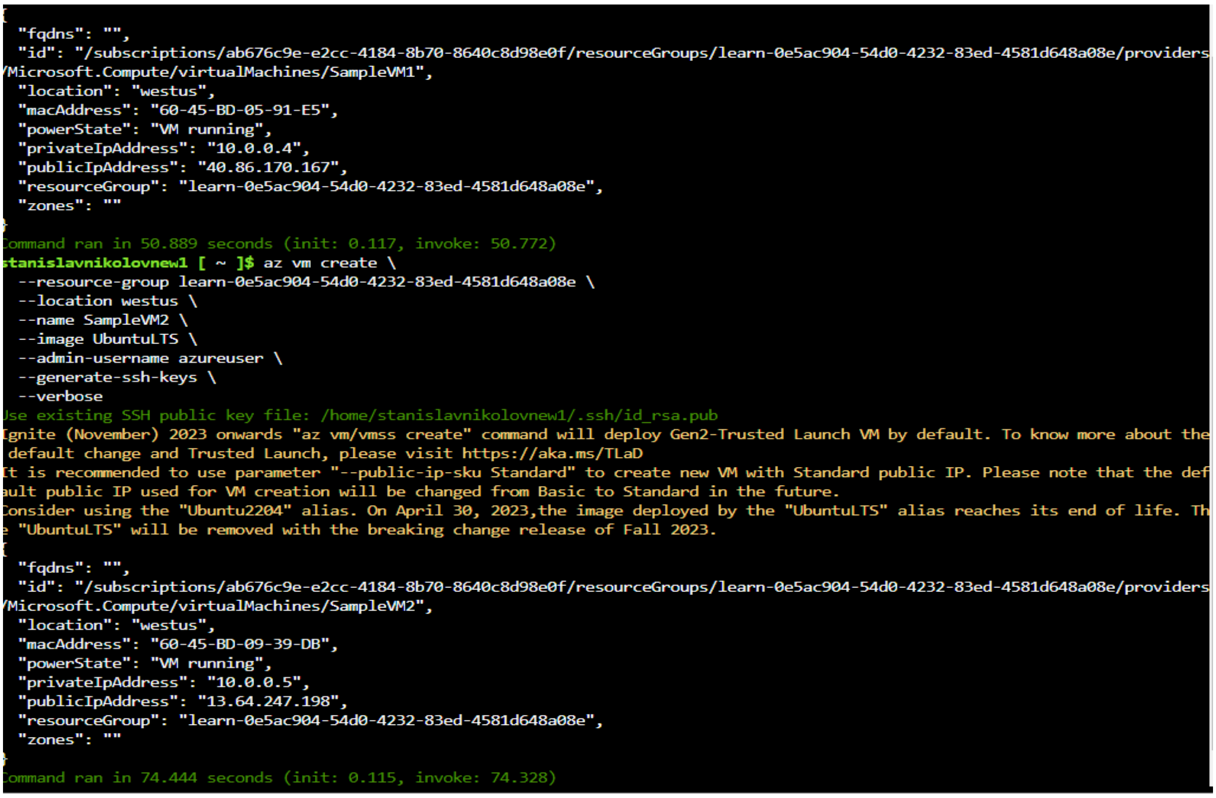
Create new

Instance details

Name * : xxxx-log-analytics

Region * : East US

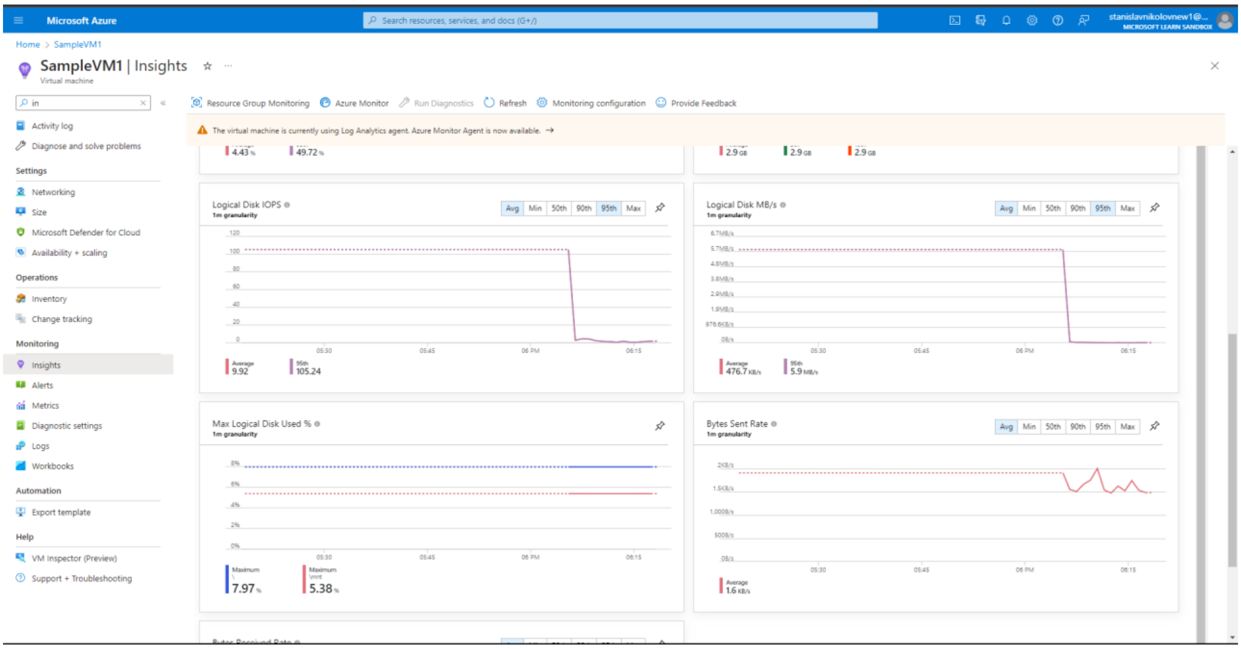
- **Creating log Analytics workspace.**



```
{
  "fqdns": "",
  "id": "/subscriptions/ab676c9e-e2cc-4184-8b70-8640c8d98e0f/resourceGroups/learn-0e5ac904-54d0-4232-83ed-4581d648a08e/providers
/Microsoft.Compute/virtualMachines/SampleVM1",
  "location": "westus",
  "macAddress": "60-45-BD-05-91-E5",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.4",
  "publicIpAddress": "40.86.170.167",
  "resourceGroup": "learn-0e5ac904-54d0-4232-83ed-4581d648a08e",
  "zones": ""
}
Command ran in 50.889 seconds (init: 0.117, invoke: 50.772)
stanislavnikolovnew1 [ ~ ]$ az vm create \
  --resource-group learn-0e5ac904-54d0-4232-83ed-4581d648a08e \
  --location westus \
  --name SampleVM2 \
  --image UbuntuLTS \
  --admin-username azureuser \
  --generate-ssh-keys \
  --verbose
Use existing SSH public key file: /home/stanislavnikolovnew1/.ssh/id_rsa.pub
Ignite (November) 2023 onwards "az vm/vmss create" command will deploy Gen2-Trusted Launch VM by default. To know more about the
 default change and Trusted Launch, please visit https://aka.ms/TLaD
It is recommended to use parameter "--public-ip-sku Standard" to create new VM with Standard public IP. Please note that the def
ault public IP used for VM creation will be changed from Basic to Standard in the future.
Consider using the "Ubuntu2204" alias. On April 30, 2023,the image deployed by the "UbuntuLTS" alias reaches its end of life. Th
e "UbuntuLTS" will be removed with the breaking change release of Fall 2023.
{
  "fqdns": "",
  "id": "/subscriptions/ab676c9e-e2cc-4184-8b70-8640c8d98e0f/resourceGroups/learn-0e5ac904-54d0-4232-83ed-4581d648a08e/providers
/Microsoft.Compute/virtualMachines/SampleVM2",
  "location": "westus",
  "macAddress": "60-45-BD-09-39-DB",
  "powerState": "VM running",
  "privateIpAddress": "10.0.0.5",
  "publicIpAddress": "13.64.247.198",
  "resourceGroup": "learn-0e5ac904-54d0-4232-83ed-4581d648a08e",
  "zones": ""
}
Command ran in 74.444 seconds (init: 0.115, invoke: 74.328)
```

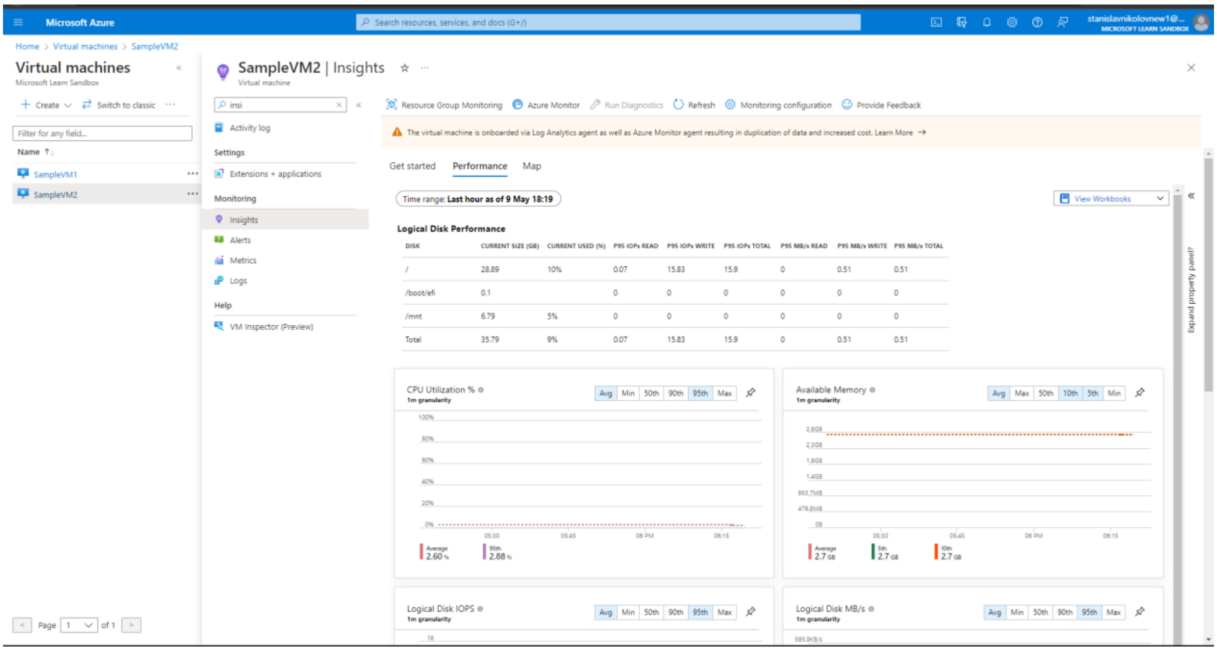
- **Setting up our environment.**

- **Onboard virtual machines to Azure Monitor VM Insights**



The virtual machine is currently using Log Analytics agent. Azure Monitor Agent is now available. →

- **SampleVM1’s Performance tab**



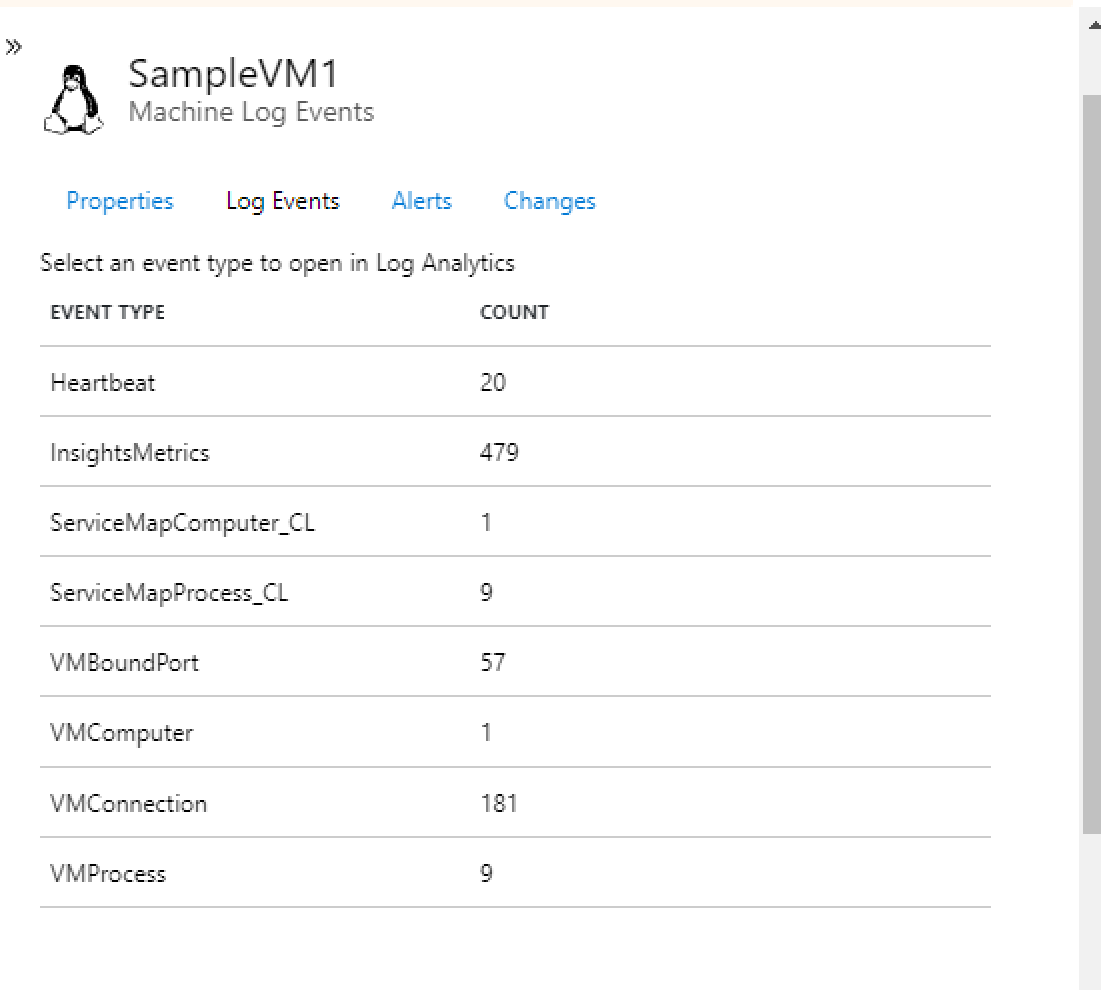
The virtual machine is onboarded via Log Analytics agent as well as Azure Monitor agent resulting in duplication of data and increased cost. Learn More →

Time range: **Last hour as of 9 May 18:19**

Logical Disk Performance

DISK	CURRENT SIZE (GB)	CURRENT USED (%)	P95 IOPs READ	P95 IOPs WRITE	P95 IOPs TOTAL	P95 MB/s READ	P95 MB/s WRITE	P95 MB/s TOTAL
/	28.89	10%	0.07	15.83	15.9	0	0.51	0.51
/boot/efi	0.1		0	0	0	0	0	0
/mnt	6.79	5%	0	0	0	0	0	0
Total	35.79	9%	0.07	15.83	15.9	0	0.51	0.51

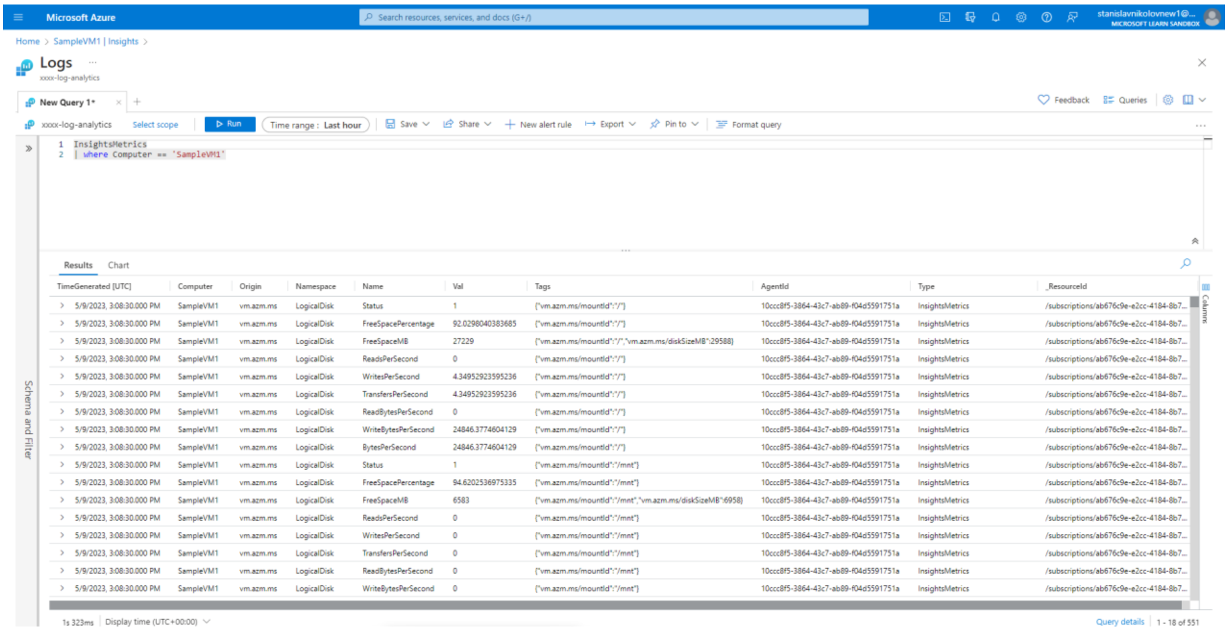
- **SampleVM2's Performance tab.**



Select an event type to open in Log Analytics

EVENT TYPE	COUNT
Heartbeat	20
InsightsMetrics	479
ServiceMapComputer_CL	1
ServiceMapProcess_CL	9
VMBoundPort	57
VMComputer	1
VMConnection	181
VMProcess	9

- **Selecting Log Events for SampleVM1.**

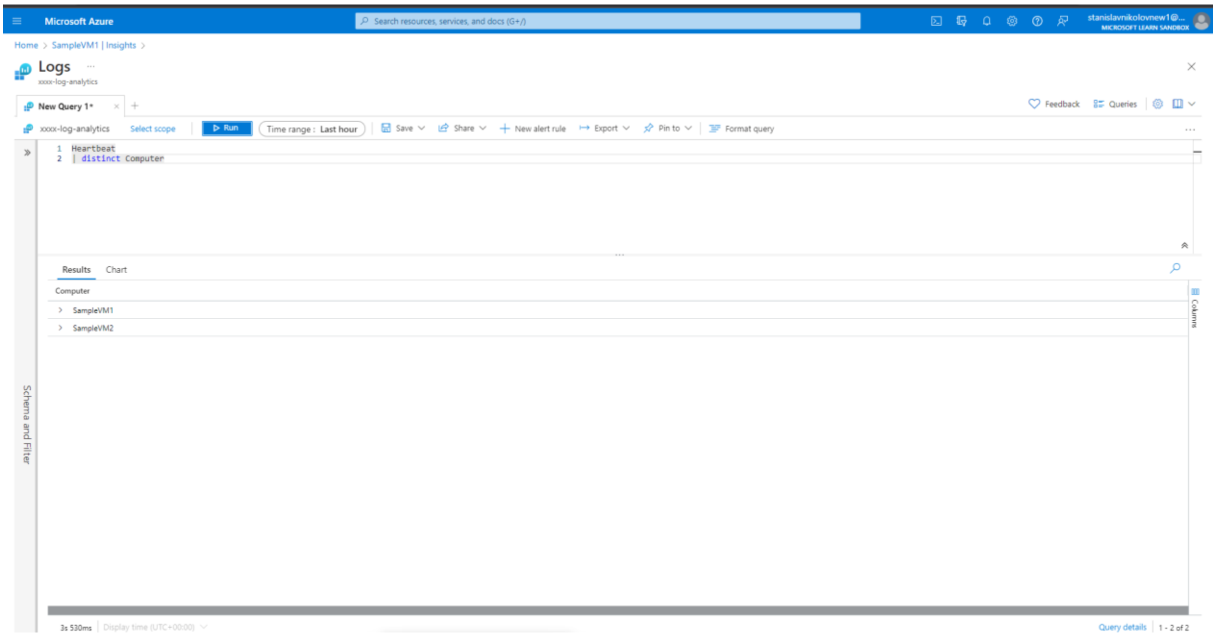


```
InsightsMetrics
| where Computer == 'SampleVM1'
```

TimeGenerated [UTC]	Computer	Origin	Namespace	Name	Val	Tags	AgentId	Type	_ResourceId
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	Status	1	{"vm.azm.ms/mountId":"/"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	FreeSpacePercentage	92.0298040383685	{"vm.azm.ms/mountId":"/"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	FreeSpaceMB	27229	{"vm.azm.ms/mountId":"/","vm.azm.ms/diskSizeMB":29588}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	ReadsPerSecond	0	{"vm.azm.ms/mountId":"/"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	WritesPerSecond	4.34952923595236	{"vm.azm.ms/mountId":"/"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	TransfersPerSecond	4.34952923595236	{"vm.azm.ms/mountId":"/"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	ReadBytesPerSecond	0	{"vm.azm.ms/mountId":"/"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	WriteBytesPerSecond	24846.3774604129	{"vm.azm.ms/mountId":"/"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	BytesPerSecond	24846.3774604129	{"vm.azm.ms/mountId":"/"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	Status	1	{"vm.azm.ms/mountId":"/mnt"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	FreeSpacePercentage	94.6202536975335	{"vm.azm.ms/mountId":"/mnt"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	FreeSpaceMB	6583	{"vm.azm.ms/mountId":"/mnt","vm.azm.ms/diskSizeMB":6958}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	ReadsPerSecond	0	{"vm.azm.ms/mountId":"/mnt"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	WritesPerSecond	0	{"vm.azm.ms/mountId":"/mnt"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	TransfersPerSecond	0	{"vm.azm.ms/mountId":"/mnt"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	ReadBytesPerSecond	0	{"vm.azm.ms/mountId":"/mnt"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...
5/9/2023, 3:08:30.000 PM	SampleVM1	vm.azm.ms	LogicalDisk	WriteBytesPerSecond	0	{"vm.azm.ms/mountId":"/mnt"}	10ccc8f5-3864-43c7-ab89-f04d5591751a	InsightsMetrics	/subscriptions/ab676c9e-e2cc-4184-8b7...

1s 323ms | Display time (UTC+00:00) | Query details | 1 - 18 of 551

- **The logs section of a Log Analytics workspace opens with a prepopulated query showing the data being collected.**

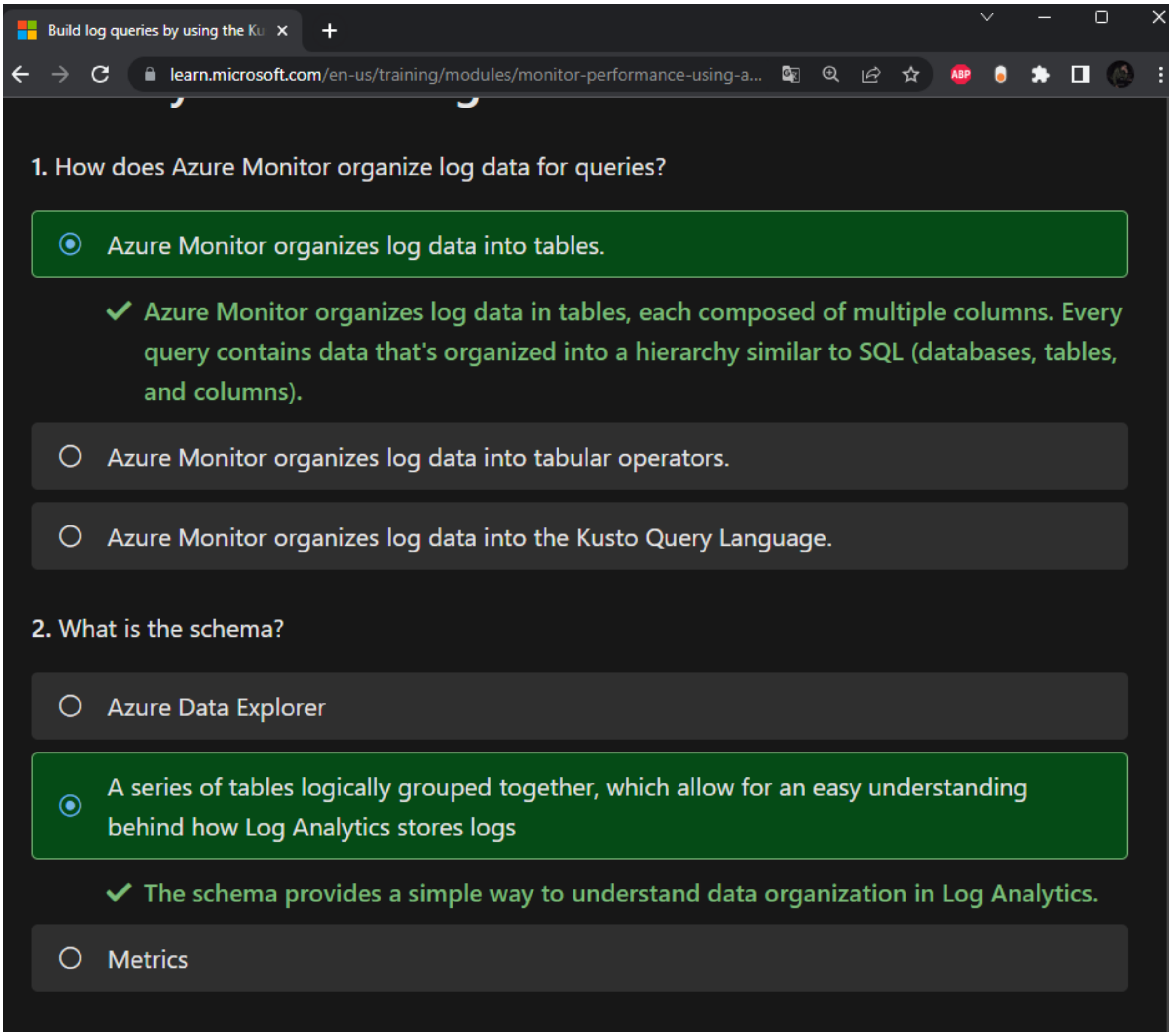


```
Heartbeat
| distinct Computer
```

Computer
SampleVM1
SampleVM2

3s 530ms | Display time (UTC+00:00) | Query details | 1 - 2 of 2

- **Building simple log queries by using the Kusto Query Language.**



Build log queries by using the Ku
learn.microsoft.com/en-us/training/modules/monitor-performance-using-a...

1. How does Azure Monitor organize log data for queries?

● Azure Monitor organizes log data into tables.

✓ Azure Monitor organizes log data in tables, each composed of multiple columns. Every query contains data that's organized into a hierarchy similar to SQL (databases, tables, and columns).

○ Azure Monitor organizes log data into tabular operators.

○ Azure Monitor organizes log data into the Kusto Query Language.

2. What is the schema?

○ Azure Data Explorer

● A series of tables logically grouped together, which allow for an easy understanding behind how Log Analytics stores logs

✓ The schema provides a simple way to understand data organization in Log Analytics.

○ Metrics

- **Final Quiz.**